Fragments of intuitionistic logic and proof complexity

Emil Jeřábek
jerabek@math.cas.cz
http://math.cas.cz/~jerabek/

Institute of Mathematics of the Czech Academy of Sciences, Prague

Logic, Algebra and Truth Degrees, June 2016, Phalaborwa
Outline

1 Propositional proof complexity

2 Intuitionistic logic

3 Intuitionistic fragments
Propositional proof complexity

1 Propositional proof complexity

2 Intuitionistic logic

3 Intuitionistic fragments
Proof complexity

Fix a language $L \subseteq \Sigma^*$

Example: (the set of tautologies of) a propositional logic

- proof system for $L$: polynomial-time predicate $P(w, \pi)$ s.t.

$$w \in L \iff \exists \pi P(w, \pi)$$

- we are interested in the length (size) of proofs

$$s_P(w) = \min\{|\pi| : P(w, \pi)\}$$

- $P$ is polynomially bounded if $s_P(w) \leq |w|^c \quad \forall w \in L$

- $P$ p-simulates $Q$ if there is a poly-time $f$ s.t.

$$Q(w, \pi) \implies P(w, f(w, \pi))$$
Proof system = **nondeterministic acceptor** for $L$

- $L$ has a polynomially bounded proof system iff $L \in \text{NP}$
- [CR7x] CPC has a polynomially bounded proof system iff $\text{NP} = \text{coNP}$
  - we expect all proof systems for CPC to require exponential-size proofs
  - only proven for weak systems (resolution, bounded-depth, . . . )

- nonclassical logics: often more complex
  - IPC: \text{PSPACE}-complete
  - in principle, could make lower bounds easier
Frege systems

Frege proof: sequence of formulas, each derived from earlier by instances of a fixed finite set of schematic axioms and rules

\[ \varphi_1, \ldots, \varphi_k \vdash \psi \]

Required: sound and complete \( \Gamma \vdash_F \varphi \iff \Gamma \vdash_L \varphi \)

- robust notion:
  - independent of the choice of rules
  - \( \equiv \) sequent calculi, natural deduction, …
  - \( \equiv \) tree-like Frege (usually)

- in classical logic (CPC):
  - lower bounds \( \Omega(n^2) \) on size, \( \Omega(n) \) on \# of lines
  - hardly any candidates for hard tautologies
Extended Frege

Frege $\rightarrow$ extended Frege (EF)

- allow introduction of abbreviations (extension variables)
  
  $q \iff \psi$

- equivalently: use circuits (dags) instead of formulas
- equivalently (sort of): count $\#$ of lines instead of size

substitution Frege (SF)

- allow explicit substitution rule
- CPC-\(EF \equiv_p \) CPC-SF
- nonclassical logics: often SF more powerful than EF
Intuitionistic logic

1 Propositional proof complexity

2 Intuitionistic logic

3 Intuitionistic fragments
Intuitionistic Frege/EF systems:

The most important tool is the feasible disjunction property

- simplest case [BM99, BP01]:
  given a proof of \( \varphi \lor \psi \), find in poly-time a proof of \( \varphi \) or \( \psi \)
- classical analogue: feasible interpolation
- \( \implies \) conditional exponential lower bounds for IPC-EF
- monotone variants [Hru07, 09]:
  \( \implies \) unconditional exponential lower bounds for IPC-EF
- generalization [J09]: exp. separation of EF from SF for IPC and si logics of unbounded branching
Without disjunction?

All known lower bounds for IPC-\(EF\) rely on feasible DP
\[\implies\text{tautologies prominently use disjunction}\]

\[\theta(\vec{p},\vec{q}) \rightarrow \alpha(\vec{p},\vec{s}) \lor \beta(\vec{q},\vec{r})\]

Question (P. Hrubeš)

What is the complexity of proving implicational tautologies in IPC-\(EF\)?

N.B.: IPC\(\rightarrow\) is still PSPACE-complete
Implicational tautologies

Answer [J15]

Just about the same as for arbitrary tautologies

poly-time transformations:

formula $\varphi \rightsquigarrow$ implicational formula $\varphi \rightarrow$

$L$-EF proof of $\varphi \iff L$-EF proof of $\varphi \rightarrow$ \hspace{1cm} ($L \supseteq IPC$)

- trade-off: restrictions on $\varphi$ or on $L$
- side effect: also eliminate $\lor, \ldots$ from proofs
Applicable to arbitrary logics $L$:

**Theorem**

Given a formula $\varphi$ with no “essential” negatively occurring $\lor$, $\bot$, we can construct in poly time

- an implicational formula $\varphi \rightarrow$
- IPC-EF proof of $\sigma(\varphi \rightarrow) \rightarrow \varphi$ for a substitution $\sigma$
- IPC-EF proof of $\varphi \rightarrow \varphi \rightarrow$
Applicable to arbitrary formulas $\varphi$:

**Theorem**

Let $L$ be an extension of IPC by implicational axioms. Given a formula $\varphi$, we can construct in poly-time

- an implicational formula $\varphi \rightarrow$
- IPC-EF proof of $\sigma(\varphi \rightarrow) \rightarrow \varphi$ for a substitution $\sigma$

s.t. given an $L$-EF proof of $\varphi$, we can construct in polytime an $L$-EF proof of $\varphi \rightarrow$
Application to known hard tautologies:

**Theorem**

There is a sequence of implicational tautologies $\varphi_n$ s.t.

