$\mathbf{APX_1}$: A Brief Tutorial & Recent Developments

Igor Oliveira

Based on joint work with {**L. Chen, J. Li, R. Williams**} and {**O. Korten, J. Li, H. Ren**}

Logical Foundations of Complexity Theory

Isaac Newton Institute for Mathematical Sciences

October 19, 2026

Summary of the Talk

- Why? Motivation for $\mathbf{APX_1}$
- Axioms for approximate counting
- Probabilistic reasoning in $\mathbf{APX_1}$ & formalization of advanced results
- Relation to other theories & unprovability

(see the papers for **witnessing theorems** and **reverse mathematics**)

Organization

Prelude: Quick Recap of Bounded Arithmetic

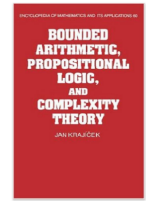
Part I: Theory APX_1

Part II: Feasible Probabilistic Reasoning

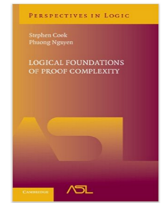
Part III: Pigeonhole Principles and Unprovability in APX_1

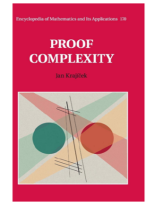
Bounded Arithmetic





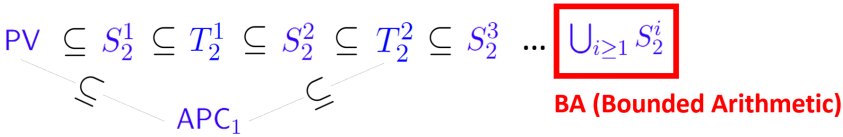
Fragments of Peano Arithmetic capturing proofs that manipulate concepts from a given complexity class.





A few notable examples:

- Cook's theory **PV** (1975), which formalizes **poly-time reasoning**
- Buss's theories $\mathbf{S}_2^i$ and $\mathbf{T}_2^i$ (1986), corresponding to the **levels of the polynomial hierarchy**
- Jeřábek's theory $\mathbf{APC}_1$ (2007) is sufficient for **probabilistic poly-time reasoning**



Several results from Algorithms & Complexity can be formalized in BA:

Randomized Matching Algorithms in APC_1 [TriManLe-Cook'11].

PCP Theorem in PV [Pich'15].

Parity $\notin \mathsf{AC}^0$ and k-Clique $\notin \mathsf{mSIZE}[n^{\sqrt{k}/100}]$ in APC_1 [Muller-Pich'19].

PIT $\in \mathsf{SIZE}[\mathrm{poly}]$ in T_2^2 [Atserias-Tzameret'25].

Dijkstra's Shortest Path Algorithm and Kruskal's Minimum Spanning Tree Algorithm in PV (Li'25).



Survey

"Meta-Mathematics of Complexity Theory"

Published March/2025

Cook's Theory PV (1975)

- Introduced by S. Cook as a **theory for polynomial-time reasoning**
- Function symbols for all poly-time algorithms (with axioms relating them) & induction for quantifier-free formulas
- Robust to different formalizations:
  - Equations via Cobham's characterization of poly-time
  - $\forall\Sigma_1^b$ fragment of Buss's theory S_2^1
  - **Jeřábek's formulation as T_2^0 over an extended language (next slide)**

PV (Jeřábek's Equivalent Formulation as T^0_2)

Intended model:

Natural numbers $\langle \mathbb{N}, 0^{\mathbb{N}}, S^{\mathbb{N}}, +^{\mathbb{N}}, \cdot^{\mathbb{N}}, \dots \rangle$

first-order language

$L = \langle 0, S, +, \cdot, \le, \#, |x|, \lfloor \frac{x}{2^y} \rfloor \rangle$

Intended meaning of the symbols:

