Meta-Mathematics of Complexity Lower Bounds

Rahul Santhanam (University of Oxford)

Plan of the Talk

- Barriers to Circuit Complexity Lower Bounds
  - Natural Proofs and Meta-Complexity
  - Proof Complexity Generators and Razborov’s Conjectures
- Barriers to Proof Complexity Lower Bounds
- Future Directions

Plan of the Talk

- *Barriers to Circuit Complexity Lower Bounds*
  - Natural Proofs and Meta-Complexity
  - Proof Complexity Generators and Razborov's Conjecture
- Barriers to Proof Complexity Lower Bounds
- Future Directions

Lower Bounds and Meta-mathematics

- Lower bounds (in circuit complexity, algebraic complexity, proof complexity etc.) are often very hard to prove
- In this best of all possible worlds, we might not have lower bounds yet, but at least we have barriers…
- Meta-mathematics of lower bounds: studies logical difficulty of proving lower bounds
- Reasons for doing meta-mathematics
  - Guides us away from lower bound techniques that are inherently limited
  - Can itself be a source of lower bound ideas

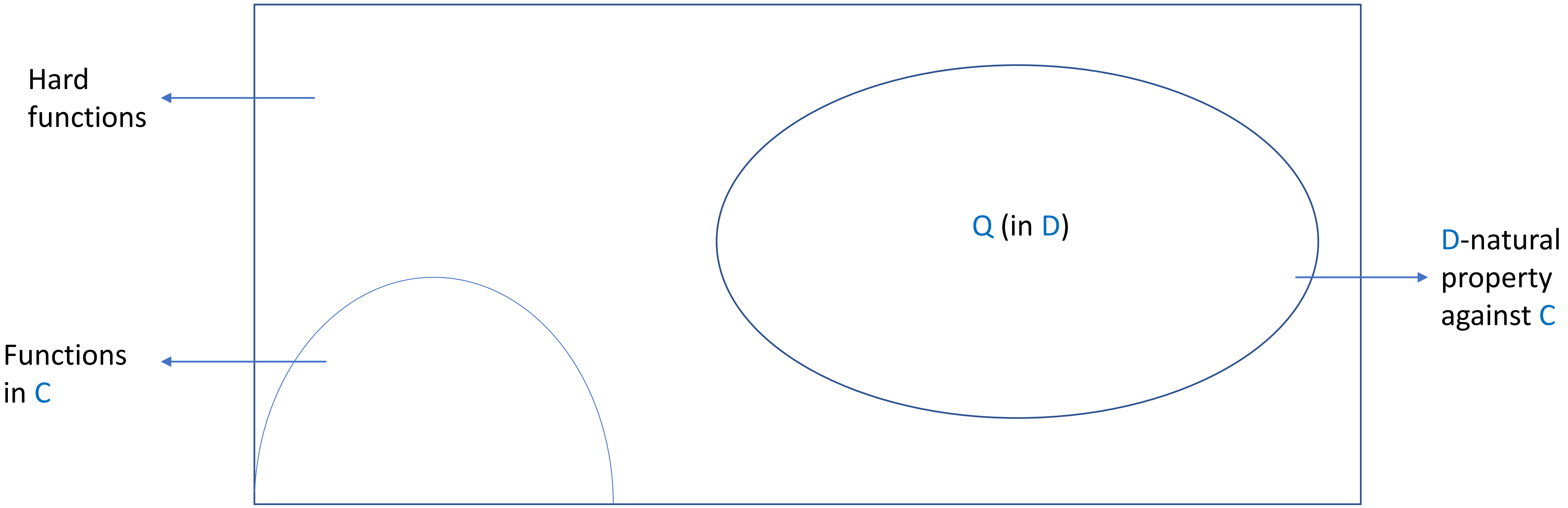
Lower Bounds in Circuit Complexity

- Are there explicit functions that require super-polynomial Boolean circuits?
- Lots of progress in the 80s on restricted circuit models: AC^0, $AC^0[p]$, monotone circuits
- Frontier hasn't expanded much since then
- Frontier problems
  - Lower bounds for ACC^0 (constant-depth circuits with modular gates of arbitrary modulus)
  - Lower bounds for depth-2 TC^0
- Various meta-mathematical approaches: relativization [BGS75], algebrization [AW09], natural proofs [RR97]

