Proof complexity workshop, Canada
21.1.2020

Why are proof complexity lower bounds hard?

Ján Pich

Institute of Mathematics
Czech Academy of Sciences

joint work with Rahul Santhanam

Lower Bounds and Metamathematics

Complexity lower bounds are hard to prove.

Metamathematics of lower bounds: understand the difficulty of proving them.

- ◦ guides us away from methods that cannot work
- ◦ inspires new approaches to lower bounds

  e.g. natural proofs → new proof complexity lower bounds → hardness magnification

- ◦ important on its own

  e.g. complexity of the minimum circuit size problem MCSP

History: Circuit Complexity

Closely related struggle we are building on

Golden age: AC^0, $AC^0[p]$, monotone circuit lower bounds ...

Barriers: natural proofs, relativization, algebrization ...

Natural proofs of Razborov-Rudich:

- ∘ a dense easy subset of hard Boolean functions
- ∘ known explicit circuit lower bounds are natural
- ∘ natural proofs against strong circuit models break SPRNGs

- influential (emphasize central role of MCSP in Complexity Theory)
- ad-hoc (natural proofs are not mathematical proofs in formal sense)

Natural proofs as proof complexity lower bounds

Razborov: $S^2_2(\alpha) \nvdash \mathsf{SAT} \notin \mathsf{P/poly}$ unless $\neg\exists$ SPRNGs

Propositional version (Razborov-Krajíček):
$tt(f, n^{O(1)})$ hard for automatizable propositional proof systems unless $\neg\exists$ SPRNG

$$tt(f,s) \in \mathsf{TAUT} \Leftrightarrow f \notin \mathsf{Circuit}[s]$$

2^n bits encoding f, $poly(s)$ variables for circuits of size s, total size: $2^{O(n)}$

Natural proofs as proof complexity lower bounds

Razborov: $S^2_2(\alpha) \nvdash \mathsf{SAT} \notin \mathsf{P/poly}$ unless $\neg\exists$ SPRNGs

Propositional version (Razborov-Krajíček):
$tt(f, n^{O(1)})$ hard for automatizable propositional proof systems unless $\neg\exists$ SPRNG

$$tt(f,s) \in \mathsf{TAUT} \Leftrightarrow f \notin \mathsf{Circuit}[s]$$

2^n bits encoding f, $poly(s)$ variables for circuits of size s, total size: $2^{O(n)}$

$tt(f,s)$:

- candidate hard tautologies for strong proof systems
- extensively studied
  - Raz: Resolution has no p-size proofs of $tt(f, n^{O(1)})$
  - Razborov: $Res(\epsilon \log n)$ does not have p-size proofs of $tt(f, n^{\omega(1)})$
  - Proof Complexity Generators

We'll use similar framework for reasoning about hardness of proof complexity LBs

Barriers on Proof Complexity Lower Bounds

- historically, **PCLBs tend to be harder** to prove than CLBs

  major example: $\mathsf{AC}^0[p]$-Frege LBs still open

- but metamathematics of PCLBs **received less attention** than metamathematics of CLBs

Earlier results on hardness of PCLBs

1. **'Simulation' barrier** (Cook-Reckhow, Krajíček-Pudlák)

$$P \vdash \mathrm{lb}(Q, n^{O(1)}, \phi) \quad \Rightarrow \quad P \text{ simulates } Q$$

$\mathrm{lb}(Q, s, \phi) \in \mathrm{TAUT} \Leftrightarrow \neg\exists$ s-size Q-proof of ϕ

$\mathrm{lb}(Q, s, \phi)$ has $poly(s, |\phi|)$ variables for Q-proofs of size s

Earlier results on hardness of PCLBs

1. **'Simulation' barrier** (Cook-Reckhow, Krajíček-Pudlák)

$$P \vdash \mathrm{lb}(Q, n^{O(1)}, \phi) \quad \Rightarrow \quad P \text{ simulates } Q$$

$\mathrm{lb}(Q, s, \phi) \in \mathrm{TAUT} \Leftrightarrow \neg\exists$ s-size Q-proof of ϕ
$\mathrm{lb}(Q, s, \phi)$ has $poly(s, |\phi|)$ variables for Q-proofs of size s

Proof. $P \vdash \mathrm{lb}(Q, n^{O(1)}, \phi) \quad \Rightarrow \quad P \vdash Ref_Q$. □

Ex. Reasoning inside EF cannot prove lower bounds for ZFC
unless EF simulates ZFC.