$|x| = \lceil \log_2(x+1) \rceil \qquad x \# y = 2^{|x||y|}$

$\lfloor \frac{x}{2^y} \rfloor$ removes the y less significant bits of x

PV is a theory in the language L, axiomatized by the induction schema (IND)

$$\varphi(0) \wedge \forall x\,(\varphi(x) \to \varphi(Sx)) \to \forall x\,\varphi(x)$$

for Σ^b_0-formulas φ, and the following formulas:

$x + 0 = x$	$x + Sy = S(x + y)$
$x \cdot 0 = 0$	$x \cdot Sy = x \cdot y + x$
$0 \le x$	$Sy \le x \leftrightarrow y < x$
$\lfloor \frac{x}{2^0} \rfloor = x$	$\lfloor \frac{x}{2^{Sy}} \rfloor = 2\lfloor \frac{x}{2^{Sy}} \rfloor \vee \lfloor \frac{x}{2^y} \rfloor = S(2\lfloor \frac{x}{2^{Sy}} \rfloor)$
$\lvert 0 \rvert = 0$	$x \ne 0 \to \lvert x \rvert = S\lvert \lfloor \frac{x}{2} \rfloor \rvert$
$0 \# 1 = 1$	$x \ne 0 \to x \# 1 = 2(\lfloor \frac{x}{2} \rfloor \# 1) \wedge (y \# x) = (y \# 1)(y \# \lfloor \frac{x}{2} \rfloor)$

where $x < y$, $\lfloor \frac{x}{2} \rfloor$, 1, 2 are abbreviations for $x \le y \wedge x \ne y$, $\lfloor \frac{x}{2^1} \rfloor$, $S0$, $SS0$, respectively.

Bounded quantifiers & sharply bounded quantifiers:

$\exists x \le t\,\varphi \Leftrightarrow \exists x\,(x \le t \wedge \varphi),$

$\forall x \le t\,\varphi \Leftrightarrow \forall x\,(x \le t \to \varphi),$

where t is a term with no occurrence of x. A bounded quantifier is *sharply bounded*, if its bounding term t is of the form $|s|$. A formula φ is (sharply) bounded if all quantifiers in φ are (sharply) bounded. The set of all sharply bounded formulas is denoted by Σ^b_0.

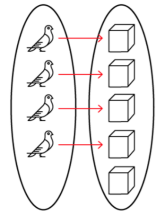
Jeřábek's Theory APC_1 (2007)

- Given $S \subseteq \{0,1\}^n$ defined by a circuit, how to express statements like $\Pr_x[x \in S] \leq 1/2$?
- **APC_1**: Extension of **PV** suitable for approx. counting and probabilistic reasoning
- **Idea:** $|S| \leq |T|$ if there is a surjection $T \twoheadrightarrow S$
- More formally, for definable sets $S, T \subseteq \{0,1\}^n$ and $\varepsilon \geq 0$,

$$S \preceq_\varepsilon T \quad \text{iff} \quad \text{there is } v > 0 \text{ and a circuit } C\colon [v] \times (T \mathbin{\dot\cup} [\varepsilon 2^n]) \twoheadrightarrow [v] \times S$$

- We write $S \approx_\varepsilon T$ when $S \preceq_\varepsilon T$ and $T \preceq_\varepsilon S$

Theory APC_1



Extension of PV with axioms dWPHP(f) for each $f \in \mathcal{L}_{\mathsf{PV}}$

dWPHP(f) : "If f maps 2^n pigeons to $2^n(1+1/n)$ holes, there is an empty hole."

$$\mathsf{PV} \subseteq S_2^1 \subseteq T_2^1 \subseteq S_2^2 \subseteq T_2^2 \subseteq S_2^3 \quad \dots \quad \bigcup_{i\geq 1} S_2^i$$

$$\mathsf{APC}_1$$

Jerabek (2007) showed the following result:

$\mathbf{APC_1}$ $\vdash$ "For every definable set X and $\varepsilon > 0$, there is s such that $X \approx_\varepsilon [s]$"

Organization

Prelude: Quick Recap of Bounded Arithmetic

Part I: Theory $\mathbf{APX_1}$

Part II: Feasible Probabilistic Reasoning

Part III: Pigeonhole Principles and Unprovability in APX_1

Overview

- For nearly 20 years, $\mathbf{APC_1}$ has been the standard weak theory for the formalization of TCS proofs that rely on **probabilities** (random variables, probabilistic method, ...)

