Disjunction properties in modal proof complexity

Emil Jeřábek

jerabek@math.cas.cz

http://math.cas.cz/~jerabek/

Institute of Mathematics, Czech Academy of Sciences, Prague

The Utrecht Logic in Progress Series
9 February 2021

Classical proof complexity

- proof system (pps) P:
  poly-time predicate $P(x, \varphi)$ "x is a P-proof of φ"
  sound and complete:
  φ has a P-proof $\iff$ it is a classical tautology
- examples: Resolution, Hilbert-Frege systems, sequent calculi, polynomial calculus, ...
- length of proofs: $s_P(\varphi) = \min\{|x| : P(x, \varphi)\}$
  polynomial in $|\varphi|$? exponential in $|\varphi|$?
- P polynomially bounded $\iff \forall \varphi \in \mathrm{TAUT}\ s_P(\varphi) \le |\varphi|^c$
- $\mathrm{NP} \ne \mathrm{coNP} \iff$ no pps is polynomially bounded
- P p-simulates Q ($Q \le_p P$): $\exists$ poly-time $t(x, \varphi)$ s.t.
  $Q(x, \varphi) \implies P(t(x, \varphi), \varphi)$

The textbook proof system

Frege system (F)

- finitely many schematic rules

$$\frac{\alpha_1\ \alpha_2\ \ \dots\ \ \alpha_d}{\alpha_0}$$

- proof of φ: sequence of formulas $\theta_0, \dots, \theta_z = \varphi$ each derived from previous ones by a substitution instance of one of the rules
- the choice of rules does not matter (up to p-equivalence)
- typical example: axiom schemata + modus ponens (MP) $\varphi, \varphi \to \psi \ / \ \psi$
- p-equivalent to sequent calculus (with cut), natural deduction

Variants of Frege

Substitution Frege (SF)

- $+$ substitution as a derivation rule

Extended Frege (EF)

- $+$ extension axioms $q \leftrightarrow \psi$ to abbreviate formulas
- equivalently: Frege with circuits instead of formulas
- equivalently: count only the number of lines, ignore the size of the formulas

Proof complexity:

- $EF \equiv_p SF$ expected to have exponential speedup over F
- unconditional lower bounds on F or EF: only $\Omega(n^2)$

Good unconditional lower bounds: only very weak pps

- Resolution, constant-depth Frege

Feasible interpolation

Interpolation problem for a pps P:
given a P-proof of $\varphi_0(\vec{p},\vec{q}^0) \vee \varphi_1(\vec{p},\vec{q}^1)$ and an assignment $\vec{a}$, pinpoint $i \in \{0,1\}$ s.t. $\varphi_i(\vec{a},\vec{q}^i)$ is a tautology

If solvable in polynomial time: P has feasible interpolation

Example: Resolution has f.i.

Feasible interpolation $\Longrightarrow$ conditional lower bounds:

- let $\langle A_0, A_1\rangle$ disjoint NP-pair not separable in P/poly
- sequence of formulas $\varphi_{n,0}, \varphi_{n,1}$ s.t. for $w \in \{0,1\}^n$, $w \in A_i \iff \exists \vec{q}^i\, \varphi_{n,i}(w,\vec{q}^i)$
- then: $\neg\varphi_{n,0}(\vec{p},\vec{q}^0) \vee \neg\varphi_{n,1}(\vec{p},\vec{q}^1)$ tautologies, have no polynomial-size P-proofs

Variant: monotone feasible interpolation
$\Longrightarrow$ unconditional exponential lower bounds

Modal logics

Normal modal logics

- language of **CPC** $+$ unary connective $\Box$
- rules of **CPC**, necessitation (Nec) $\varphi \,/\, \Box\varphi$, the schema

$$\Box(\varphi \to \psi) \to (\Box\varphi \to \Box\psi) \tag{K}$$

  $+$ additional axiom schemata

- this talk: mostly transitive logics, i.e., including

$$\Box\varphi \to \Box\Box\varphi \tag{4}$$

Modal proof systems

L finitely axiomatizable normal modal logic

Frege system L-F

- finite set R of schematic rules s.t. $\Gamma \vdash_R \varphi \iff \Gamma \vdash_L \varphi$
- the choice of R does not matter (up to p-equivalence)
  canonical choice: MP, Nec, axiom schemata
- p-equivalent to sequent calculi (for logics that have them)

Extended Frege L-EF, substitution Frege L-SF

- L-$EF \leq_p L$-SF, but in general not equivalent:
  L unbounded branching $\implies$
  L-SF exponential speedup over L-EF (unconditionally!)