Natural Proofs

- Given a complexity class D and a circuit class C, a D-natural proof against C is a property Q of Boolean functions (represented by their truth tables of size N) such that:
  - Constructivity: Q in D
  - Usefulness: Q(F) = 1 => F not in C
  - Density: At least a $1/N^{O(1)}$ fraction of Boolean functions F satisfy Q

Natural Proofs

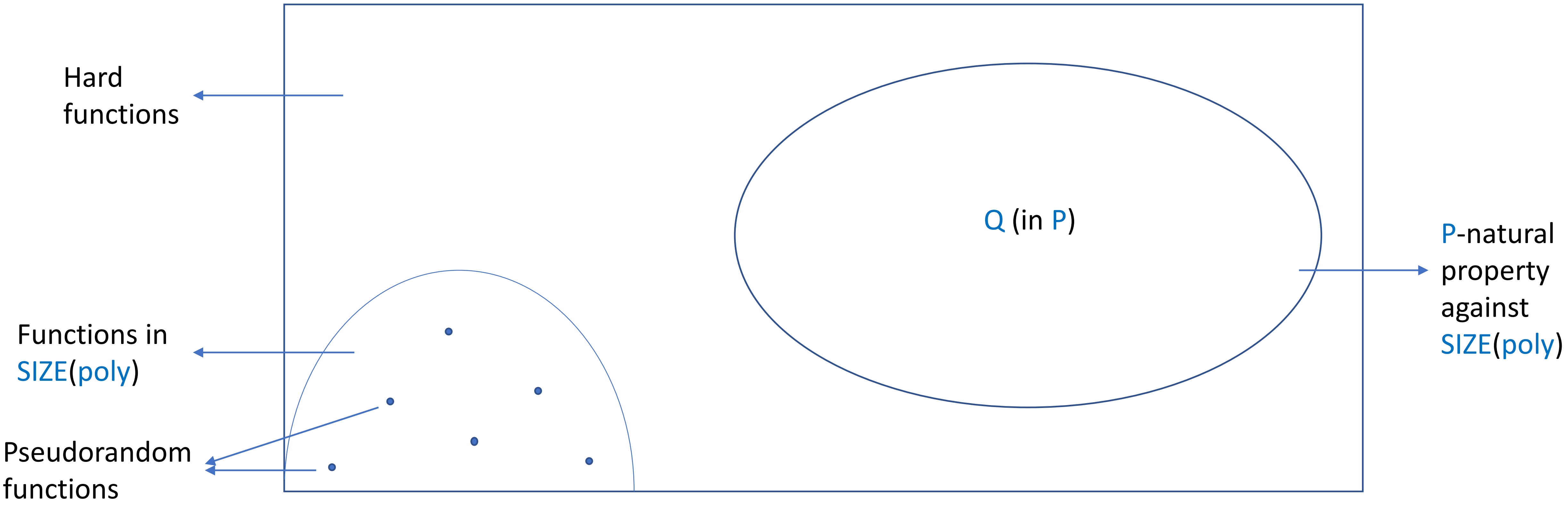


Natural Proofs

- Given a complexity class D and a circuit class C, a D-natural proof against C is a property Q of Boolean functions (represented by their truth tables of size N) such that:
  - Constructivity: Q in D
  - Usefulness: Q(F) = 1 => F not in C
  - Density: At least a $1/N^{O(1)}$ fraction of Boolean functions F satisfy Q
- Razborov and Rudich observed that standard circuit lower bound proofs against restricted circuit classes yield P-natural proofs against C
- Main theorem [RR97]: If exponentially hard one-way functions exist, there are no P-natural proofs against SIZE(poly)

Natural Proofs: Proof of Main Theorem

Lemma [GGM86]: If exponentially hard one-way functions exist, then there is pseudorandom function family in SIZE(poly) against SIZE($2^{O(n)}$)



Q distinguishes random from pseudorandom, and is poly-time computable. Contradiction!

