Disjunction-free disjunction property

Emil Jeřábek

Institute of Mathematics
Czech Academy of Sciences
jerabek@math.cas.cz
https://users.math.cas.cz/~jerabek/

Computability in Europe, Batumi
Shota Rustaveli State University, 27 July 2023

Outline

1. **Classical proof complexity**
2. **Non-classical proof complexity**
3. **Lower bound for implicational logic**

Classical proof complexity

1. Classical proof complexity
2. Non-classical proof complexity
3. Lower bound for implicational logic

Propositional proof systems

Proof system (pps): relation $P \subseteq \text{Form} \times \Sigma^*$ s.t.

- P is decidable in polynomial time
- φ is a tautology $\iff \exists \pi\, P(\varphi, \pi)$

Main measure: length (=size) of proofs

- P polynomially bounded if all tautologies φ have P-proofs of size $\leq |\varphi|^c$
- P p-simulates Q ($P \geq_p Q$):
  polynomial-time translation of Q-proofs to P-proofs
- P and Q are p-equivalent ($P \equiv_p Q$): $P \geq_p Q$ & $Q \geq_p P$

Theorem (Cook, Reckhow '79):
NP = **coNP** $\iff \exists$ polynomially bounded pps

Frege (aka Hilbert-style) systems

R: finite set of schematic Frege rules $\alpha_1, \dots, \alpha_k \vdash \alpha_0$

R-derivation of φ from Γ: $\varphi_0, \dots, \varphi_t = \varphi$ where each φ_i derived from φ_j, $j < i$ by an instance of an R-rule, or $\varphi_i \in \Gamma$

If $\Gamma \vdash_R \varphi \iff \Gamma \vDash \varphi$: Frege system F_R

- typically: modus ponens + axiom schemata
- all Frege systems p-equivalent (Reckhow '76)
  $\implies$ write $\mathrm{F} = \mathrm{F}_R$
- p-equivalent to tree-like Frege F^* (Krajíček '94)
- p-equivalent to sequent calculus and natural deduction (Reckhow '76)
- known lower bounds: number of lines $\Omega(n)$, size $\Omega(n^2)$ (Krajíček '95)

Feasible interpolation

General lower bound method for weak pps (Krajíček '97):

P has feasible interpolation if for every P-proof Π of

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

there exists a Boolean circuit $C(\vec{p})$, $|C| \le |\Pi|^c$, s.t.

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

Feasible interpolation

General lower bound method for weak pps (Krajíček '97):

P has feasible interpolation if for every P-proof Π of

$$\alpha(\vec{p},\vec{q}) \lor \beta(\vec{p},\vec{r})$$

there exists a Boolean circuit $C(\vec{p})$, $|C| \le |\Pi|^c$, s.t.

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

Theorem: If P has f.i., and $\exists$ a disjoint **NP**-pair not separable by polynomial-size circuits, then P is not polynomially bounded

Circuit lower bounds

Lower bounds on the size of general circuits:

- random functions $\{0,1\}^n \to \{0,1\}$: size $\gtrsim 2^n/n$ whp
- explicit functions: size $\geq 5n$ or so
  $\implies$ f.i. only yields conditional lower bounds

Monotone circuits ($\wedge$, $\vee$, 0, 1):

- Razborov '85: superpolynomial lower bound for Clique
- Alon–Boppana '87: improved to exponential lower bound
- also applies to the Clique–Colouring **NP**-pair (Tardos '87)

Theorem (Alon–Boppana '87):
For $k = \lfloor \sqrt{n} \rfloor$, any monotone circuit separating k-colourable n-vertex graphs from graphs containing a $(k+1)$-clique has size $n^{\Omega(n^{1/4})}$

Monotone feasible interpolation

P has monotone feasible interpolation if for every P-proof Π of

$$\alpha(\vec{p},\vec{q}) \lor \beta(\vec{p},\vec{r})$$

where $\vec{p}$ only occur positively in α,
there exists a monotone circuit $C(\vec{p})$, $|C| \le |\Pi|^c$, s.t.

