A simplified lower bound on intuitionistic implicational proofs

Emil Jeřábek

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

Logic Seminar
Institute of Mathematics, Prague, 15 May 2023

Outline

1. Non-classical Frege lower bounds
2. Intuitionistic implicational logic
3. Lower bound for implicational logic
4. Two notes on classical Frege

Non-classical Frege lower bounds

Overview of lower bounds

Classical Frege (or EF): number of lines $\Omega(n)$, size $\Omega(n^2)$

Nonclassical Frege systems L-F:
exponential lower bounds for many logics L

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

Further strengthening:

- separation between EF and SF (J. '09)
- purely implicational tautologies (J. '17)

Based on variants of feasible disjunction property

Feasible disjunction property

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

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

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

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

Lower bounds based on f.d.p.

F.d.p. can serve the role of feasible interpolation (Buss–Pudlák '01)

Proof system $P \geq_p$ 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 Π: circuit C, $|C| = |\Pi|^{O(1)}$, such that for all $\vec{a} \in \{0, 1\}^n$,

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

Lower bounds based on f.d.p.

F.d.p. can serve the role of feasible interpolation (Buss–Pudlák '01)

Proof system $P \geq_p$ 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 Π: circuit C, $|C| = |\Pi|^{O(1)}$, such that

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

$\implies$ conditional lower bounds (disjoint **NP**-pairs inseparable in **P**/**poly**)

Monotone version

An analogue of monotone f.i. (Hrubeš '07)

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

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

- for $P = \text{IPC-F}$ and other proof systems, f.d.p. extends to: P-proof Π of $(**) \implies$ monotone circuit C, $|C| = |\Pi|^{O(1)}$,

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

$\implies$ unconditional lower bounds
(exponential monotone circuit lower bounds)

Exponential lower bounds

In the realm of extensions of IPC-F:

(Hrubeš '07,'09)

- exponential lower bounds for IPC-F
- the bounds are on the number of lines
  $\Longrightarrow$ also apply to Extended Frege

(J. '09)

- generalize to L-EF for all logics $L \supseteq$ IPC of unbounded branching (i.o.w., $L \subseteq \mathrm{BD}_2$ or $L \subseteq \mathrm{KC} + \mathrm{BD}_3$)
- exponential speed-up of IPC Substitution Frege over L-EF

(J. '17)

- the bounds hold for purely implicational tautologies . . .

Implicational translation

(J. '17) L an extension of IPC by implicational axioms
$\implies$ given φ, construct in poly-time

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

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

Also:

- variants for arbitrary $L \supseteq$ IPC under restrictions on φ
- converse elimination of connectives from proofs:
  e.g., $\mathrm{IPC}_{\to}$-EF $\equiv_p$ IPC-EF for implicational tautologies

In a galaxy far, far away

Persistent claims by L. Gordeev and E. H. Haeusler:

- implicational IPC tautologies have polynomial-size proofs in dag-like natural deduction
- **NP** $=$ **PSPACE**
- published, some people seem to take them 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)
- reduction to implicational logic (J. '17)
- monotone circuit lower bounds (Alon–Boppana '87)
- simulation of natural deduction by Frege (idea Reckhow '76, Cook–Reckhow '79, but for a different system)

$\Longrightarrow$ desire for something simpler/more direct

Intuitionistic implicational logic

Intuitionistic/minimal implicational logic

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

the set of formulas: Form

Notation: $(\varphi_{n-1} \to (\cdots \to (\varphi_1 \to (\varphi_0 \to \psi))\cdots))$

$$= \varphi_{n-1} \to \cdots \to \varphi_1 \to \varphi_0 \to \psi$$

$$= \langle \varphi_i \rangle_{i<n} \to \psi$$

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:

$$
\begin{array}{c}
\\ \\ \\
(\to\mathsf{E})\ \dfrac{\varphi \quad \varphi\to\psi}{\psi}
\end{array}
\qquad\qquad
\begin{array}{c}
[\varphi] \quad \longleftarrow \text{ discharged} \\
\vdots \\
(\to\mathsf{I})\ \dfrac{\psi}{\varphi\to\psi}
\end{array}
$$

- every leaf of the proof tree must be discharged

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

- every leaf of the proof dag must be discharged on every path to the root
- how to check in polynomial-time?