Earlier results on hardness of PCLBs

1. **'Simulation' barrier** (Cook-Reckhow, Krajíček-Pudlák)

$$P \vdash \mathrm{lb}(Q, n^{O(1)}, \phi) \quad \Rightarrow \quad P \text{ simulates } Q$$

$\mathrm{lb}(Q, s, \phi) \in \mathrm{TAUT} \Leftrightarrow \neg\exists$ s-size Q-proof of ϕ
$\mathrm{lb}(Q, s, \phi)$ has $poly(s, |\phi|)$ variables for Q-proofs of size s

Proof. $P \vdash \mathrm{lb}(Q, n^{O(1)}, \phi) \quad \Rightarrow \quad P \vdash Ref_Q$. □

Ex. Reasoning inside EF cannot prove lower bounds for ZFC unless EF simulates ZFC.

2. **'Translation' barrier** (Cook-Urquhart, Buss, Krajíček-Pudlák)

$$\mathrm{PV}_1 \nvdash \forall n\ \exists \phi_n \in \mathrm{TAUT}, |\phi_n| = n \text{ s.t.}$$
$$\forall \pi, |\pi| = n^{\log n}, \pi \text{ is not EF-proof of } \phi_n$$

$\mathrm{PV}_1 \vdash$ Haken's lower bound for Resolution (Pitassi-Cook)
$\mathrm{PV}_1 \vdash^?$ constant-depth Frege lower bounds (Bellantoni-Pitassi-Urquhart)

Earlier results on hardness of PCLBs

3. **'Witnessing' barrier** (Krajíček)

$$\mathrm{PV}_1 \nvdash \mathrm{NP} \neq \mathrm{coNP} \text{ unless } \mathrm{NP} \cap \mathrm{coNP} \subseteq_A \mathrm{Circuit}[2^{n^{\epsilon}}]$$

NP $\neq$ coNP formalized so that

$$\# \text{ of assignments of hard } \phi_n \in \mathrm{TAUT} \text{ is feasible}$$

i.e. 2^n is a length of some number

Earlier results on hardness of PCLBs

3. **'Witnessing' barrier** (Krajíček)

$$\mathsf{PV}_1 \nvdash \mathsf{NP} \neq \mathsf{coNP} \text{ unless } \mathsf{NP} \cap \mathsf{coNP} \subseteq_A \mathsf{Circuit}[2^{n^{\epsilon}}]$$

NP $\neq$ coNP formalized so that

$\#$ of assignments of hard $\phi_n \in$ TAUT is feasible

i.e. 2^n is a length of some number

4. **Reductions to hard problems**

IPS not p-bounded $\Rightarrow$ VP $\neq$ VNP (Grochow-Pitassi)

EF not p-bounded $\Rightarrow$ P $\neq$ NP consistent with S^1_2

Our results: natural proofs for proof complexity

Natural proofs (more details)

$\mathcal{F}_n$: Boolean functions on n inputs

$\mathcal{C} \subseteq \mathcal{F}_n$ is $\mathcal{B}$-natural proof useful against $\mathcal{D}$ iff

Constructivity. truth tables of $f \in \mathcal{C}$ recognizable by a $\mathcal{B}$-circuit with 2^n inputs and size $2^{O(n)}$

Largeness. $\Pr[f \in \mathcal{C}] \geq 1/2^{O(n)}$

Usefulness. $f \in \mathcal{C} \Rightarrow f \notin \mathcal{D}$

Natural proofs (more details)

$\mathcal{F}_n$: Boolean functions on n inputs

$\mathcal{C} \subseteq \mathcal{F}_n$ is $\mathcal{B}$-natural proof useful against $\mathcal{D}$ iff

Constructivity. truth tables of $f \in \mathcal{C}$ recognizable by a $\mathcal{B}$-circuit with 2^n inputs and size $2^{O(n)}$

Largeness. $\Pr[f \in \mathcal{C}] \geq 1/2^{O(n)}$

Usefulness. $f \in \mathcal{C} \Rightarrow f \notin \mathcal{D}$

Razborov-Rudich: SPRNGs $\Rightarrow \neg\exists$ P/poly-natural proof against P/poly.