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

Theorem: If P has m.f.i. then P is not polynomially bounded

Example:
Resolution has f.i. and m.f.i.
Frege likely does not

Non-classical proof complexity

Non-classical Frege systems

L finitely axiomatizable propositional logic $\Longrightarrow$ Frege system L-F

Unconditional exponential lower bounds for many logics L:

- Hrubeš '07,'09: some modal logics, intuitionistic logic (Frege, Extended Frege)
- J. '09: extensions of K4 or IPC with unbounded branching
- Jalali '21: extensions of FL included in . . .

Further strengthening:

- exponential separation between Extended Frege and Substitution Frege (J. '09)
- purely implicational tautologies (J. '17)

Feasible disjunction property

P proof system for $L \supseteq \mathrm{IPC}$:

P has the feasible disjunction property if given a P-proof of $\varphi_0 \lor \varphi_1$, we can compute in polynomial time $i \in \{0, 1\}$ such that $\vdash_L \varphi_i$

Modal logics: the same with $\Box\varphi_0 \lor \Box\varphi_1$

Example: IPC-F has f.d.p.

(Buss–Pudlák '01) f.d.p. can serve the role of f.i.
$\implies$ conditional lower bounds

(Hrubeš '07) analogue of monotone f.i.
$\implies$ unconditional lower bounds

f.d.p. serving as f.i.

$P \geq_p$ IPC-F closed under substitution of $0, 1$:

- $\alpha(\vec{p}, \vec{q}) \lor \beta(\vec{p}, \vec{r})$ classical tautology $\implies$ IPC proves

$$(*) \qquad \bigwedge_{i<n} (p_i \lor \neg p_i) \to \neg\neg\alpha(\vec{p}, \vec{q}) \lor \neg\neg\beta(\vec{p}, \vec{r})$$

- if P has f.d.p. and $(*)$ has a short P-proof: small circuit C such that for all $\vec{a} \in \{0, 1\}^n$,

$$C(\vec{a}) = 1 \implies \vdash \neg\neg\alpha(\vec{a}, \vec{q})$$
$$C(\vec{a}) = 0 \implies \vdash \neg\neg\beta(\vec{a}, \vec{r})$$

f.d.p. serving as f.i.

$P \geq_p$ IPC-F closed under substitution of $0, 1$:

- $\alpha(\vec{p}, \vec{q}) \vee \beta(\vec{p}, \vec{r})$ classical tautology $\implies$ IPC proves

$$(*) \qquad \bigwedge_{i<n}(p_i \vee \neg p_i) \to \neg\neg\alpha(\vec{p}, \vec{q}) \vee \neg\neg\beta(\vec{p}, \vec{r})$$

- if P has f.d.p. and $(*)$ has a short P-proof:
  small circuit C such that

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

In a galaxy far, far away

Persistent claims by L. Gordeev and E. H. Haeusler (2016–):

- implicational IPC tautologies have polynomial-size proofs in dag-like natural deduction
- **NP** = **PSPACE**
- published ('19,'20), some people seem to take it seriously

Flatly contradicts known lower bounds, but this requires a complex argument, hard to track down by non-specialists:

- IPC-F lower bounds (Hrubeš '07)
- monotone circuit lower bounds (Alon–Boppana '87)
- reduction to implicational logic (J. '17)
- simulation of natural deduction by Frege (idea Reckhow '76, Cook–Reckhow '79, but for a different system)

$\Longrightarrow$ desire for something simpler/more direct

Lower bound for implicational logic

Intuitionistic/minimal implicational logic

Language: $\to$, atoms $p_0, p_1, p_2, \dots$

the set of formulas: Form

Notation: $\varphi \to \psi \to \chi \to \omega = (\varphi \to (\psi \to (\chi \to \omega)))$

Frege system $F_{\to}$:

$$\vdash (\varphi \to \psi \to \chi) \to (\varphi \to \psi) \to (\varphi \to \chi)$$

$$\vdash \varphi \to \psi \to \varphi$$

$\varphi, \varphi \to \psi \vdash \psi$

Sequent calculus $LJ_{\to}$: structural rules (incl. cut) +

$$\frac{}{\varphi \Longrightarrow \varphi} \qquad \frac{\Gamma \Longrightarrow \varphi \quad \Gamma, \psi \Longrightarrow \alpha}{\Gamma, \varphi \to \psi \Longrightarrow \alpha} \qquad \frac{\Gamma, \varphi \Longrightarrow \psi}{\Gamma \Longrightarrow \varphi \to \psi}$$