Verification of $NM_{\to}$-proofs

$NM_{\to}$-derivation $\Pi = \langle V, E, \gamma \rangle$ with root ϱ:

- $\langle V, E \rangle$ underlying dag
- $\gamma = \langle \gamma_v : v \in V \rangle$ formula labels

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

Compute A_v inductively in polynomial time:

$$A_v = \begin{cases} \{\gamma_v\} & v \text{ is a leaf} \\ A_{u_0} \cup A_{u_1} & v \text{ is an } ({\to}\mathrm{E})\text{-node with premises } u_0, u_1 \\ A_u \smallsetminus \{\alpha\} & v \text{ is an } ({\to}\mathrm{I})\text{-node with premise } u,\ \gamma_v = \alpha \to \beta \end{cases}$$

Π is a sound $NM_{\to}$-proof of γ_ϱ iff $A_\varrho = \varnothing$

Equivalence of implicational calculi

For context:

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

- $\mathrm{F} \equiv_p \mathrm{LJ} \equiv_p \mathrm{ND}$ go back to Reckhow '76, Cook–Reckhow '79
- $\mathrm{F} \equiv_p \mathrm{F}^*$ due to Krajíček, implicational version J. '17
- for $\mathrm{IPC}_{\to}$, proved in detail in J. '23 with improved bounds
- we will not use this, but prove the lower bounds directly for all three proof systems

Lower bound for implicational logic

Efficient Kleene's slash

Let $P \subseteq \mathrm{Form}$

P-slash: a unary predicate $|\varphi$ on Form s.t.

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

NB: free to choose $|p$ for atoms p

Observe: $|(\Gamma \to \psi) \iff \nparallel\varphi$ for some $\varphi \in \Gamma$, or $|\psi$

Kleene's original $\Gamma \mid \varphi$ has $P = \{\varphi : \Gamma \vdash \varphi\}$

We will take for P an efficiently computable finite set (suitable closure of a given proof)

Soundness of slash

Proof $\Pi \implies P \subseteq \mathrm{Form}$ is Π-closed if

- $F_\to$: $\Pi \subseteq P$,
  $\varphi, \varphi \to \psi \in P \implies \psi \in P$ for each φ, ψ
- $LJ_\to$: $\Gamma \subseteq P \implies \varphi \in P$ for each sequent $\Gamma \Longrightarrow \varphi$ in Π,
  $\varphi, \varphi \to \psi \in P \implies \psi \in P$ for each φ, ψ
- $NM_\to$: $A_v \subseteq P \implies \gamma_v \in P$ for each v

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

- by induction on the length of the proof (essentially)

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, $\{\varphi_i : i < n\} \subseteq \mathrm{Form}$
$\implies \exists$ monotone circuit C of size $\bigl(|\Pi| + \sum_i |\varphi_i|\bigr)^{O(1)}$ s.t.

$$C(x_0, \dots, x_{n-1}) = 1 \iff \varphi_0 \in \mathrm{cl}_\Pi(\{\varphi_i : x_i = 1\})$$

- only polynomially many formulas involved
- describe inductive construction of closure
- terminates after polynomially many iterations

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 $u \implies \vdash \alpha_i$

Monotone feasible interpolation

Theorem: Given a proof Π of

$$\Big\langle (p_i \to u) \to (p'_i \to u) \to u \Big\rangle_{i<n} \\ \to \big(\alpha(\vec{p}, \vec{q}) \to u\big) \to \big(\beta(\vec{p}\,', \vec{r}) \to u\big) \to u,$$

there is a monotone circuit C of size $|\Pi|^{O(1)}$ such that

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

Clique–Colouring disjoint NP pair

For a graph $G = \langle V, E\rangle$, the following cannot happen:

- G is k-colourable
- G contains a $(k+1)$-clique

For $V = [n]$, represent E by an $\binom{n}{2}$-tuple of Boolean variables

Fix $k = \lfloor \sqrt{n} \rfloor$

Theorem (Alon–Boppana '87):
Any monotone circuit separating k-colourable graphs from graphs containing a $(k+1)$-clique has size $n^{\Omega(n^{1/4})}$

Improves a superpolynomial lower bound by Razborov '85

Clique–Colouring tautologies

p_{ij} $(i, j < n)$: represent E
q_{il} $(i < n,\ l < k)$: colouring $V \to [k]$
r_{mi} $(m \le k,\ i < n)$: embedding $K_{k+1} \to G$