[more later]

Feasible disjunction property

L has the disjunction property (DP) if

$$\vdash_L \Box\varphi_0 \vee \Box\varphi_1 \implies \vdash_L \varphi_0 \text{ or } \vdash_L \varphi_1$$

DP as a computational task (P proof system for L):
given a P-proof of $\Box\varphi_0 \vee \Box\varphi_1$, pinpoint $i \in \{0, 1\}$ s.t. $\vdash_L \varphi_i$

If computable in polynomial time: P has feasible DP

If we can compute a P-proof of φ_i: constructive feasible DP

NB: L has DP $\implies$ L-$\textsc{Taut}$ is PSPACE-hard
(**K**, **K4**, **S4**, **GL**, **Grz**, . . . : PSPACE-complete)

PSPACE $\neq$ NP $\implies$ superpolynomial lower bounds
on all proof systems for L

Prototypical example

Theorem

$\mathbf{K}$-F has constructive feasible DP

Proof: Given a proof $\pi = \{\theta_0, \dots, \theta_z\}$ of $\bigvee_{i<k} \Box\varphi_i$, let Π be the closure of π under MP.

Define a Boolean assignment to modal formulas s.t.

$$v(\Box\varphi) = 1 \iff \varphi \in \Pi.$$

By induction on $j \leq z$, prove $v(\theta_j) = 1$ (easy).

Thus, $v\left(\bigvee_{i<k} \Box\varphi_i\right) = 1$, which means $\varphi_i \in \Pi$ for some $i < k$. Π is a valid proof.

Feasible DP and lower bounds

Lemma

If there exists a disjoint NP-pair not separable in P/poly, and if L-F or L-EF has feasible DP, then it is not polynomially bounded

If

$$\varphi(\vec{p},\vec{q}) \lor \psi(\vec{p},\vec{r})$$

is a classical tautology without a small interpolant, then

$$\bigwedge_i (\Box p_i \lor \Box\neg p_i) \to \Box\varphi(\vec{p},\vec{q}) \lor \Box\psi(\vec{p},\vec{r})$$

is an L-tautology without a short proof

Hrubeš monotone interpolation

If

$$\alpha(\vec{p}, \vec{q}) \to \beta(\vec{p}, \vec{r}) \tag{1}$$

is a classical tautology with α monotone in $\vec{p}$, then

$$\alpha(\Box\vec{p}, \vec{q}) \to \Box\beta(\vec{p}, \vec{r}) \tag{2}$$

is a **K**-tautology

Common proofs of feasible DP generalize to:
if (2) has a short proof, then (1) has a small monotone interpolant $C(\vec{p})$

$$\alpha(\vec{p}, \vec{q}) \to C(\vec{p}), \qquad C(\vec{p}) \to \beta(\vec{p}, \vec{r})$$

$\Longrightarrow$ unconditional exponential lower bounds

EF versus SF

- L-$EF \le_p L$-SF; in fact, L-$EF \equiv_p$ tree-like L-SF
- L-$EF \equiv_p L$-SF if $L \supseteq$ **KB** or if L tabular

For transitive L, a partial dichotomy:

- L-$EF \equiv_p L$-$SF \equiv_p$ **CPC**-EF for many L of bounded width:
  - L bounded depth and width, or
  - $L = \mathbf{K4BW}_k, \mathbf{S4BW}_k, \mathbf{GLBW}_k, \mathbf{K4GrzBW}_k, \mathbf{S4GrzBW}_k$
  - L cofinal subframe logic (restricted class of tautologies)

  proof-theoretic analogues of poly-size model property
- L-SF exponential speedup over L-EF
  for L of unbounded branching
  - based on Hrubeš-style monotone interpolation