Natural deduction

Prawitz-style tree-like natural deduction:

$$[\varphi] \longleftarrow \text{discharged}$$

$$\vdots$$

$$(\to\mathrm{E})\ \frac{\varphi \quad \varphi\to\psi}{\psi} \qquad\qquad (\to\mathrm{I})\ \frac{\psi}{\varphi\to\psi}$$

- every leaf of the proof tree must be discharged

Gordeev & Haeusler dag-like natural deduction $\mathrm{NM}_{\to}$:

- every leaf of the proof dag must be discharged on every path to the root
- checkable in polynomial-time: inductively compute for each node $v \in V$ the set

$$A_v = \{\gamma_u : u \text{ leaf, undischarged on some path to } v\}$$

Notation: $\langle V, E\rangle$ underlying dag, γ_v = formula label of node v

Efficient Kleene's slash

For $P \subseteq \mathrm{Form}$: a P-slash is a unary predicate $|\varphi$ on Form s.t.

$$|(\varphi \to \psi) \iff (\underbrace{|\varphi \text{ and } \varphi \in P}_{\|\varphi} \implies |\psi)$$

- free to choose $|p$ for atoms p
- Kleene's original $\Gamma \mid \varphi$ has $P = \{\varphi : \Gamma \vdash \varphi\}$, we take for P an efficiently computable finite set

For a proof Π: P is Π-closed if $\forall v \, (A_v \subseteq P \implies \gamma_v \in P)$

Lemma: Π proof of φ, P is Π-closed, $|$ is a P-slash $\implies |\varphi$

- by induction on the length of the proof

Constructibility of Π-closure

$\mathrm{cl}_\Pi(X)$ = smallest Π-closed set $P \supseteq X$

Observation: $\varphi \in \mathrm{cl}_\Pi(X) \implies X \vdash \varphi$

$\mathrm{cl}_\Pi(X)$ is computable in polynomial time, moreover:

Lemma: Π proof, $F = \{\varphi_i : i < n\} \subseteq \mathrm{Form}$, $\varphi \in \mathrm{Form}$
$\implies \exists$ monotone circuit C of size $|\Pi|^3$ s.t.

$$C(x_0, \dots, x_{n-1}) = 1 \iff \varphi \in \mathrm{cl}_\Pi(\{\varphi_i : x_i = 1\})$$

- describe inductive construction of closure
- only involves formulas from Π
- terminates in $|\Pi|$ steps

Feasible disjunction property

Theorem: Given a proof Π of

$$\varphi = \bigl(\alpha_0(\vec{p}) \to u\bigr) \to \bigl(\alpha_1(\vec{p}) \to u\bigr) \to u,$$

we can compute in polynomial time $i \in \{0,1\}$ s.t. $\vdash \alpha_i$

Proof: $P = \mathrm{cl}_\Pi(\alpha_0 \to u, \alpha_1 \to u)$, $|$ P-slash s.t. $\nmid u$

We have $|\varphi \implies \nparallel(\alpha_0 \to u)$ or $\nparallel(\alpha_1 \to u)$

$\nparallel(\alpha_i \to u) \implies \nmid(\alpha_i \to u) \implies \|\alpha_i \implies \alpha_i \in P$