Classical tautologies:

$$\neg\Bigg[\bigg(\bigwedge_{i<n}\bigvee_{l<k} q_{il} \wedge \bigwedge_{\substack{i,j<n\\ l<k}}(q_{il} \wedge q_{jl} \to \neg p_{ij})\bigg) \wedge \bigg(\bigwedge_{m\le k}\bigvee_{i<n} r_{mi} \wedge \bigwedge_{\substack{l<m\le k\\ i,j<n}}(r_{li} \wedge r_{mj} \to p_{ij})\bigg)\Bigg]$$

Clique–Colouring tautologies

p_{ij} $(i, j < n)$: represent E
q_{il} $(i < n,\ l < k)$: colouring $V \to [k]$
r_{mi} $(m \le k,\ i < n)$: embedding $K_{k+1} \to G$

Classical tautologies:

$$\Big(\bigwedge_{i<n} \bigvee_{l<k} q_{il} \to \bigvee_{\substack{i,j<n \\ l<k}} (q_{il} \wedge q_{jl} \wedge p_{ij})\Big)$$
$$\vee \Big(\bigwedge_{m\le k} \bigvee_{i<n} r_{mi} \to \bigvee_{\substack{l<m\le k \\ i,j<n}} (r_{li} \wedge r_{mj} \wedge \neg p_{ij})\Big)$$

Clique–Colouring tautologies

p_{ij}, p'_{ij} $(i, j < n)$: represent E and its complement
q_{il} $(i < n,\ l < k)$: colouring $V \to [k]$
r_{mi} $(m \le k,\ i < n)$: embedding $K_{k+1} \to G$

Classical tautologies:

$$\bigwedge_{i,j<n}(p_{ij} \vee p'_{ij}) \to \Big[\Big(\bigwedge_{i<n}\bigvee_{l<k} q_{il} \to \bigvee_{\substack{i,j<n\\ l<k}}(q_{il} \wedge q_{jl} \wedge p_{ij})\Big) \vee \Big(\bigwedge_{m\le k}\bigvee_{i<n} r_{mi} \to \bigvee_{\substack{l<m\le k\\ i,j<n}}(r_{li} \wedge r_{mj} \wedge p'_{ij})\Big)\Big]$$

Clique–Colouring tautologies

p_{ij}, p'_{ij} $(i, j < n)$: represent E and its complement
q_{il} $(i < n,\ l < k)$: colouring $V \to [k]$
r_{mi} $(m \le k,\ i < n)$: embedding $K_{k+1} \to G$

Intuitionistic tautologies:

$$\bigwedge_{i,j<n} (p_{ij} \vee p'_{ij}) \to \Bigl[\Bigl(\bigwedge_{i<n} \bigvee_{l<k} q_{il} \to \bigvee_{\substack{i,j<n \\ l<k}} (q_{il} \wedge q_{jl} \wedge p_{ij}) \Bigr) \vee \Bigl(\bigwedge_{m \le k} \bigvee_{i<n} r_{mi} \to \bigvee_{\substack{l<m\le k \\ i,j<n}} (r_{li} \wedge r_{mj} \wedge p'_{ij}) \Bigr) \Bigr]$$

Clique–Colouring tautologies

p_{ij}, p'_{ij} $(i, j < n)$: represent E and its complement
q_{il} $(i < n,\ l < k)$: colouring $V \to [k]$
r_{mi} $(m \le k,\ i < n)$: embedding $K_{k+1} \to G$
u: auxiliary

Intuitionistic tautologies:

$$\Big[\Big(\bigwedge_{i<n}\bigvee_{l<k} q_{il} \to \bigvee_{\substack{i,j<n\\ l<k}} (q_{il} \wedge q_{jl} \wedge p_{ij})\Big) \to u\Big]$$
$$\to \Big[\Big(\bigwedge_{m\le k}\bigvee_{i<n} r_{mi} \to \bigvee_{\substack{l<m\le k\\ i,j<n}} (r_{li} \wedge r_{mj} \wedge p'_{ij})\Big) \to u\Big]$$
$$\to \bigwedge_{i,j<n} (p_{ij} \vee p'_{ij}) \to u$$

Clique–Colouring tautologies

p_{ij}, p'_{ij} $(i, j < n)$: represent E and its complement
q_{il} $(i < n,\ l < k)$: colouring $V \to [k]$
r_{mi} $(m \le k,\ i < n)$: embedding $K_{k+1} \to G$
u, v, w: auxiliary

