

A Unified Formal Framework for Relativization, Algebrization, and Natural Proof Barriers via Pseudorandomness

Dennj Osele
dennj.osele@gmail.com

Abstract

We present a unified, formally verified framework explaining the three major known barriers to proving $\mathbf{P} \neq \mathbf{NP}$: relativization, algebrization, and natural proofs. Rather than treating these barriers as distinct phenomena, we show that all three arise as instances of a single obstruction: the inability of restricted proof techniques to distinguish pseudorandom Boolean functions from truly random ones.

Our framework is developed in the Lean proof assistant and introduces an abstract notion of *observer-bounded proof techniques*. Within this setting, we prove a general barrier theorem: if pseudorandom functions exist against a class of observers, then no proof technique bounded by that class can certify a complexity separation.

Classical barrier results are recovered as corollaries, and their known hierarchy is formally derived. We further show that breaking the natural proofs barrier is necessary for breaking the others, yielding a precise characterization of what any successful $\mathbf{P} \neq \mathbf{NP}$ proof must accomplish.

This work provides a machine-verified unification of complexity-theoretic barriers and reframes pseudorandomness as the central explanatory principle behind the difficulty of circuit lower bounds.

The complete Lean formalization is available at:

<https://github.com/dennj/Pseudorandomness>

Keywords: Computational Complexity, P vs NP, Pseudorandomness, Natural Proofs, Relativization, Algebrization, Formal Verification

1. Introduction

Since the inception of complexity theory, progress on fundamental separation problems such as $\mathbf{P} \neq \mathbf{NP}$ has been repeatedly obstructed by a sequence of “barriers.” Among the most influential are:

- *Relativization* [1],
- *Natural Proofs* [2],
- *Algebrization* [4].

Each barrier demonstrates that a broad class of proof techniques is insufficient to resolve central open problems. However, these barriers have traditionally been studied independently, using different mathematical formalisms and intuitions.

In this paper, we argue that these barriers are not fundamentally distinct. Instead, they are manifestations of a single underlying limitation: *the inability of restricted proof techniques to distinguish pseudorandom Boolean functions from random ones*.

We formalize this insight in a general framework that:

1. Abstracts proof techniques as collections of bounded distinguishers (“observers”),
2. Defines pseudorandomness relative to observer classes,
3. Proves a universal barrier theorem subsuming all known barriers.

All results are mechanized in the Lean proof assistant, providing machine-checked certainty.

2. State of the Art and Related Work

The difficulty of resolving \mathbf{P} versus \mathbf{NP} has long been understood to stem not merely from technical obstacles, but from deep limitations inherent in broad classes of proof techniques. Over the past five decades, three major meta-barriers have been identified: relativization, natural proofs, and algebrization. Each barrier rules out a wide family of approaches and has profoundly shaped the direction of complexity theory.

2.1. Relativization

The relativization barrier was introduced by Baker, Gill, and Solovay [1], who demonstrated the existence of oracles A and B such that $\mathbf{P}^A = \mathbf{NP}^A$ while $\mathbf{P}^B \neq \mathbf{NP}^B$. This result showed that any proof resolving \mathbf{P} versus \mathbf{NP} must be non-relativizing, meaning that it cannot hold uniformly relative to all oracles. As a consequence, classical diagonalization and simulation arguments were rendered insufficient for major separations.

Relativization became the first recognized meta-barrier, motivating the search for techniques that exploit internal structure of computations rather than treating machines as black boxes.

2.2. Natural Proofs

Razborov and Rudich [2] introduced the natural proofs barrier, identifying a common pattern underlying nearly all known circuit lower bound arguments. A proof is *natural* if it relies on a property of Boolean functions that is both constructive (efficiently checkable) and large (satisfied by a non-negligible fraction of functions).

They proved that, assuming the existence of cryptographically secure pseudorandom functions, no natural proof can establish super-polynomial circuit lower bounds. In particular, natural proofs cannot separate \mathbf{P} from \mathbf{NP} under standard cryptographic assumptions. This result revealed an unexpected connection between circuit lower bounds and pseudorandomness, reframing lower bound proofs as implicit distinguishers against pseudorandom functions.