Natural Proofs

- A lesson from natural proofs: traditional “slice and measure” techniques are unlikely to be able to prove strong lower bounds
- An interesting feature of [RR97]: the difficulty of showing circuit lower bounds follows from a *circuit lower bounds assumption*

Meta-Complexity

- Meta-complexity studies the computational complexity of problems that are themselves about complexity
- Minimum Circuit Size Problem (MCSP)
  - Input: A Boolean function F on n bits, given by its truth table of size $N=2^n$. Also a parameter $s <= N$
  - Output: Yes iff F has a Boolean circuit of size at most s
- Time-Bounded Kolmogorov Complexity Problem (K^t): here t is some fixed polynomial time bound
  - Input: A string X of length N and a parameter $s <= N$
  - Output: Yes iff there is a program p of size at most s such that $U(p, \varepsilon)$ outputs X in at most $t(N)$ steps
- MCSP[s] denotes the version where s is a fixed function of N

Solving MCSP on Average

- A natural distribution over inputs to MCSP[s] is the uniform distribution over N-bit strings
- We say MCSP[s] is zero-error easy on average if there is an efficient algorithm that
  - Always outputs 0, 1 or '?'
  - Never outputs the wrong answer on any input
  - Outputs the correct answer for at least a 1/poly(N) fraction of inputs
- Proposition: P-Natural proofs useful against SIZE(s) exists iff MCSP[s] is zero-error easy on average

Perspective: Chaitin's Theorem

- Theorem [C74]: For any sound formal system F, there is a constant c such that F cannot prove any statement of the form "K(x) > c"
- Proof sketch: If there are large enough c for which we can show "K(x) > c" in F, then we can find the first such x for which such a proof exists using a program of size log(c) + O(1). Contradiction.
- Chaitin's theorem states that formal systems of *unbounded* computational power cannot prove non-trivial lower bounds on *time-unbounded* Kolmogorov complexity
- When studying meta-mathematics of lower bounds, we are interested in whether resource-bounded formal systems can prove non-trivial lower bounds on resource-bounded versions of Kolmogorov complexity

Plan of the Talk

- Barriers to Circuit Complexity Lower Bounds
  - Natural Proofs and Meta-Complexity
  - *Proof Complexity Generators and Razborov's Conjecture*
- Barriers to Proof Complexity Lower Bounds
- Future Directions

Beyond Natural Proofs

- Natural proofs have been enormously influential in complexity theory
  - Extremely useful heuristically in evaluating the power of a lower bound technique
  - Are key to understanding connections between learning, pseudorandomness and meta-mathematics of lower bounds
- But the concept has some issues
  - Definition somewhat ad hoc (dictated by the cryptographic hardness result that can be shown)
  - Natural proofs aren’t really proofs in a formal mathematical sense
  - This meta-mathematical approach doesn’t directly model the hard function for which the lower bound is shown

Provability of Circuit Lower Bounds

- A related but more formal approach: study the difficulty of proving "F is a hard function" in various logical theories/proof systems
- This approach was taken by Razborov [R95], who formalized this statement in the context of bounded arithmetic and propositional proof complexity, and showed that certain weak propositional proof systems (comparable in power to Resolution) cannot prove such a statement for *any* function F
- Further conjectures along these lines in [R97], [ABRW02], [K04], [R15]

Formalization: Circuit Lower Bound Tautologies

- Let F be a Boolean function on n variables given by its truth table, and s be a size bound
- $tt(F,s)$ is a propositional tautology stating that for all circuits C of size s, C does not compute F
  - This can be expressed as a DNF of size $O(2^n \text{poly}(s))$, which is the disjunction of 2^n DNFs ϕ_x, one for each $x \in \{0,1\}^n$, where ϕ_x expresses $C(x) \neq F(x)$
  - Propositional variables encode the circuit C

Propositional Proof Complexity

- Studies the power of propositional proof systems (pps) to prove propositional tautologies (TAUT)
- A pps (resp. non-uniform pps) R is a poly-time (resp. poly-size) computable binary relation s.t.
  - $\exists$ y R(ϕ,y) iff ϕ $\in$ TAUT
- An R-proof of a tautology ϕ is a string y such that R(ϕ,y) holds. The R-proofsize of ϕ is the smallest size of an R-proof of ϕ
- We seek to understand, for various ppses R and natural families of tautologies $\{\phi_n\}$, how R-proofsize(ϕ_n) grows with $|\phi_n|$

Are Circuit Lower Bound Tautologies Hard?