Intuitionistic tautologies:

$$\Biggl[\biggl(\Bigl(\bigvee_{\substack{i,j<n\\ l<k}} (q_{il} \wedge q_{jl} \wedge p_{ij}) \to v\Bigr) \to \bigwedge_{i<n} \bigvee_{l<k} q_{il} \to v\biggr) \to u\Biggr]$$

$$\to \Biggl[\biggl(\Bigl(\bigvee_{\substack{l<m\le k\\ i,j<n}} (r_{li} \wedge r_{mj} \wedge p'_{ij}) \to w\Bigr) \to \bigwedge_{m\le k} \bigvee_{i<n} r_{mi} \to w\biggr) \to u\Biggr]$$

$$\to \bigwedge_{i,j<n} (p_{ij} \vee p'_{ij}) \to u$$

Clique–Colouring tautologies

p_{ij}, p'_{ij} $(i, j < n)$: represent E and its complement
q_{il} $(i < n,\ l < k)$: colouring $V \to [k]$
r_{mi} $(m \le k,\ i < n)$: embedding $K_{k+1} \to G$
u, v, w: auxiliary

Intuitionistic implicational tautologies:

$$\tau_n = \big\langle (p_{ij} \to u) \to (p'_{ij} \to u) \to u \big\rangle_{i,j<n} \to (\alpha_n \to u) \to (\beta_n \to u) \to u$$

where

$$\alpha_n = \big\langle \langle q_{il} \to v \rangle_{l<k} \to v \big\rangle_{i<n} \to \langle q_{il} \to q_{jl} \to p_{ij} \to v \rangle_{\substack{i,j<n \\ l<k}} \to v$$

$$\beta_n = \big\langle \langle r_{mi} \to w \rangle_{i<n} \to w \big\rangle_{m\le k} \to \langle r_{li} \to r_{mj} \to p'_{ij} \to w \rangle_{\substack{l<m\le k \\ i,j<n}} \to w$$

The lower bound

Lemma: The formulas τ_n are intuitionistic implicational tautologies of size $O(n^2k^2) = O(n^3)$

Monotone feasible interpolation $\implies$

Lemma: If τ_n has a proof of size s, then there is a monotone circuit of size $s^{O(1)}$ separating the Clique–Colouring **NP** pair

Alon–Boppana bound $\implies$

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 $|\varphi|^{\Omega(|\varphi|^{1/12})}$

Extensions

With a bit more effort, the same argument yields almost the full strength of the lower bound from J. '17:

- full language of IPC
- logics of unbounded branching included in BD_2
  - $\{\to, \land, \lor\}$-fragments of logics of unbounded branching are all included in BD_2
  - fragments with $\neg$: not necessarily
    some only included in $\mathsf{KC} + \mathsf{BD}_3$, require extra argument
- exponential speedup of SF over EF
  - τ_n has poly-size $\mathsf{IPC}_{\to}$-SF proofs
    (using classical EF proofs of PHP)

The bound can be improved to $2^{\Omega(|\varphi|^{1/10}/(\log|\varphi|)^{1/5})}$

Two notes on classical Frege

Classical Frege systems

Consider arbitrary Frege systems F for CPC
(in fixed language: say, $\{\wedge, \vee, \neg, \top, \bot\}$)

- finitely many schematic Frege rules $\alpha_1, \dots, \alpha_c \vdash \alpha_0$
- implicationally sound and complete
- tree-like version F^*
- measures: size $s_F(\varphi)$, number of lines $k_F(\varphi)$

Theorems:

- (Reckhow '76) Any Frege systems F_0, F_1 are p-equivalent
- (Krajíček '9?) For any Frege system F, $F \equiv_p F^*$

Question: How efficient are these simulations in general?

Reckhow's theorem

p-simulation of F_0 by F_1:

- The argument in Reckhow '76 gives $k_{\mathsf{F}_1}(\varphi) = O(k_{\mathsf{F}_0}(\varphi))$, $s_{\mathsf{F}_1}(\varphi) = O(s_{\mathsf{F}_0}(\varphi)^2)$
- Krajíček '19 claims $O(s_{\mathsf{F}_0}(\varphi))$ without explanation
- Question: Does the bound $s_{\mathsf{F}_1}(\varphi) = O(s_{\mathsf{F}_0}(\varphi))$ hold?