2.3. Algebrization

Aaronson and Wigderson [4] identified algebrization as a further barrier that subsumes relativization. Algebrization models proof techniques that allow oracle access not only to a Boolean function, but also to its low-degree polynomial extension over a field, capturing the power of arithmetization used in results such as $\mathbf{IP} = \mathbf{PSPACE}$.

They showed that while algebrization suffices to explain known non-relativizing results, major open problems such as \mathbf{P} vs. \mathbf{NP} , \mathbf{NP} vs. \mathbf{BPP} , and \mathbf{NEXP} vs. \mathbf{P}/poly do not algebrize. Consequently, any resolution of these problems must rely on fundamentally non-algebrizing techniques.

2.4. Axiomatic and Structural Refinements

Several works have sought to formalize and refine these barriers. Impagliazzo, Kabanets, and Kolokolova [5] introduced an axiomatic framework

capturing arithmetization via an Arithmetic Checkability axiom, showing that many central separations are independent of this axiom. Aydinlioğlu and Bach [6] further unified relativization and algebrization through affine relativization, providing a clean logical characterization of algebrizing proofs.

More recently, Hirahara, Lu, and Ren [7] proposed bounded relativization, showing that many known non-relativizing results still hold relative to restricted oracle classes, sharpening our understanding of the precise limits of existing techniques.

2.5. Pseudorandomness Beyond Complexity Theory

Pseudorandomness has also emerged as a unifying theme beyond complexity theory, notably in analytic number theory. Work by Green [8], Green and Tao [9], Sarnak [10], Granville and Soundararajan [11], and Tao and Teräväinen [12] frames deep number-theoretic conjectures, including the Riemann Hypothesis, as statements about the indistinguishability of arithmetic functions from random sequences.

Wigderson [13, 14] has explicitly drawn parallels between pseudorandomness in complexity theory and randomness phenomena in number theory, suggesting a shared conceptual foundation.

3. Contribution and Positioning

While prior work has identified and refined individual barriers, no existing framework unifies relativization, natural proofs, and algebrization under a single formal principle. Each barrier has traditionally been studied in isolation or via pairwise comparisons.

This work provides the first unified framework that:

- Models proof techniques abstractly as collections of bounded observers,
- Defines all known barriers as instances of indistinguishability from pseudorandomness,
- Proves a single universal barrier theorem from which relativization, natural proofs, and algebrization follow as corollaries,
- Formally derives the known hierarchy among barriers,
- Is fully mechanized and verified in the Lean proof assistant.

In contrast to previous approaches, which classify techniques syntactically or via oracle access, our framework is semantic: it characterizes proof power in terms of the ability to distinguish structure from pseudorandomness. This observer-based perspective subsumes classical barriers and connects them to cryptography, learning theory, and analytic number theory.

To our knowledge, no prior work provides a machine-verified, observer-centric unification of all major complexity-theoretic barriers. This positions the present work as both a synthesis of existing insights and a foundational step toward a more general theory of proof limitations in complexity theory.

4. Overview of the Framework

4.1. Boolean Functions and Circuits

We work with Boolean functions $f : \{0, 1\}^n \rightarrow \{0, 1\}$, represented extensionally by their truth tables. Standard notions of circuit size, polynomial bounds, and explicitness are assumed.

Circuit lower bounds are expressed using predicates such as:

$$\text{HasPolyCircuits}(f), \quad \text{RequiresSuperPolyCircuits}(f).$$

4.2. Observers and Observer Classes

An *observer* is an abstract distinguisher that:

- Takes a Boolean function as input,
- Computes a statistic,
- Attempts to distinguish the function from uniform randomness.

An *observer class* is a set of observers subject to resource constraints.

We define three fundamental observer classes:

- **Query-bounded observers:** limited oracle access (relativization),
- **Degree-bounded observers:** low-degree algebraic tests (algebrization),
- **Polynomial-time observers:** efficient distinguishers (natural proofs).

These classes form a strict hierarchy.

4.3. Formalizing Resource Bounds

A natural question arises: what prevents an “observer” from simply encoding the entire truth table, making every function trivially distinguishable?