- Question: Given a pps Q, for which Boolean functions F and size bounds s does tt(F,s) have short Q-proofs?
- [R95a] implies that essentially all known explicit circuit lower bounds can be shown in Extended Frege, and often in Frege or weaker systems
- An even more significant barrier than the Natural Proofs barrier would be if EF could not show any non-trivial lower bounds for general circuits
- We seem far from proving *any* interesting EF lower bounds, but perhaps we could get conditional results for EF as well as unconditional results for weaker Q (where we have lower bounds)?

Conjecture X

- Conjecture: For *every* Boolean function F on n variables, $tt(F, n^{\omega(1)})$ does not have EF-proofs of polynomial size
- I do not give a reference because while Razborov has mentioned this conjecture in talks, it does not seem to have appeared in published work
- Also, Krajicek has posed closely related conjectures in [K01,K01a]
- Conjecture X for Q: For *every* Boolean function F on n variables, $tt(F, n^{\omega(1)})$ does not have Q-proofs of polynomial size

Pseudo-Random Generators for Propositional Proof Systems

- [ABRW02] define and study the notion of a pseudo-random generator (PRG) for a pps Q
  - A mapping G from n bits to m bits, where $m > n$, is called a PRG for Q if the propositional formula encoding $G(x) \neq y$ does not have poly-size Q-proofs for any x of length n and y of length m
- Conjecture X for Q holds if the *truth-table generator* mapping a circuit of size $n^{\omega(1)}$ on n variables to the corresponding truth table of size 2^n is a PRG for Q
  - Indeed, it suffices to construct a PRG for Q that is *succinctly* computable from its n-bit seed

Relationship to Razborov's Conjectures

- Razborov [R15] states 2 conjectures – Conjecture 1 and Conjecture 2 – that are related to what we consider
  - Conjecture 1 states that the Nisan-Wigderson PRG based on any poly-time predicate that is hard on average for poly-size formulas is a PRG for Frege
  - Conjecture 2 states the Nisan-Wigderson PRG based on an NP ∩ coNP predicate that is hard on average for poly-size Boolean circuits is a PRG for EF
- Under the assumption that P does not have poly-size formulas on average, Conjecture 1 implies Conjecture X for Frege

What is Known

- [R95] showed that Conjecture X is true for any pps Q with feasible interpolation under standard cryptographic assumptions
- [R04] showed unconditionally that Conjecture X is true for Res
- [R15] showed unconditionally that Conjecture X is true for Res(o(log log(n))) and PCR
- If NEXP does not have poly-size circuits, there is a pps Q such that Conjecture X does not hold for Q

An Observation

- Observation: Conjecture X holds iff there is no polynomial-time algorithm that finds EF-proofs of $tt(F, n^{\omega(1)})$ for infinitely many F
- Proof sketch:
  - Let F on n variables be such a function with truth table y of length $N = 2^n$ and let w be a Q-proof of size $poly(N)$ for $tt(F, n^{\omega(1)})$
  - Note that yw is the truth table of a Boolean function F' on $O(n)$ variables that requires circuits of size $n^{\omega(1)}$ (assuming wlog that $|w|$ is a power of 2)
  - A short proof that $tt(F', n^{\omega(1)})$ holds can be generated efficiently from a short proof that $tt(F, n^{\omega(1)})$ holds, i.e., from w

Plan of the Talk

- Barriers to Circuit Complexity Lower Bounds
  - Natural Proofs and Meta-Complexity
  - Proof Complexity Generators and Razborov's Conjectures
- *Barriers to Proof Complexity Lower Bounds*
- Future Directions

What is Known about Proof Complexity Lower Bounds?