Rudich: Super-bits $\Rightarrow \neg\exists$ NP-natural proof against P/poly.

Super-bit. (PRG safe against nondeterministic circuits)
$g : \{0,1\}^n \mapsto \{0,1\}^{n+1}$ computable in P/poly s.t. $\exists\epsilon > 0$,
$\forall$ nondeterministic circuits C of size 2^{n^ϵ},

$$\Pr[C(y) = 1] - \Pr[C(g(y)) = 1] < 1/|C|$$

Proof complexity version of natural proofs

Recall: $tt(f,s) \in \text{TAUT} \Leftrightarrow f \notin \text{Circuit}[s]$

$\text{lb}(Q,s,\phi) \in \text{TAUT} \Leftrightarrow \neg\exists$ s-size Q-proof of ϕ

Definition: pps Q defines Q-natural property useful against pps P

$$\equiv$$

$$Q \vdash \text{lb}(P, 2^{O(n)}, tt(f, n^{O(1)})) \text{ for } \frac{1}{2^{O(n)}} \text{ of all } f \in \mathcal{F}_n$$

Proof complexity version of natural proofs

Recall: $tt(f,s) \in \mathrm{TAUT} \Leftrightarrow f \notin \mathrm{Circuit}[s]$

$\mathrm{lb}(Q,s,\phi) \in \mathrm{TAUT} \Leftrightarrow \neg\exists$ s-size Q-proof of ϕ

Definition: pps Q defines Q-natural property useful against pps P

$$\equiv$$

$$Q \vdash \mathrm{lb}(P, 2^{O(n)}, tt(f, n^{O(1)})) \text{ for } \frac{1}{2^{O(n)}} \text{ of all } f \in \mathcal{F}_n$$

WHY this definition?

- constructivity: replaced by provability
- largeness: accepts many hard tautologies instead of hard functions
- $\mathrm{tt}(f,s)$: candidate hard tautologies for strong proof systems
  we consider also random 3CNFs instead of $tt(f,s)$ formulas

Note: if we want $\phi \in \mathrm{TAUT}$ hard for all pps

ϕ cannot be generated in (det.) p-time, i.e. focus on random ϕ

(Alternative definitions possible)

Proof complexity version of natural proofs

Recall: $tt(f,s) \in \mathrm{TAUT} \Leftrightarrow f \notin \mathrm{Circuit}[s]$

$\mathrm{lb}(Q,s,\phi) \in \mathrm{TAUT} \Leftrightarrow \neg\exists$ s-size Q-proof of ϕ

Definition: pps Q defines Q-natural property useful against pps P

$$\equiv$$

$$Q \vdash \mathrm{lb}(P, 2^{O(n)}, tt(f, n^{O(1)})) \text{ for } \frac{1}{2^{O(n)}} \text{ of all } f \in \mathcal{F}_n$$

WHY this definition?

- constructivity: replaced by provability
- largeness: accepts many hard tautologies instead of hard functions
- tt(f, s): candidate hard tautologies for strong proof systems
  we consider also random 3CNFs instead of $tt(f,s)$ formulas

Note: if we want $\phi \in \mathrm{TAUT}$ hard for all pps

ϕ cannot be generated in (det.) p-time, i.e. focus on random ϕ

(Alternative definitions possible)

Ex.: EF-natural proofs useful against Resolution?

Theorem 1

Super-bits $\Rightarrow \forall$ pps P simulating Resolution

for each f, $\text{tt}(f, n^{O(1)})$ hard for P

or $\forall$ pps Q,

$\neg\exists$ Q-natural property useful against P.

Theorem 1

Super-bits $\Rightarrow$ $\forall$ pps P simulating Resolution

for each f, $\mathrm{tt}(f, n^{O(1)})$ hard for P

or $\forall$ pps Q,

$\neg\exists$ Q-natural property useful against P.

Proof: By counterpositive. Assume $P \vdash tt(f, n^k)$

Suffices to construct NP/poly-natural property useful against P/poly:

Theorem 1

Super-bits $\Rightarrow \forall$ pps P simulating Resolution

for each f, $\mathrm{tt}(f, n^{O(1)})$ hard for P

or $\forall$ pps Q,

$\neg\exists$ Q-natural property useful against P.