In our Lean formalization, each observer carries explicit resource fields with semantic constraints:

```
structure BoundedObserver (n : Nat) where
  observe : BoolFun n -> Real
  randomExpectation : Real
  bound : Nat
  queryComplexity : Nat
  algebraicDegree : Nat
  timeComplexity : Nat
  -- Semantic constraints:
  query_degree_bound : algebraicDegree <= queryComplexity + 1
  degree_time_bound : timeComplexity <= (n + 1)^(algebraicDegree + 1)
  bound_ge_time : bound >= timeComplexity
```

Key design choices:.

1. **Nonuniform model.** Observers are modeled as nonuniform function families, akin to circuit families. This matches the standard treatment of natural proofs, where the “constructivity” condition refers to polynomial-size circuits, not uniform algorithms.
2. **Resource constraints are enforced.** An observer claiming `timeComplexity = T` must satisfy $T \leq (n+1)^k$ to belong to $\text{PolyTimeObservers}(n, k)$. An observer reading the entire truth table would require $T = 2^n$, violating polynomial bounds for all fixed k .
3. **The hierarchy is proven, not axiomatized.** The inclusion $\text{QueryBounded}(q) \subseteq \text{DegreeBounded}(q+1)$ follows from $\text{algebraicDegree} \leq \text{queryComplexity} + 1$.
 1. No additional axioms are needed.

Concrete example: A query-bounded observer.. Consider an observer that queries a Boolean function $f : \{0, 1\}^n \rightarrow \{0, 1\}$ at a fixed point x_0 and

outputs $f(x_0)$:

```
observe(f) = f(x₀)
randomExpectation = 1/2
queryComplexity = 1
algebraicDegree = 1
timeComplexity = 1
```

This observer belongs to $\text{QueryBounded}(1)$, $\text{DegreeBounded}(2)$, and $\text{PolyTime}(k)$ for any $k \geq 1$. It distinguishes any function f with $f(x_0) \neq 1/2$ —but a pseudorandom function, by definition, must satisfy $|f(x_0) - 1/2| < \varepsilon$ for small ε against any polynomial-size family of such observers.

What this prevents.. An “observer” that tries to compute the entire truth table would have $\text{timeComplexity} = 2^n$, which exceeds $(n + 1)^k$ for any fixed k when n is large. Such an observer cannot belong to any polynomial-time observer class, so it is excluded from the natural proofs barrier.

This is precisely the content of the natural proofs barrier: if an observer could efficiently distinguish hard functions from random, PRFs could not exist.

4.4. Pseudorandomness

A Boolean function f is *pseudorandom relative to an observer class \mathcal{O}* if no observer in \mathcal{O} can distinguish f from random with non-negligible advantage.

This definition is intentionally minimal and technique-agnostic.

5. Proof Techniques as Observer-Bounded Objects

We model a *proof technique* as:

- A set of observers it implicitly uses,
- A soundness condition certifying a separation,
- A boundedness condition relative to an observer class.

This abstraction allows us to reason about entire families of proofs rather than individual arguments.

6. The Unified Barrier Theorem

We now state our main result precisely. First, we fix notation.

Definition 6.1 (Observer Class). An *observer class* \mathcal{O}_n is a set of functions $\text{obs} : \{0,1\}^{2^n} \rightarrow \mathbb{R}$ (taking truth tables as input) equipped with a bound $B(\text{obs})$.

Definition 6.2 (Pseudorandomness). A Boolean function $f : \{0,1\}^n \rightarrow \{0,1\}$ is ε -pseudorandom to \mathcal{O}_n if for all $\text{obs} \in \mathcal{O}_n$:

$$|\text{obs}(f) - \mathbb{E}_{g \sim \mathcal{U}}[\text{obs}(g)]| < \varepsilon$$

where \mathcal{U} is the uniform distribution over Boolean functions.

Definition 6.3 (Proof Technique). A *proof technique* T relative to observer class \mathcal{O}_n consists of:

- A predicate $\text{Cert}_T(f)$ asserting that T “certifies” f as hard (e.g., requires super-polynomial circuits),
- A *soundness requirement*: if $\text{Cert}_T(f)$ holds, then there exists $\text{obs} \in \mathcal{O}_n$ such that $|\text{obs}(f) - \mathbb{E}[\text{obs}]| \geq 1/B(\text{obs})$.

