Proof systems for modal logics

Emil Jeřábek

jerabek@math.cas.cz

Institute of Mathematics of the AS CR, Prague

Propositional proof complexity

Studies efficiency (absolute or relative) of proof systems.

A propositional proof system (pps) is a poly-time function P whose range are the tautologies [Cook, Reckhow '79]

Example: Frege systems, sequent calculi, resolution, Lovász–Schrijver, . . .

A pps P p-simulates a pps Q ($Q \leq_p P$) if we can translate Q-proofs to P-proofs of the same formula in polynomial time.

Basic motivation: computational complexity ($\mathbf{NP} \stackrel{?}{=} \mathbf{coNP}$)
$\Rightarrow$ most often: classical logic ($\mathbf{CPC}$).
Nothing stops us from considering non-classical logics.
($\mathbf{NP} \stackrel{?}{=} \mathbf{PSPACE}$)

Modal and si logics

A normal modal logic (nml):

- Boolean connectives, unary connective $\Box$
- contains $\mathbf{CPC}$, $\Box(\varphi \to \psi) \to (\Box\varphi \to \Box\psi)$, closed under substitution, modus ponens, necessitation ($\varphi \vDash \Box\varphi$)

Example: $\mathbf{K}$, $\mathbf{K4}$, $\mathbf{T}$, $\mathbf{S4}$, $\mathbf{GL}$, $\mathbf{Grz}$, $\mathbf{S4.2}$, $\mathbf{K4.3}$, $\mathbf{KTB}$, $\mathbf{S5}$, ...
(there should be $2^{\aleph_0}$ dots rather than three)

An intermediate = superintuitionistic (si) logic:

- intuitionistic connectives $\to$, $\wedge$, $\vee$, $\bot$
- contains the intuitionistic logic ($\mathbf{IPC}$), closed under substitution, modus ponens

Example: $\mathbf{IPC}$, $\mathbf{CPC}$, $\mathbf{KC}$, $\mathbf{LC}$, $\mathbf{KP}$, ...

Frege systems

Frege systems (F) (aka Hilbert-style calculi):

- finite set P of Frege rules $\varphi_1, \dots, \varphi_n \vdash \varphi$
- proof: a sequence of formulas, each an assumption of the proof or derived from earlier ones by an instance of a P-rule
- sound: $\vdash_P \varphi \Rightarrow \models_L \varphi$
- strongly complete: $\Gamma \models_L \varphi \Rightarrow \Gamma \vdash_P \varphi$

Standard Frege systems: strongly sound ($\Gamma \vdash_P \varphi \Rightarrow \Gamma \models_L \varphi$)
We denote the standard Frege system for a logic L by L-F.

Many other common proof systems are p-equivalent to L-F: sequent calculi (with cut), natural deduction

Extended and substitution Frege

Given a Frege system (its set of Frege rules), we can also define other proof systems.

Extended Frege (EF) systems:

- may introduce shorthands (extension variables) for formulas: $q_\varphi \leftrightarrow \varphi$
- or: work with circuits instead of formulas
- or: count only lines of the proof, not individual symbols

Substitution Frege (SF) systems:

- may use substitution directly as a rule of inference

General simulations

Consider a principle of the form:

(S) If φ is valid in L, then φ' is valid in L'.

(Typically a model-theoretic argument.)

Let P be a proof system for L, and P' a proof system for L'.
A feasible version of (S):

(FS) Given a P-proof of φ, we can construct in polynomial time a P'-proof of φ'.

Example: If $L = L'$, $\varphi = \varphi'$, it's the usual p-simulation of pps.

Disjunction property

DP: If $\vdash_L \varphi \vee \psi$, then $\vdash_L \varphi$ or $\vdash_L \psi$.
Example: $\mathbf{IPC}$, $\mathbf{KP}$, $\mathbf{T}_k$, ...
Restricted variant (φ, ψ negative): all si $L \not\supseteq \mathbf{KC}$.