Proof: By counterpositive. Assume $P \vdash tt(f, n^k)$

Suffices to construct NP/poly-natural property useful against P/poly:

$$S := \{g \in \mathcal{F}_n \mid Q \vdash lb(P, 2^{O(n)}, \mathrm{tt}(f \oplus g, n^k/3))\}$$

Theorem 1

Super-bits $\Rightarrow \forall$ pps P simulating Resolution

for each f, $\text{tt}(f, n^{O(1)})$ hard for P

or $\forall$ pps Q,

$\neg\exists$ Q-natural property useful against P.

Proof: By counterpositive. Assume $P \vdash tt(f, n^k)$

Suffices to construct NP/poly-natural property useful against P/poly:

$$S := \{g \in \mathcal{F}_n \mid Q \vdash lb(P, 2^{O(n)}, \text{tt}(f \oplus g, n^k/3))\}$$

Constuctivity ✓   Largeness ✓

Usefulness:

Theorem 1

Super-bits $\Rightarrow$ $\forall$ pps P simulating Resolution

for each f, $\mathrm{tt}(f, n^{O(1)})$ hard for P

or $\forall$ pps Q,

$\neg\exists$ Q-natural property useful against P.

Proof: By counterpositive. Assume $P \vdash tt(f, n^k)$

Suffices to construct NP/poly-natural property useful against P/poly:

$$S := \{g \in \mathcal{F}_n \mid Q \vdash lb(P, 2^{O(n)}, \mathrm{tt}(f \oplus g, n^k/3))\}$$

Constuctivity ✓ Largeness ✓

Usefulness:

Claim: $P \vdash \mathrm{tt}(f \oplus g, n^k/3) \vee \mathrm{tt}(g, n^k/3)$

Therefore, $g \in \mathrm{Circuit}[n^k/3] \Rightarrow P \vdash \mathrm{tt}(f \oplus g, n^k/3) \Rightarrow g \notin S$ $\square$

Theorem 2 (Unconditional LB)

Definition: The existence of super-bits admits feasible proofs if

$\forall$ non-uniform pps P $\exists$ pps Q s.t. for $1 - 1/2^{\omega(n)}$ fraction of f_n's

$$Q \vdash \mathrm{lb}(P, 2^{O(n)}, \mathrm{tt}(f_n, n^{O(1)}))$$

Theorem 2: The existence of super-bits does not admit feasible proofs.

Theorem 2 (Unconditional LB)

Definition: The existence of super-bits admits feasible proofs if

$\forall$ non-uniform pps P $\exists$ pps Q s.t. for $1 - 1/2^{\omega(n)}$ fraction of f_n's

$$Q \vdash \mathrm{lb}(P, 2^{O(n)}, \mathrm{tt}(f_n, n^{O(1)}))$$

Theorem 2: The existence of super-bits does not admit feasible proofs.

Note: Thm 2 unconditional but does not imply NP $\neq$ coNP
because $\mathrm{lb}(P, 2^{O(n)}, \mathrm{tt}(f_n, n^{O(1)}))$ might not be a tautology.

Proof:

$\exists$ NP-natural property against P/poly $\Rightarrow$ ✓

else $\Rightarrow$ SAT $\notin$ P/poly

$\Rightarrow$ $\exists$ pps P s.t. $P \vdash \mathrm{tt}(SAT, n^2)$

$\Rightarrow$ $\neg\exists$ Q-natural proof against P (by Theorem 1)

□

Theorem 2 (Unconditional LB)

Definition: The existence of super-bits admits feasible proofs if

$\forall$ non-uniform pps P $\exists$ pps Q s.t. for $1 - 1/2^{\omega(n)}$ fraction of f_n's

$$Q \vdash \mathrm{lb}(P, 2^{O(n)}, \mathrm{tt}(f_n, n^{O(1)}))$$

Theorem 2: The existence of super-bits does not admit feasible proofs.

Note: Thm 2 unconditional but does not imply NP $\neq$ coNP
because $\mathrm{lb}(P, 2^{O(n)}, \mathrm{tt}(f_n, n^{O(1)}))$ might not be a tautology.