The soundness requirement captures the intuition that any proof technique must implicitly distinguish the hard function from random functions—otherwise, how could it identify the function as “special”?

Theorem 6.4 (Observer Barrier—Formal Statement). *Let \mathcal{O}_n be an observer class and let T be a proof technique relative to \mathcal{O}_n . If f is $(1/B)$ -pseudorandom to \mathcal{O}_n for all observers with bound B , then $\neg\text{Cert}_T(f)$.*

Proof. Suppose $\text{Cert}_T(f)$. By soundness, there exists $\text{obs} \in \mathcal{O}_n$ with $|\text{obs}(f) - \mathbb{E}[\text{obs}]| \geq 1/B(\text{obs})$. But f is $(1/B(\text{obs}))$ -pseudorandom to \mathcal{O}_n , so $|\text{obs}(f) - \mathbb{E}[\text{obs}]| < 1/B(\text{obs})$. Contradiction. \square

Remark 6.1 (Conditional Nature). The theorem is *unconditional* as a logical implication. The *assumption* that pseudorandom functions exist against \mathcal{O}_n is what makes it non-trivial. For $\mathcal{O}_n = \text{PolyTime}$, this assumption is the standard cryptographic hypothesis that PRFs exist.

Remark 6.2 (What “Certification” Means). The predicate $\text{Cert}_T(f)$ is abstract. In applications:

- For circuit lower bounds: $\text{Cert}_T(f)$ means “ T proves f requires circuits of size $> n^{\omega(1)}$ ”

- For P vs NP: $\text{Cert}_T(f)$ means “ T proves that the language defined by f is not in P”

The theorem applies to any such predicate satisfying the soundness requirement.

Remark 6.3 (Why Not Quantify Over “Property Classes”?). One might attempt a formulation like: “If $\{f_n\}$ is pseudorandom against \mathcal{O} and has property P , then no \mathcal{O} -bounded proof can show all functions with property Q require super-polynomial circuits.” This is less precise because:

1. It conflates *existence* of pseudorandom functions with *properties* of proof techniques. Our formulation separates these cleanly.
2. The relationship between P and Q is unspecified. In Razborov-Rudich, the key is that a *single* property must be both useful (implies hardness) and large (many functions satisfy it). Our “soundness requirement” captures this directly.
3. “Super-polynomial circuit size” is specific to natural proofs. Relativization concerns oracle separations; algebraization concerns algebraic proof barriers. Our abstract $\text{Cert}_T(f)$ predicate generalizes across all barrier types.

The present formulation applies uniformly to all three barriers without modification.

This theorem is proved once in Lean and instantiated to recover each classical barrier.

7. Recovering Classical Barriers

7.1. Relativization

Relativizing techniques are bounded by query-limited observers. If pseudorandom functions fool such observers, relativizing proofs fail.

7.2. Algebraization

Algebraizing techniques are bounded by low-degree observers. Degree-pseudorandomness blocks all such methods.

7.3. Natural Proofs: A Complete Derivation

We now show in detail how the Razborov-Rudich natural proofs barrier follows as a corollary of the Observer Barrier Theorem.

7.3.1. The Razborov-Rudich Framework (1997)

Razborov and Rudich [2] define a *natural proof* against a circuit class \mathcal{C} as a property \mathcal{P} of Boolean functions satisfying:

1. **Constructivity:** There exists a polynomial-size circuit family that, given the truth table of f , decides whether $f \in \mathcal{P}$.

2. **Largeness:** A non-negligible fraction of all Boolean functions satisfy \mathcal{P} :

$$\Pr_{f \sim \mathcal{U}}[f \in \mathcal{P}] \geq 2^{-O(n)}$$

3. **Usefulness:** Every $f \in \mathcal{P}$ requires super-polynomial circuits:

$$f \in \mathcal{P} \implies f \notin \mathcal{C}$$

Razborov-Rudich Theorem: If pseudorandom function families exist against polynomial-size circuits, then no natural proof can establish super-polynomial circuit lower bounds against \mathbf{P}/poly .