Frame measures

Invariants of (Kripke or general) transitive frames:

- depth $=$ maximal length of strict chains
- width $=$ maximal size of antichains in rooted subframes
- branching $=$ maximal number of immediate successor clusters of any point

A logic L has depth (width) $\le k$
$\iff$ all descriptive L-frames have depth (width) $\le k$
$\iff$ $L \supseteq \mathbf{K4BD}_k$ ($\mathbf{K4BW}_k$)

L has branching $\le k \iff L \supseteq \mathbf{K4BB}_k$
The expected semantics only for finite frames:

If L has the finite model property, then
L branching $\le k \iff$ all finite L-frames have branching $\le k$

EF versus *SF* (cont'd)

Examples:

- **S5**, **S4**.3, **K4**.3, **GL**.3 have width 1
  - L-$EF \equiv_p L$-SF
  - lower bounds on L-EF as hard to get as for **CPC**-EF
- **K4**, **S4**, **GL**, **S4**.2, **S4BD**$_2$ have unbounded branching
  - exponential separation of L-EF from L-SF

Question

What about logics of bounded branching but unbounded width?

Basic logics of bounded branching

Consider $L = \mathbf{K4BB}_k$ $(k \geq 2) \pm \mathbf{S4}, \mathbf{GL}, \mathbf{Grz}$

$$\Box\Big[\bigvee_{i=0}^{k}\Box\Big(\boxdot\varphi_i \to \bigvee_{j\neq i}\boxdot\varphi_j\Big) \to \bigvee_{i=0}^{k}\boxdot\varphi_i\Big] \to \bigvee_{i=0}^{k}\Box\bigvee_{j\neq i}\boxdot\varphi_j \qquad (\mathrm{BB}_k)$$

- have DP
- PSPACE-complete, need exponential-size models
  - the above strategies for proving $L\text{-}EF \equiv_p L\text{-}SF \equiv_p \mathbf{CPC}\text{-}EF$ are out of question
- Does L-EF have feasible DP?
- Can we prove unconditional lower bounds on L-EF?
- Does L-SF have exponential speedup over L-EF?

Proof complexity of $\mathbf{K4BB}_k$ and friends

Not as clear-cut as before:

- L-EF likely does not have feasible DP
  - the DP problem for L-EF equivalent to a special case of interpolation for **CPC**-EF
  - in particular: reduces to a disjoint NP-pair (trivial upper bound: PSPACE)
- L-SF has conditionally speedup over L-EF (likely exponential)
  - assuming PSPACE $\neq$ NP, or
  - assuming the **CPC**-EF interpolation pair is not a complete disjoint NP-pair

More generally, applies to $L = L_0 \oplus \mathbf{BB}_k$, L_0 an extensible logic

- key tool: feasibility of extension rules in L_0-EF

Extensible logics

Common way to show that $L \supseteq \mathbf{K4}$ has DP:

- if $\nvdash_L \varphi_i$ for $i < n$, fix rooted L-frames F_i that invalidate φ_i
- combine them to a single L-frame whose root then invalidates $\bigvee_{i<n} \Box\varphi_i$
- specifically: take the disjoint union $\sum_{i<n} F_i$, attach a new root (reflexive $\circ$ or irreflexive $\bullet$) notation: $\left(\sum_{i<n} F_i\right)^{\circ}$, $\left(\sum_{i<n} F_i\right)^{\bullet}$

L is $*$-extensible ($* \in \{\circ, \bullet\}$) if the class of descriptive L-frames closed under the formation of $\left(\sum_{i<n} F_i\right)^{*}$

Examples:

- **K4**, **GL**, **K4Grz** are $\bullet$-extensible
- **K4**, **S4**, **K4Grz**, **S4Grz** are $\circ$-extensible