Proof:

$\exists$ NP-natural property against P/poly $\Rightarrow$ ✓

else $\Rightarrow$ SAT $\notin$ P/poly

$\Rightarrow \exists$ pps P s.t. $P \vdash \mathrm{tt}(SAT, n^2)$

$\Rightarrow \neg\exists$ Q-natural proof against P (by Theorem 1)

□

Compare to natural proofs: Thm 2 unconditional but
does not necessarilly work for specific systems like EF

Feige's hypothesis (random 3CNFs)

$U_{\Delta,n}$: distribution over 3CNFs on n inputs with Δn clauses, $\Delta > 0$

pick each clause by selecting 3 literals uniformly at random from $2n$ possibilities

Nondeterministic Feige's hypothesis:

$\forall$ non-uniform pps R w.h.p. $\phi \in$ UNSAT but $\neg\phi$ hard for R.

Definition: Nondeterministic Feige's hypothesis admits feasible proofs if

$\forall$ non-uniform pps P $\exists$ pps Q s.t. for $1 - o(1)$ fraction of ϕ,

$$Q \vdash \mathrm{lb}(P, |\phi|^k, \phi).$$

Feige's hypothesis (random 3CNFs)

$U_{\Delta,n}$: distribution over 3CNFs on n inputs with Δn clauses, $\Delta > 0$
pick each clause by selecting 3 literals uniformly at random from $2n$ possibilities

Nondeterministic Feige's hypothesis:

$\forall$ non-uniform pps R w.h.p. $\phi \in$ UNSAT but $\neg\phi$ hard for R.

Definition: Nondeterministic Feige's hypothesis admits feasible proofs if

$\forall$ non-uniform pps P $\exists$ pps Q s.t. for $1 - o(1)$ fraction of ϕ,

$$Q \vdash \mathrm{lb}(P, |\phi|^k, \phi).$$

Theorem 3: Super-bits $\Rightarrow$ $\neg\exists$ feasible proof of nondet. Feige hypothesis

Feige's hypothesis (random 3CNFs)

$U_{\Delta,n}$: distribution over 3CNFs on n inputs with Δn clauses, $\Delta > 0$
pick each clause by selecting 3 literals uniformly at random from $2n$ possibilities

Nondeterministic Feige's hypothesis:

$\forall$ non-uniform pps R w.h.p. $\phi \in$ UNSAT but $\neg\phi$ hard for R.

Definition: Nondeterministic Feige's hypothesis admits feasible proofs if

$\forall$ non-uniform pps P $\exists$ pps Q s.t. for $1 - o(1)$ fraction of ϕ,

$$Q \vdash \mathrm{lb}(P, |\phi|^k, \phi).$$

Theorem 3: Super-bits $\Rightarrow \neg\exists$ feasible proof of nondet. Feige hypothesis

Proof: Use $KT(y) = min\{|d| + t; U^d(i) = y_i \text{ in } t \textit{ steps}\}$

Claim: If $KT(\phi)$ high, then ϕ unsatisfiable.

Proceed as in Thm 1 but with tautologies expressing high KT instead of $tt(f, s)$.

□

First-order unprovability of $\exists$ Super-bits

We can show that the existence of super-bits cannot be proved in theories of bounded arithmetic either.

First-order unprovability of $\exists$ Super-bits

We can show that the existence of super-bits cannot be proved in theories of bounded arithmetic either.

- also unconditional result
- completely different proof

Theorem 4: $\mathsf{PV}_1 \nvdash \exists$ Super-bits.

$\exists$ Super-bits formalized so that 2^n is a length of a number.

First-order unprovability of $\exists$ Super-bits

We can show that the existence of super-bits cannot be proved in theories of bounded arithmetic either.

- also unconditional result
- completely different proof

Theorem 4: $\mathrm{PV}_1 \nvdash \exists$ Super-bits.

$\exists$ Super-bits formalized so that 2^n is a length of a number.

Proof:

Builds on Krajíček's proof of a conditional unprovability of $\mathrm{NP} \neq \mathrm{coNP}$.

□

Further questions

- Show **hardness of PCLBs for specific systems** such as EF?
- Show **unconditional hardness** of non-deterministic **Feige's hypothesis**?
- Get hardness of PCLBs for **other families of random tautologies**?
  All p-time samplable families?
- Find more applications of **non-constructive methods in Proof Complexity**.
- Better understanding of metamathematics of lower bounds and
  connections between Proof Complexity and Circuit Complexity LBs?

Thank You for Your Attention

Krajíček's Fest & **Complexity Theory with a Human Face**

1-4 September 2020, Tábor, Czech Republic

more info: `users.math.cas.cz/~pich`