7.3.2. Translation to Observer Framework

We now translate each component:

Step 1: Constructivity \Rightarrow Polynomial-time observer.. Let \mathcal{P} be a constructive property with deciding circuit of size $s(n) = n^c$. Define an observer:

$$\begin{aligned} \text{observe}_{\mathcal{P}}(f) &= \mathbf{1}[f \in \mathcal{P}] \in \{0, 1\} \\ \text{timeComplexity} &= s(n) = n^c \end{aligned}$$

Since $s(n)$ is polynomial, we have $\text{observe}_{\mathcal{P}} \in \text{PolyTimeObservers}(n, c)$.

Step 2: Largeness \Rightarrow Non-trivial random expectation.. Let $\delta = \Pr_{f \sim \mathcal{U}}[f \in \mathcal{P}]$. By largeness, $\delta \geq 2^{-O(n)}$. The random expectation is:

$$\mathbb{E}_{f \sim \mathcal{U}}[\text{observe}_{\mathcal{P}}(f)] = \delta$$

Step 3: Usefulness \Rightarrow Soundness requirement.. Suppose a proof technique T uses \mathcal{P} to certify hardness. That is:

$$\text{Cert}_T(f) \iff f \in \mathcal{P}$$

If $f \in \mathcal{P}$, then:

$$|\text{observe}_{\mathcal{P}}(f) - \mathbb{E}[\text{observe}_{\mathcal{P}}]| = |1 - \delta| = 1 - \delta$$

Since δ is small ($\leq 1/2$ for typical properties), this gives distinguishing advantage $\geq 1/2$.

This establishes the soundness requirement: if $\text{Cert}_T(f)$, then $\text{observe}_{\mathcal{P}}$ distinguishes f from random.

7.3.3. Derivation of Natural Proofs Barrier

Theorem 7.1 (Natural Proofs Barrier—Derived). *If there exists f that is $(1/B)$ -pseudorandom to $\text{PolyTimeObservers}(n, k)$ for all k , then no natural proof can certify that f requires super-polynomial circuits.*

Proof. Let \mathcal{P} be a natural property (constructive, large, useful). We apply Theorem 6.4:

1. **Observer class:** $\mathcal{O}_n = \text{PolyTimeObservers}(n, k)$ for k such that the constructivity circuit has size $\leq n^k$.
2. **Observer:** $\text{observe}_{\mathcal{P}} \in \mathcal{O}_n$ (by constructivity).
3. **Proof technique:** T uses \mathcal{P} , with $\text{Cert}_T(f) \iff f \in \mathcal{P}$.
4. **Soundness:** If $f \in \mathcal{P}$, then $|\text{observe}_{\mathcal{P}}(f) - \mathbb{E}[\text{observe}_{\mathcal{P}}]| \geq 1/2$ (by largeness + usefulness).
5. **Pseudorandomness assumption:** f is pseudorandom to \mathcal{O}_n .

By Theorem 6.4, $\neg\text{Cert}_T(f)$, i.e., $f \notin \mathcal{P}$.

Since \mathcal{P} was arbitrary, no natural property \mathcal{P} contains f . Hence no natural proof certifies that f is hard. \square

7.3.4. Connection to Cryptographic Assumption

The Razborov-Rudich theorem requires pseudorandom function families (PRFs) to exist against polynomial-size circuits. The Goldreich-Goldwasser-Micali (GGM) construction [3] shows:

One-way functions exist \Rightarrow PRFs exist against PolyTime

Combining with our derivation:

OWFs exist \Rightarrow PRFs exist \Rightarrow Observer Barrier for PolyTime \Rightarrow Natural Proofs Barrier

This chain is fully formalized in Lean, with the PRF assumption as the only external hypothesis.

7.3.5. What This Derivation Shows

The natural proofs barrier is *not* a separate phenomenon from the observer barrier—it *is* the observer barrier instantiated to polynomial-time observers. The Razborov-Rudich conditions (constructivity, largeness, usefulness) are exactly what is needed to construct a poly-time observer satisfying our soundness requirement.

In Lean, this is captured by definitional equality:

```
theorem natural_proofs_barrier :=  
  observer_barrier (PolyTimeObservers n k) f hPR
```

8. Barrier Hierarchy and Strength

We formally derive the hierarchy:

$$\text{Relativizing} \subseteq \text{Algebrizing} \subseteq \text{Natural}.$$

As a consequence, breaking the natural proofs barrier is necessary for breaking the others.