Extension rules

The $\left(\sum_{i<n} F_i\right)^*$ construction implies not just DP, but admissibility of more general extension rules

$$\frac{\bigwedge_{j<m} B^*(\chi_j) \to \bigvee_{i<n} \Box\varphi_i}{\bigwedge_{j<m} \boxdot\chi_j \to \varphi_0, \dots, \bigwedge_{j<m} \boxdot\chi_j \to \varphi_{n-1}} \qquad (\mathrm{Ext}^*)$$

where $B^\bullet(\varphi) = \Box\varphi$, $B^\circ(\varphi) = (\varphi \leftrightarrow \Box\varphi)$

Lemma

L is $*$-extensible $\iff$ Ext^* is L-admissible

Feasibility of extension rules

Theorem

L is $*$-extensible ($* \in \{\bullet, \circ\}$) $\implies$
Ext^* is constructibly feasible for L-EF

- L can be axiomatized by axioms of a special form
- adapt the "Boolean assignment" argument for feasible DP

DP for $\mathbf{BB}_k$ (basic idea)

$L = L_0 \oplus \mathbf{BB}_k$, L_0 $*$-extensible

$L\text{-}EF \vdash \bigvee_{u<k} \Box\varphi_u \implies L_0\text{-}EF \vdash \bigwedge_{l<m} \boxdot A_l \to \bigvee_{u<k} \Box\varphi_u$:

$$A_l = \Box\Big[\bigvee_{i\le k}\Box\Big(\boxdot\psi_{l,i} \to \bigvee_{j\ne i}\boxdot\psi_{l,j}\Big) \to \bigvee_{i\le k}\boxdot\psi_{l,i}\Big] \to \bigvee_{i\le k}\Box\bigvee_{j\ne i}\boxdot\psi_{l,j}$$

For all $\sigma \in [k+1]^m$, get L_0-EF proofs of

$$\bigwedge_{l<m} B^*\Big(\bigvee_{i\le k}\boxdot\psi_{l,i} \to \bigvee_{j\ne\sigma(l)}\boxdot\psi_{l,j}\Big) \to \bigvee_{u<k}\Box\varphi_u$$

Feasible Ext* $\implies$ L_0-EF proofs of

$$\bigwedge_{l<m}\boxdot\Big(\bigvee_{i\le k}\boxdot\psi_{l,i} \to \bigvee_{j\ne\sigma(l)}\boxdot\psi_{l,j}\Big) \to \varphi_u$$

for some $u \in [k]$

DP for BB_k (basic idea, cont'd)

Combinatorial principle

$\forall\sigma \in [k+1]^m \, \exists u \in [k] \, R(\sigma, u) \implies$

$\exists u \in [k] \, \forall\tau \in [k+1]^m \, \exists\sigma \in [k+1]^m \, \big(\sigma \# \tau \wedge R(\sigma, u)\big)$,

where $\sigma \# \tau$ denotes $\forall l < m \, \sigma(l) \neq \tau(l)$

$\implies$ there is $u < k$ s.t. $\forall\tau \in [k+1]^m$, have L_0-EF proofs of

$$\bigwedge_l \boxdot\big(\bigvee_i \boxdot\psi_{l,i} \to \boxdot\psi_{l,\tau(l)}\big) \to \varphi_u$$

Better argument $\implies$ L-EF proofs of

$$\bigwedge_l \big(\bigvee_i \boxdot\psi_{l,i} \to \boxdot\psi_{l,\tau(l)}\big) \to \varphi_u$$

$\implies$ φ_u is an L-tautology

References

- S. Buss, P. Pudlák: On the computational content of intuitionistic propositional proofs, Ann. Pure Appl. Logic 109 (2001), 49–64
- P. Hrubeš: Lower bounds for modal logics, J. Symb. Logic 72 (2007), 941–958
- P. Hrubeš: On lengths of proofs in non-classical logics, Ann. Pure Appl. Logic 157 (2009), 194–205
- E. J.: Frege systems for extensible modal logics, Ann. Pure Appl. Logic 142 (2006), 366–379
- E. J.: Substitution Frege and extended Frege proof systems in non-classical logics, Ann. Pure Appl. Logic 159 (2009), 1–48
- E. J.: On the proof complexity of logics of bounded branching, 2020, arXiv:2004.11282 [cs.LO]
- J. Krajíček: Proof complexity, Cambridge University Press, 2019