- $\varphi_n$ has poly-time constructible $\text{IPC}_{\rightarrow}$-$\text{SF}$ proofs
- $\varphi_n$ requires exponential-size $L$-$\text{EF}$ proofs for any $L \supseteq \text{IPC}$ of unbounded branching
Eliminate connectives from proofs

The argument involves elimination of $\lor / \bot$ from $L$-$EF$ proofs of implicational tautologies

- basic idea: emulate $\bot$ by

$$\bigwedge_{i} p_i$$

and $\alpha \lor \beta$ by

$$\bigwedge_{i} ((\alpha \rightarrow p_i) \rightarrow (\beta \rightarrow p_i) \rightarrow p_i)$$

- related to Diego’s theorem
Theorem

Let $P$ be an extension of the standard IPC-EF calculus by an implicational axiom schema.

Given a $P$-proof of $\varphi$, we can construct in poly time a $P$-proof $\pi$ of $\varphi$ s.t.

- if $\bot$ doesn’t occur in $\varphi$, it doesn’t occur in $\pi$
- the only disjunctions in $\pi$ are subformulas of $\varphi$
The argument does not eliminate conjunctions:

- no “definition” of $\land$ by implicational formulas?
- we even get new conjunctions when eliminating $\lor$ or $\bot$

**Question**

Can we generalize the elimination theorem to $\land$ anyway?
Intuitionistic fragments

1. Propositional proof complexity

2. Intuitionistic logic

3. Intuitionistic fragments
Proofs in fragments

Forget length of proofs

Our elimination result implies:

**Corollary**

Let $X$ be a set of implicational axioms

If $IPC + X$ proves an implicational formula $\varphi$, then so does $IPC_{\rightarrow,\land} + X$

That is: $IPC + X \rightarrow = (IPC_{\rightarrow,\land} + X) \rightarrow$

Similar consequences also hold for fragments with $\lor$ or $\bot$

Let us name the concept . . .
Hereditary conservativity

\( L_C = \text{the fragment of logic } L \text{ in language } C \)

**Definition**

Let

- \( C_0, C_1 \) be languages with a common sublanguage \( C \)
- \( L_i \) be a logic in language \( C_i, i = 0, 1 \)

Then \( L_0 \) is hereditarily \( C \)-conservative over \( L_1 \) if

\[
(L_0 + X)_C \subseteq (L_1 + X)_C
\]

for all sets \( X \) of \( C \)-formulas
Corollary

Let $\rightarrow \in C \subseteq C_i \subseteq C_{IPC}$, $i = 0, 1$. Then

$$C_0 \subseteq C_1 \quad \text{or} \quad \land \in C_1$$  \hspace{1cm} (i)

\[\Downarrow\]

IPC\(_{C_0}\) is hereditarily $C$-conservative over IPC\(_{C_1}\)  \hspace{1cm} (ii)

If we could eliminate $\land$ the same way, we could drop (i)
Hereditary conservativity for IPC (2)

**Theorem [Wro80]**

Let $\rightarrow \in C \subseteq C_i \subseteq C_{\text{IPC}}$, $i = 0, 1$. Then

$$C_0 \subseteq C_1 \quad \text{or} \quad \land \in C_1$$

(i)

\[\iff\]

IPC$_{C_0}$ is hereditarily $C$-conservative over IPC$_{C_1}$

(ii)

\[\implies\]

we cannot eliminate $\land$ in such a generality
The next best thing (using a different method):

**Theorem**

Let $P$ be an extension of the standard IPC-EF calculus by an implicational axiom schema $\alpha$ such that

$$(\text{IPC} + \alpha) \rightarrow = \text{IPC} \rightarrow + \alpha$$

Given a $P$-proof of $\varphi$, we can construct in poly time a $P$-proof $\pi$ of $\varphi$ s.t.

- if $\bot$ doesn’t occur in $\varphi$, it doesn’t occur in $\pi$
- the only disjunctions in $\pi$ are subformulas of $\varphi$
- the only conjunctions in $\pi$ are subformulas of $\varphi$
Thank you for attention!
S. R. Buss, G. Mints: The complexity of the disjunction and existential properties in intuitionistic logic, APAL 99 (1999), 93–104


S. A. Cook, R. A. Reckhow: The relative efficiency of propositional proof systems, JSL 44 (1979), 36–50

P. Hrubeš: Lower bounds for modal logics, JSL 72 (2007), 941–958

_______: A lower bound for intuitionistic logic, APAL 146 (2007), 72–90

_______: On lengths of proofs in non-classical logics, APAL 157 (2009), 194–205

E. Jeřábek: Substitution Frege and extended Frege proof systems in non-classical logics, APAL 159 (2009), 1–48