9. Applications Beyond Complexity Barriers

The observer-pseudorandomness framework extends naturally to other domains where bounded observers interact with structured objects.

9.1. Connection to Learning Theory

Carmosino, Impagliazzo, Kabanets, and Kolokolova [16] established a surprising equivalence between natural proofs and PAC learning:

Natural proofs exist against circuit class \mathcal{C} if and only if \mathcal{C} is PAC-learnable.

Our framework explains *why* this equivalence holds: both natural proofs and learning reduce to the same underlying capability—**distinguishing from random**.

9.1.1. Learning as Distinguishing

A PAC learner for circuit class \mathcal{C} must, given random examples from a target function $f \in \mathcal{C}$, output a hypothesis h that approximates f . The key observation:

A successful learner implicitly *distinguishes* functions in \mathcal{C} from random functions.

If f were indistinguishable from random, no learner could find structure to exploit. The learner's success depends on detecting non-random patterns.

9.1.2. Natural Proofs as Distinguishing

A natural proof uses a property \mathcal{P} that is:

- **Constructive:** Efficiently checkable (= poly-time observer)
- **Large:** Satisfied by many functions (= non-trivial random expectation)
- **Useful:** Implies hardness (= soundness requirement)

The proof succeeds by *distinguishing* hard functions (in \mathcal{P}) from random functions (mostly not in \mathcal{P}).

9.1.3. The Unified View

In our framework, both reduce to the existence of a polynomial-time observer that distinguishes \mathcal{C} -functions from random:

Capability	Observer	What it distinguishes
Learning \mathcal{C}	Learner	\mathcal{C} from random
Natural proof against \mathcal{C}	Property tester	Hard functions from random

If pseudorandom functions exist against poly-time observers, *both* capabilities are blocked simultaneously. This is why the Carmosino equivalence holds: natural proofs and learning are two manifestations of the same phenomenon.

Our Lean formalization captures this connection in `Applications/CarmosinoEquivalence.lean`, proving:

```
theorem carmosino_from_observer_barrier :
  (Exists f, IsPseudorandomTo f (PolyTimeObservers n k)) ->
  Exists f, Not (NaturalProofsExist C k) /\ Not (IsLearnable C k)
```

Note: We formalize the *existential* equivalence, not the constructive algorithm from the original paper.

9.2. Connection to Control Theory

The observer framework connects to a classical result in control theory: Kalman's observability theory [17].

9.2.1. Linear Systems and Observability

Consider a discrete-time linear system:

$$\begin{aligned} x_{t+1} &= Ax_t \\ y_t &= Cx_t \end{aligned}$$

where $x_t \in \mathbb{R}^n$ is the state and $y_t \in \mathbb{R}^m$ is the output.

A system is *observable* if the initial state x_0 can be uniquely determined from the output sequence $(y_0, y_1, \dots, y_{n-1})$.

9.2.2. Observability as Distinguishing

Kalman's observability criterion states:

A system is observable iff the *unobservable subspace* is trivial (contains only zero).

The unobservable subspace consists of states that produce zero output for all time—states that are *indistinguishable from zero* by any output measurement.

9.2.3. The Pseudorandomness Connection

We prove in `Applications/ControlTheoryBridge.lean`:

Theorem 9.1 (Observability Bridge). *A linear system is observable if and only if no non-zero state is pseudorandom to output observers.*

Here, an *output observer* is a linear functional computed from the output sequence:

$$\text{obs}(x_0) = \sum_{t=0}^{n-1} \langle c_t, y_t \rangle$$

A state x is *pseudorandom to output observers* if $\text{obs}(x) = \text{obs}(0)$ for all such observers—i.e., x is indistinguishable from zero.

Proof sketch. (\Rightarrow) If observable, distinct states produce distinct outputs. Hence no non-zero state equals zero on all observers.