Modal DP: if $\vdash_L \Box\varphi \vee \Box\psi$, then $\vdash_L \varphi$ or $\vdash_L \psi$.
Example: $\mathbf{K}$, $\mathbf{K4}$, $\mathbf{S4}$, $\mathbf{GL}$, ...
Restricted variants hold for almost all nml.

Feasible DP:
L-F (and L-EF), where L is

- $\mathbf{IPC}$ [Buss, Mints '99]
- $\mathbf{S4}$, $\mathbf{S4.1}$, $\mathbf{Grz}$, $\mathbf{GL}$ [Ferrari & al. '05]
- "extensible" modal logics [J. '06]
- ...

Feasible DP for K (example)

Theorem: If π is a $\mathbf{K}$-F-proof of $\bigvee_{i \leq k} \Box\varphi_i$, then the closure of π under MP contains φ_i for some $i \leq k$.

Proof:

Let Π be the closure. Define a propositional valuation v by

$$v(\Box\varphi) = 1 \quad \text{iff} \quad \varphi \in \Pi.$$

We show $v(\varphi) = 1$ for all $\varphi \in \pi$ by induction:

- The steps for rules of $\mathbf{CPC}$, and Nec are trivial.
- $\Box(\varphi \to \psi) \to (\Box\varphi \to \Box\psi)$: OK, as Π is closed under MP.

Hence $v(\bigvee_{i \leq k} \Box\varphi_i) = 1$, which implies $\varphi_i \in \Pi$ for some i by the definition of v. QED

NB: In $\mathbf{IPC}$, use Kleene-like slash for v [Mints, Kojevnikov '04]

Admissible rules

A multiple-conclusion rule $\varphi_1, \dots, \varphi_n \,/\, \psi_1, \dots, \psi_m$ is admissible in L, if for every substitution σ:

$$\forall i \;\vdash_L \sigma\varphi_i \quad \Rightarrow \quad \exists j \;\vdash_L \sigma\psi_j$$

Example: DP = $p \vee q \,/\, p, q$
Kreisel–Putnam rule $\neg p \to q \vee r \,/\, (\neg p \to q) \vee (\neg p \to r)$

Theorem: If L is

- $\mathbf{IPC}$ [Mints, Kojevnikov '04]
- an extensible modal logic (e.g. $\mathbf{K4}$, $\mathbf{S4}$, $\mathbf{GL}$) [J. '06]

then every L-admissible rule is feasibly admissible in L-F (and L-EF).

Corollary: All Frege systems for L are p-equivalent.

Partial conservativity

Example: $\mathbf{IPC}$-F p-simulates $\mathbf{CPC}$-F wrt negative formulas.
Proof: Prefix $\neg\neg$ to every formula in the proof. QED

Example: $\mathbf{KC}$-F p-simulates $\mathbf{CPC}$-F wrt essentially negative formulas.

Theorem [J. ’07]
$\mathbf{IPC}$-F p-simulates $\mathbf{KC}$-F wrt $\bot$-free formulas.

Proof: Let v be the classical valuation which makes every variable true. Use the translation

$$(\varphi \to \psi)^* = \begin{cases} \bot & v(\varphi \to \psi) = 0, \\ \varphi^* \to \psi^* & v(\varphi \to \psi) = 1. \end{cases}$$

Partial conservativity (cont'd)

Theorem [essentially Atserias & al. '02]
$\mathbf{IPC}$-F p-simulates $\mathbf{CPC}$-F wrt formulas $\alpha_1 \to \alpha_2$, where α_i are monotone.

Let L^A denote the extension of L with universal modality Ap:

$$A(\varphi \to \psi) \to (A\varphi \to A\psi)$$

$$A\varphi \to \varphi \qquad\qquad A\varphi \vee A\neg A\varphi$$

$$A\varphi \to \Box\varphi \qquad\qquad \varphi \vdash A\varphi$$

Semantics: $x \Vdash A\varphi \quad \text{iff} \quad \forall y\, (y \Vdash \varphi)$

Theorem [J. '07] If L is a si or transitive modal logic, then L^A-EF is p-equivalent to L-SF wrt L-formulas.