- Super-polynomial lower bounds are known only for relatively weak ppses
  - Haken [H85] showed lower bounds on Resolution proofs of the Pigeonhole Principle
  - Ajtai [A94] showed lower bounds on AC^0-Frege proofs of the Pigeonhole Principle
  - No non-trivial lower bounds are known for the Frege or Extended Frege ppses
- On the one hand, proof complexity lower bounds have historically been harder to show than circuit complexity lower bounds
- On the other hand, there is almost no work on formally justifying their difficulty

Which Tautologies are Believed to be Hard?

- Can we find a sequence of poly-time constructible tautologies $\{\phi_n\}$, $|\phi_n| = n$, such that $\{\phi_n\}$ is hard for *every* pps R?
  - No! We can define a pps R which simply computes the sequence for itself, exploiting poly-time constructibility, and accepts all such tautologies with proofs of size zero
- Moral: We should use *randomness* when generating hard instances
- Candidate Hard distributions
  - Random k-DNFs with Δn clauses, for large enough Δ
  - Random circuit lower bound tautologies, expressing that a random Boolean function does not have small Boolean circuits (Rudich's Conjecture)

Meta-mathematics of Proof Complexity

- For candidate hard distributions, formalize and study the question of whether proof complexity lower bounds for formulas sampled from this distributions are hard to show

Main Results of [PS19]: An Informal Statement

- In the results below, “candidate hard instances” = random circuit lb tautologies
- Conditional Result: If candidate hard instances are hard for every non-uniform pps, then there is a pps R for which R-proofsize lower bounds on candidate hard instances are hard to prove (for every non-uniform pps)
  - Proof complexity lower bounds are hard because they are *true*
- Unconditional Result: There is a non-uniform pps R for which R-proofsize lower bounds on candidate hard instances are hard to prove (for every non-uniform pps)
  - Proof by “win-win” argument: If assumption of Conditional Result holds, we can apply the result to get our conclusion. If not, then consider the non-uniform pps R for which candidate instances are not hard. For this R, lower bound proofs *do not exist*, and hence conclusion holds

Formalization: Metamathematics of Proof Complexity

- How do we formalize the notion that a proof complexity lower bound is hard to prove?
- It is natural to use the meta-mathematical interpretation of ppses, and insist that the proof complexity lower bound, appropriately formalized, is *itself* provable in some pps
- Indeed, known proof complexity lower bounds such as those for Resolution and AC^0-Frege have short proofs in the Extended Frege proof system when appropriately formalized [CP90, BPU92]

Formalization: Proof Complexity Lower Bound Formulas

- Given a pps R, a propositional formula ϕ and a size bound t, $R\text{-pflb}(\phi,t)$ is a propositional formula asserting that ϕ does not have R-proofs of size t
  - This can be expressed as a DNF of size $poly(|\phi|+t)$, where the propositional variables encode a candidate R-proof of ϕ of size t, and the DNF encodes a simulation of the verifier for R to check that the candidate proof is invalid
- Similar formalization for non-uniform pps R

Formal Statement of Main Results [PS19]

- Theorem 1: If Rudich's Conjecture holds, then there is a constant d and a pps R such that for every non-uniform pps Q, with high probability over choice of F, R-pflb(tt(F,n^d), m^d) does not have poly-size Q-proofs (where $m = |\mathrm{tt}(F,n^d)|$)
- Theorem 2: If Rudich's Conjecture holds, then there is a constant d and a pps R such that for every non-uniform pps Q, with high probability over choice of random k-DNF ϕ, R-pflb(ϕ, m^d) does not have poly-size Q-proofs (where $m = |\phi|$)
- Theorem 3 (Unconditional Result): There is a non-uniform pps R such that for every non-uniform pps Q, with high probability over choice of F, R-pflb(tt(F,n^d), m^d) does not have poly-size Q-proofs (where $m = |\mathrm{tt}(F,n^d)|$)