(\Leftarrow) If some non-zero x is pseudorandom (indistinguishable from 0), then x and 0 produce identical outputs, violating observability. \square

9.2.4. Cross-Domain Analogy

The mathematical structure is identical across domains:

Domain	Observer Class	Pseudorandom Object	Consequence
Complexity	Query-bounded	Hard function	Cannot prove separation
Complexity	Degree-bounded	Hard function	Cannot prove separation
Complexity	Poly-time	Hard function	Cannot prove separation
Control	Output observers	Unobservable state	Cannot identify state

In all cases: **bounded observers cannot detect structure in pseudorandom objects.**

This connection suggests that the observer-pseudorandomness paradigm may have broader applicability beyond complexity theory.

10. Implications for P vs. NP

Our framework yields a precise constraint:

Any proof of $\mathbf{P} \neq \mathbf{NP}$ must either break the natural proofs barrier or exploit non-pseudorandom structure beyond polynomial-time distinguishability.

This statement is proved formally and does not rely on informal intuition.

11. Formal Verification

All definitions and theorems are mechanized in Lean 4 with Mathlib. This includes:

- Observer hierarchies,
- Pseudorandomness properties,
- Barrier implications,
- Meta-theorems about proof techniques.

To our knowledge, this is the first machine-verified unification of complexity-theoretic barriers.

Code Availability.. The complete Lean formalization is available at:

<https://github.com/dennj/Pseudorandomness>

12. Conclusion

We have shown that relativization, algebrization, and natural proofs are not separate obstructions, but instances of a single phenomenon rooted in pseudorandomness. By formalizing this insight, we provide a clearer roadmap for future lower-bound research and a rigorous explanation for decades of stalled progress.

References

- [1] T. Baker, J. Gill, R. Solovay, Relativizations of the $\mathbf{P} =? \mathbf{NP}$ question, *SIAM Journal on Computing*, 4(4):431–442, 1975.
- [2] A. Razborov, S. Rudich, Natural proofs, *Journal of Computer and System Sciences*, 55(1):24–35, 1997.
- [3] O. Goldreich, S. Goldwasser, S. Micali, How to construct random functions, *Journal of the ACM*, 33(4):792–807, 1986.
- [4] S. Aaronson, A. Wigderson, Algebrization: A new barrier in complexity theory, *ACM Transactions on Computation Theory*, 1(1), 2009.
- [5] R. Impagliazzo, V. Kabanets, A. Kolokolova, An axiomatic approach to algebrization, *Proceedings of STOC*, 2009.
- [6] E. Aydinlioglu, E. Bach, Affine relativization: Unifying the algebrization and relativization barriers, *Electronic Colloquium on Computational Complexity*, TR17-111, 2017.
- [7] S. Hirahara, L. Lu, J. Ren, Bounded relativization, *Electronic Colloquium on Computational Complexity*, TR23-083, 2023.
- [8] B. Green, On (not) computing the Möbius function using bounded depth circuits, *Combinatorics, Probability and Computing*, 21(6):942–953, 2012.
- [9] B. Green, T. Tao, The Möbius function is strongly orthogonal to nilsequences, *Annals of Mathematics*, 175(2):541–566, 2012.
- [10] P. Sarnak, Möbius randomness and dynamics, *Notices of the South African Mathematical Society*, 43(2):89–97, 2012.
- [11] A. Granville, K. Soundararajan, Pretentious multiplicative functions and analytic number theory, *preprint / monograph in preparation*.

- [12] T. Tao, J. Teräväinen, Quantitative bounds for Gowers uniformity of the Möbius and von Mangoldt functions, *Annals of Mathematics*, to appear, 2023.
- [13] A. Wigderson, Randomness and pseudorandomness, IAS Lecture Notes, 2009.
- [14] A. Wigderson, *Mathematics and Computation*, Princeton University Press, 2019.
- [15] S. Vadhan, Pseudorandomness, *Foundations and Trends in Theoretical Computer Science*, 7(1–3), 2012.
- [16] M. Carmosino, R. Impagliazzo, V. Kabanets, A. Kolokolova, Learning algorithms from natural proofs, *Proceedings of the 31st Conference on Computational Complexity (CCC)*, 10:1–10:24, 2016.
- [17] R.E. Kalman, Mathematical description of linear dynamical systems, *SIAM Journal on Control*, 1(2):152–192, 1963.