Model checking

If L has poly model property, and is FO on finite frames:
Describe L-validity of φ by a classical formula φ^L
$\Rightarrow$ poly-time faithful interpretation of L in $\mathbf{CPC}$

Theorem [J. '07]
If L is

- tabular, or
- of finite width and depth, or
- $\mathbf{K4BW}_k \pm \mathbf{S4} \pm \mathbf{Grz} \pm \mathbf{GL}$, or
- $\mathbf{LC}$,

then L-EF is p-equivalent to $\mathbf{CPC}$-EF wrt $(\cdot)^L$.

Lower bounds

"Construct simulations to show the nonexistence of simulations"

[Pudlák '99] Feasible DP gives a kind of feasible interpolation for classical logic. Hence circuit lower bounds imply lower bounds on the length of proofs:

Theorem If there exists a pair of disjoint $\mathbf{NP}$ sets inseparable in $\mathbf{P}/poly$, there are superpolynomial LB on the size of $\mathbf{IPC}$-F-proofs.

[Hrubeš '06] A more clever variant of FDP gives feasible monotone interpolation $\Rightarrow$ can use known unconditional LB on monotone circuits:

Theorem There are exponential LB on the size of EF-proofs in $\mathbf{K}$, $\mathbf{S4}$, $\mathbf{GL}$, $\mathbf{IPC}$.

EF and SF

Classically, EF and SF are p-equivalent. In general: L-$EF \leq_p L$-SF, actually L-$EF \equiv_p L$-SF^* (treelike SF)

The results above ("model checking", . . .) imply:

Theorem [J. '07] L-$EF \equiv_p L$-SF, if L is

- an extension of $\mathbf{KB}$,
- tabular,
- of finite width and depth,
- $\mathbf{LC}$, $\mathbf{K4BW}_k \pm \mathbf{S4} \pm \mathbf{Grz} \pm \mathbf{GL}$.

OTOH, a generalization of Hrubeš's LB gives:

Theorem [J. '07] If L is a si or modal logic with infinite branching, then L-SF has exponential speed-up over L-EF.

Some questions

Problem Does $\mathbf{IPC}$-EF simulate $\mathbf{S4}$-EF-proofs of formulas translated by the Gödel–Tarski–McKinsey translation?

(More generally: ϱL-EF vs. L-EF)

Problem Separate L-EF from L-F for some logic L.

Thank you for attention!

References

A. Atserias, N. Galesi, P. Pudlák, *Monotone simulations of non-monotone proofs*, JCSS 65 (2002), 626–638.

S. Buss, G. Mints, *The complexity of the disjunction and existential properties in intuitionistic logic*, APAL 99 (1999), 93–104.

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

M. Ferrari, C. Fiorentini, G. Fiorino, *On the complexity of the disjunction property in intuitionistic and modal logics*, TOCL 6 (2005), 519–538.

P. Hrubeš, *Lower bounds for modal logics*, to appear in JSL.

References (cont'd)

P. Hrubeš, *A lower bound for intuitionistic logic*, APAL 146 (2007), 72–90.

E. Jeřábek, *Frege systems for extensible modal logics*, APAL 142 (2006), 366–379.

E. Jeřábek, *Substitution Frege and extended Frege proof systems in non-classical logics*, preprint, 2007.

G. Mints, A. Kojevnikov, *Intuitionistic Frege systems are polynomially equivalent*, Zapiski Nauchnyh Seminarov POMI 316 (2004), 129–146.

P. Pudlák, *On the complexity of propositional calculus*, in: Sets and Proofs, Invited papers from Logic Colloquium'97, CUP 1999, 197–218.