We can compute i s.t. $\alpha_i \in P$

Then: $\alpha_0 \to u, \alpha_1 \to u \vdash \alpha_i$

Substitute $\top$ for $u \implies$ get $\vdash \alpha_i$

Monotone feasible interpolation

Theorem: Given a proof Π of

$$
\begin{aligned}
&\big((p_0 \to u) \to (p_0' \to u) \to u\big) \\
&\quad \to \big((p_1 \to u) \to (p_1' \to u) \to u\big) \\
&\qquad \to \big((p_2 \to u) \to (p_2' \to u) \to u\big) \\
&\qquad\qquad\qquad\qquad \ddots \\
&\qquad\qquad \to \big((p_n \to u) \to (p_n' \to u) \to u\big) \\
&\qquad\qquad\qquad \to \big(\alpha(\vec{p},\vec{q}) \to u\big) \to \big(\beta(\vec{p}\,',\vec{r}) \to u\big) \to u,
\end{aligned}
$$

there is a monotone circuit C of size $|\Pi|^3$ such that

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

The lower bound

τ_n: intuitionistic implicational tautologies of size $O(n^3)$ expressing disjointness of the Clique–Colouring **NP** pair

Monotone feasible interpolation $\Longrightarrow$

Lemma: If τ_n has a proof of size s, then there is a monotone circuit of size s^3 separating the Clique–Colouring pair

Alon–Boppana bound $\Longrightarrow$

Theorem: Any proof of τ_n has size $n^{\Omega(n^{1/4})}$

Corollary: There are infinitely many intuitionistic implicational tautologies φ that require proofs of size $|\varphi|^{\Omega(|\varphi|^{1/12})}$

Other calculi

The argument adapts to $\mathrm{F}_{\to}$ or $\mathrm{LJ}_{\to}$:

- adjust the definition of Π-closed sets

Actually: $\mathrm{F}_{\to} \equiv_p \mathrm{LJ}_{\to} \equiv_p \mathrm{NM}_{\to} \equiv_p \underbrace{\mathrm{F}^*_{\to} \equiv_p \mathrm{LJ}^*_{\to} \equiv_p \mathrm{NM}^*_{\to}}_{\text{tree-like versions}}$

- $\mathrm{F}_{\to} \equiv_p \mathrm{LJ}_{\to} \equiv_p \mathrm{NM}_{\to}$ go back to Reckhow '76
- $\mathrm{F}_{\to} \equiv_p \mathrm{F}^*_{\to}$ due to Krajíček, implicational version J. '17

Further extensions of the lower bound (as in J. '09, J. '17):

- full language of IPC
- superintuitionistic logics $\mathrm{IPC} \subseteq L \subseteq \mathrm{BD}_2$
- exponential separation between Extended Frege and Substitution Frege

References

- N. Alon, R. B. Boppana: The monotone circuit complexity of Boolean functions, Combinatorica 7 (1987), 1–22
- 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
- L. Gordeev, E. H. Haeusler: Proof compression and NP versus PSPACE, Studia Logica 107 (2019), 53–83
- ________: Proof compression and NP versus PSPACE II, Bull. Sect. Logic Univ. Łódź 49 (2020), 213–230
- ________: Proof compression and NP versus PSPACE II: addendum, Bull. Sect. Logic Univ. Łódź 51 (2022), 197–205
- 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
- R. Jalali: Proof complexity of substructural logics, APAL 172 (2021), art. 102972, 31 pp

References (cont'd)

- E. J.: Substitution Frege and extended Frege proof systems in non-classical logics, APAL 159 (2009), 1–48
- ________: Proof complexity of intuitionistic implicational formulas, APAL 168 (2017), 150–190
- ________: A simplified lower bound for implicational logic, 2023, 31 pp, arXiv:2303.15090 [cs.LO]
- S. Jukna: Boolean function complexity: Advances and frontiers, Springer, 2012, xvi+620 pp
- J. Krajíček: Bounded arithmetic, propositional logic, and complexity theory, Cambridge Univ. Press, 1995, xiv+343 pp
- J. Krajíček: Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic, JSL 62 (1997), 457–486
- ________: Proof complexity, Cambridge Univ. Press, 2019, 530 pp
- A. A. Razborov: Lower bounds on the monotone complexity of some Boolean functions, Math. USSR, Doklady 31 (1985), 354–357
- R. A. Reckhow: On the lengths of proofs in the propositional calculus, Ph.D. thesis, Univ. Toronto, 1976
- É. Tardos: The gap between monotone and non-monotone circuit complexity is exponential, Combinatorica 7 (1987), 141–142