Line-by-line simulation:

- substitution instances of an F_0-rule $\alpha_1, \dots, \alpha_c \vdash \alpha_0$ have F_1-derivations with $O(1)$ lines and linear size
- $\tilde{s}_{\mathsf{F}_1}(\varphi) = O(\tilde{s}_{\mathsf{F}_0}(\varphi))$ where $\tilde{s}(\varphi) \ge s(\varphi)$ is "inferential size"

Inferential size

Definition:

- inferential size of an instance $\sigma(\alpha_1), \dots, \sigma(\alpha_c) \vdash \sigma(\alpha_0)$ of a Frege rule is $\sum_i |\sigma(\alpha_i)|$
- inferential size of an F-proof is the sum of inferential sizes of all inferences
- $\tilde{s}_F(\varphi) =$ minimal inferential size of an F-proof of φ

Observation:

- tree-like proof of size s has inf. size $O(s)$
- proof with k lines and size (or: max. formula size) s has inf. size $O(sk) = O(s^2)$

Inferential size of Modus Ponens proofs

Lemma: F = Modus Ponens + axioms $\Longrightarrow$
a nonredundant F-proof with size s has inf. size $O(s)$

- axioms have total inf. size $O(s)$
- $\varphi, \varphi \to \psi \vdash \psi$ has inf. size $O(|\varphi \to \psi|)$,
  each $\varphi \to \psi$ can only be used once like this

More generally: This works if for each F-rule

$$\alpha_1(p_0, \dots, p_{t-1}), \dots, \alpha_c(p_0, \dots, p_{t-1}) \vdash \alpha_0(p_0, \dots, p_{t-1})$$

there is i such that all p_j variables occur in α_i

General case

Question: Is $\tilde{s}_F(\varphi) = O(s_F(\varphi))$ true for all Frege systems F?

Case in point:

(R) $$p \to q, q \to r \vdash p \to r$$

- the system (R) + axioms does satisfy $\tilde{s}_F(\varphi) = O(s_F(\varphi))$
  - chase a path in a directed graph
  - not a Frege system: cannot be implicationally complete
- (R) + (MP) + axioms?

Krajíček's theorem

Bounds claimed in Krajíček '19 for $\mathrm{F} \equiv_p \mathrm{F}^*$:

- $k = k_{\mathrm{F}}(\varphi)$, $s = s_{\mathrm{F}}(\varphi) \implies$
  $k_{\mathrm{F}^*}(\varphi) = O(k \log k)$, $s_{\mathrm{F}^*}(\varphi) = O(sk \log k) = O(s^2 \log s)$

Works for (MP) + axioms, but not for arbitrary F:

- A proof of φ_j from $\bigwedge_{i<n} \varphi_i$ with $O(\log n)$ steps?
  - proof of height $O(\log n)$
  - F^*-derivation of $\alpha \wedge \beta \vdash \alpha$ using the premise only once?

More generally: Works if there is an F^*-derivation of $p, p \to q \vdash q$ using each premise only once

- better bound in J. '23: $s_{\mathrm{F}^*}(\varphi) = O(\tilde{s}_{\mathrm{F}}(\varphi)(\log k)^2)$

Counterexample

Proposition: For each d, there is a Frege system F such that $k_{F^*}(\varphi) = \Omega(k_F(\varphi)^d)$ for all φ and $s_{F^*}(\varphi) = \Omega(s_F(\varphi)^d)$ for infinitely many φ

Proof: $\mathrm{F}_c = \text{axioms} + \underbrace{p, \dots, p}_{c}, \underbrace{p \to q, \dots, p \to q}_{c} \vdash q$

- dag-like $\mathrm{F}_c = \mathrm{F}_1$ (the standard Frege system)
- by induction on k: φ has F_c^*-proof with k lines $\implies$ F_1^*-proof of height $\log_c k$ $\implies$ $2^{\log_c k} = k^{1/\log c}$ lines
- this gives $k_{\mathrm{F}_c^*}(\varphi) \geq k_{\mathrm{F}_c}(\varphi)^{\log c}$
- for proof size: take φ s.t. $k_{\mathrm{F}_1}(\varphi) = \Omega(n)$, $s_{\mathrm{F}_1}(\varphi) = O(n^2)$ $\implies$ $s_{\mathrm{F}_c^*}(\varphi) \geq k_{\mathrm{F}_c^*}(\varphi) = \Omega(n^{\log c}) = \Omega(s_{\mathrm{F}_c}(\varphi)^{(\log c)/2})$

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

References (cont'd)

- R. Jalali: Proof complexity of substructural logics, APAL 172 (2021), art. 102972, 31 pp
- 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]
- 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