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.

$$Q(w, \pi) \implies P(w, f(w, \pi))$$

Relation to computational complexity

Proof system = nondeterministic acceptor for L

- L has a polynomially bounded proof system iff $L \in \mathrm{NP}$
- [CR7x] CPC has a polynomially bounded proof system iff $\mathrm{NP} = \mathrm{coNP}$
  - 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: 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

$$\varphi_1, \dots, \varphi_k \,/\, \psi$$

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 $\to$ extended Frege (EF)

- allow introduction of abbreviations (extension variables)

$$q \rightleftarrows \psi$$

- 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

Intuitionistic proof complexity

Intuitionistic Frege/EF systems:

The most important tool is the feasible disjunction property

- simplest case [BM99,BP01]:
  given a proof of $\varphi \vee \psi$, find in poly-time a proof of φ or ψ
- classical analogue: feasible interpolation
- $\Longrightarrow$ conditional exponential lower bounds for IPC-*EF*
- monotone variants [Hru07,09]:
  $\Longrightarrow$ 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
$\Longrightarrow$ tautologies prominently use disjunction

$$\theta(\vec{p}, \vec{q}) \to \alpha(\vec{p}, \vec{s}) \vee \beta(\vec{q}, \vec{r})$$

Question (P. Hrubeš)

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

N.B.: $\mathrm{IPC}_{\to}$ is still PSPACE-complete

Implicational tautologies

Answer [J15]

Just about the same as for arbitrary tautologies

poly-time transformations:

formula $\varphi \rightsquigarrow$ implicational formula $\varphi^{\to}$

L-EF proof of $\varphi \leftrightsquigarrow$ L-EF proof of $\varphi^{\to}$ $\qquad (L \supseteq \mathrm{IPC})$

- trade-off: restrictions on φ or on L
- side effect: also eliminate $\vee, \dots$ from proofs

Sample result (1)

Applicable to arbitrary si logics L:

Theorem

Given a formula φ with no "essential" negatively occurring $\vee, \bot$, we can construct in poly time

- an implicational formula $\varphi^{\to}$
- IPC-*EF* proof of $\sigma(\varphi^{\to}) \to \varphi$ for a substitution σ
- IPC-*EF* proof of $\varphi \to \varphi^{\to}$

Sample result (2)

Applicable to arbitrary formulas φ:

Theorem

Let L be an extension of IPC by implicational axioms.

Given a formula φ, we can construct in poly-time

- an implicational formula $\varphi^{\to}$
- IPC-*EF* proof of $\sigma(\varphi^{\to}) \to \varphi$ for a substitution σ

s.t. given an *L*-*EF* proof of φ, we can construct in poly time an *L*-*EF* proof of $\varphi^{\to}$

Sample result (3)

Application to known hard tautologies:

Theorem

There is a sequence of implicational tautologies φ_n s.t.

- φ_n has poly-time constructible $\mathrm{IPC}_{\to}$-SF proofs
- φ_n requires exponential-size L-EF proofs
  for any $L \supseteq \mathrm{IPC}$ of unbounded branching

Eliminate connectives from proofs

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

- basic idea: emulate $\bot$ by

$$\bigwedge_i p_i$$

and $\alpha \vee \beta$ by

$$\bigwedge_i ((\alpha \to p_i) \to (\beta \to p_i) \to p_i)$$

- related to Diego's theorem

Sample result (4)

Theorem

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

Given a P-proof of φ, we can construct in poly time a P-proof π of φ s.t.

- if $\perp$ doesn't occur in φ, it doesn't occur in π
- the only disjunctions in π are subformulas of φ

Conjunctions?

The argument does not eliminate conjunctions:

- no "definition" of $\wedge$ by implicational formulas?
- we even get new conjunctions when eliminating $\vee$ or $\bot$

Question

Can we generalize the elimination theorem to $\wedge$ 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 $\mathrm{IPC} + X$ proves an implicational formula φ, then so does $\mathrm{IPC}_{\to,\wedge} + X$

That is: $(\mathrm{IPC} + X)_{\to} = (\mathrm{IPC}_{\to,\wedge} + X)_{\to}$

Similar consequences also hold for fragments with $\vee$ or $\perp$

Let us name the concept ...

Hereditary conservativity

L_C = the fragment of logic L 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

Hereditary conservativity for IPC (1)

Corollary

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

$$C_0 \subseteq C_1 \quad \text{or} \quad \wedge \in C_1 \tag{i}$$

$$\Big\Downarrow$$

$$\mathrm{IPC}_{C_0} \text{ is hereditarily } C\text{-conservative over } \mathrm{IPC}_{C_1} \tag{ii}$$

If we could eliminate $\wedge$ the same way, we could drop (i)

Hereditary conservativity for IPC (2)

Theorem [Wro80]

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

$$C_0 \subseteq C_1 \quad \text{or} \quad \wedge \in C_1 \qquad \text{(i)}$$

$$\Updownarrow$$

$$\mathrm{IPC}_{C_0} \text{ is hereditarily } C\text{-conservative over } \mathrm{IPC}_{C_1} \qquad \text{(ii)}$$

$\Longrightarrow$ we cannot eliminate $\wedge$ in such a generality

Elimination of $\wedge$

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 α such that

$$(\mathrm{IPC} + \alpha)_{\to} = \mathrm{IPC}_{\to} + \alpha$$

Given a P-proof of φ, we can construct in poly time a P-proof π of φ s.t.

- if $\bot$ doesn't occur in φ, it doesn't occur in π
- the only disjunctions in π are subformulas of φ
- the only conjunctions in π are subformulas of φ

Thank you for attention!

References

- S. R. Buss, G. Mints: The complexity of the disjunction and existential properties in intuitionistic logic, APAL 99 (1999), 93–104
- S. R. Buss, P. Pudlák: On the computational content of intuitionistic propositional proofs, APAL 109 (2001), 49–64
- 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
- ________: Proof complexity of intuitionistic implicational formulas, preprint, 2015, 45 pp., arXiv:1512.05667 [cs.LO]
- A. Wroński: On reducts of intermediate logics, Bull. Sect. Log. 9 (1980), 176–179