A Slide about the Proofs

- Intuitively, the idea for Theorem 1 is that Rudich's Conjecture allows us to show the existence of *pseudorandom* tautologies, i.e., random-looking tautologies that have short proofs in some pps R. Because pseudorandom tautologies have short R-proofs, R-proofsize lower bounds *do not hold* for such tautologies
- On the other hand, Rudich's Conjecture implies that super-polynomial R-proofsize lower bounds *do hold* for random tautologies. If these lower bounds have short proofs in some pps Q, this allows us to distinguish random from pseudorandom – a contradiction!
- The proof of Theorem 2 builds on work of [HS17] on average-case reductions from SAT to MCSP

Perspective: Circuit Complexity vs Proof Complexity

- There are few direct connections between circuit complexity and proof complexity, but there are various similarities
  - There is a rough analogy between proving circuit lower bounds for a circuit class C and proof complexity lower bounds for the system C-Frege where lines of the proof are circuits from C
  - Some of the best proof complexity lower bounds, eg., for AC^0-Frege, are inspired by circuit lower bound techniques
- Theorems 1 and 3 can be thought of as giving an analogue of the natural proofs barrier for proof complexity

Natural Proofs vs Results of [PS19]

Natural Proofs Barrier

- Rules out efficient *algorithms* for hardness of random Boolean functions
- Is conditional on the existence of one-way functions
- Applies even to restricted circuit classes such as TC^0

Our Results

- Rule out efficient *proofs* for hardness of random tautologies
- Are unconditional
- Apply only to strong proof systems and not to systems such as EF

Using a Proof System Against Itself

- Is it true in general for strong enough pps R that R finds it hard to prove R-proofsize lower bounds (cf. [P20])?

Iterated Lower Bounds Hypothesis [ST21]

- Given a pps R and a formula ϕ that does not have short R-proofs, define the iterated lower bound formulas as follows:
  - $\phi_0 = \phi$
  - $\phi_{n+1} = \text{R-pflb}(\phi_n, |\phi_n|^{\omega(1)})$
- Iterated Lower Bounds Hypothesis [ST21]: For any reasonable strong enough pps R, the sequence of formulas $\{\phi_n\}$ is a sequence of hard tautologies for R
- The Hypothesis holds for Resolution, by applying non-automatability results of [AM20, G19] , and show that a constant number of iterations preserves hardness for random truth table formulas for strong R, using ideas of [PS19]

Can the Ideal Proof System Prove Lower Bounds against Itself?

- Ideal Proof System (IPS) of Grochow and Pitassi [GP18] is an algebraic proof system where proofs are algebraic circuits witnessing that a set of polynomial equations has no common zero
- Theorem [ST21]: There is an explicit sequence of formulas ψ_n conjectured to be hard for IPS such that VNP ≠ VP iff IPS cannot efficiently prove lower bounds against itself for the formulas ψ_n
- This gives an *equivalence* between proof complexity lower bounds and algebraic complexity lower bounds
  - Moreover, the equivalence works for *any* reasonable algebraic proof system at least as strong as IPS

[PS19] vs [ST21]

Barrier of [ST21]

- Rules out efficient proofs for hardness of explicit formulas
- Is conditional on VNP ≠ VP
- Applies to the well-studied proof system IPS

Barrier of [PS19]

- Rules out efficient proofs for hardness of random tautologies
- Is unconditional
- Applies only to strong (non-constructive) proof systems and not to systems such as EF

Plan of the Talk

- Barriers to Circuit Complexity Lower Bounds
  - Natural Proofs and Meta-Complexity
  - Proof Complexity Generators and Razborov’s Conjectures
- Barriers to Proof Complexity Lower Bounds
- *Future Directions*

Barriers: Pragmatic Questions

- Is there a good explanation of why current fixed-polynomial circuit lower bounds (for formulas, branching programs, circuits etc.) are stuck where they are?
- What are the limits of lifting results?

Barriers: Conceptual Questions

- Is there any complexity-theoretic evidence that proving lower bounds for Frege or EF is hard?
- Is there a plausible hardness assumption which implies that algebraic natural proofs do not exist?

Barriers: Technical Questions

- Falsify the Iterated Lower Bound's Hypothesis, eg., for AC^0-Frege
- Prove Conjecture X for AC^0-Frege