- However, $\mathbf{APC_1}$ uses a powerful counting principle (**dWPHP**)
  Potentially stronger than needed

- We propose the theory $\mathbf{APX_1}$: a weaker bounded arithmetic theory serving as a **base theory** for **"probabilistic polynomial-time reasoning"**

Why weaken APC_1?

- **Philosophical:** Want probabilities but dWPHP axiom might not be "feasible" [ILW'23]: Given $C\colon \{0,1\}^n \to \{0,1\}^{n+1}$, how to find/certify y such that, for all x, $C(x) \neq y$?
- **Unprovability of complexity-theoretic conjectures:** Want an appropriate theory, but not more: strong axioms complicate unprovability arguments.
- **Reverse mathematics of TCS:** understand minimal axioms required to prove theorems. APC_1 is an overly powerful base theory for correspondences weaker than dWPHP.
- **Applications in cryptography:** Recent line of work connecting bounded arithmetic and the construction of cryptographic primitives ([Hsieh-Jain-Li-Mathialagan'26], ...).
- **Proof complexity of derandomization:** Can we formulate and study the feasible provability of prBPP = prP?

Comparing PV, APX_1, and APC_1

- **PV** formalizes p-time functions + induction for poly-time predicates.
- $\mathbf{APC_1} = \mathbf{PV} + \mathbf{dWPHP}(\mathrm{PV})$, provides approx. counting and probabilistic reasoning.
- **dWPHP** plays two roles:

  (i) enables approximate counting: every p-time definable set has a size.
  (ii) acts as a strong counting principle to prove probability inequalities.

Key Design Principle for $\mathbf{APX_1}$: Approximate counting as a central primitive (rather than deriving it from a stronger pigeonhole principle).

Computational perspective

$$\mathbf{PV} \lesssim \mathbf{APX_1} \lesssim \mathbf{APC_1}$$

deterministic polytime

det. polytime + **CAPP**

" prBPP $\subseteq$ prP "

det. polytime + **Range Avoidance**

" $\exists f \notin \mathrm{SIZE}[2^{\varepsilon n}]$ "

APX_1 in one slide: The approximate counting oracle P

- Extend the language of PV with a new function symbol $P(C, \Delta)$.
- Inputs: Boolean circuit $C : \{0,1\}^n \to \{0,1\}$ and a precision parameter Δ.
- Intended meaning: $P(C, \Delta)$ provides a rational approximation to

$$p(C) \triangleq \mathbb{P}_{x \leftarrow \{0,1\}^n}[C(x) = 1]$$

  within additive error $\delta \approx 1/|\Delta|$.

  (For convenience, we often write $P_\delta(C)$ for $P(C, \Delta)$, where $\delta = 1/|\Delta|$.)

- Add **"simple axioms"** that force P_δ to behave like "counting over the hypercube" **(?)**

Axioms for P_δ

Axioms are universal PV(P)-equations; $\beta^{-1} \in \mathrm{Log}$ is a "slack parameter" (think of it as $o(1)$).

1. **Basic Axiom:** $P_\delta(C)$ is a rational in $[0,1]$ (with feasibility/output-length bounds).
2. **Boundary Axiom:** if C is syntactically constant then $P_\delta(C) \in \{0,1\}$ and matches C.
3. **Precision Consistency:** for any precision parameters $\delta_1^{-1}, \delta_2^{-1}, \beta^{-1} \in \mathrm{Log}$,

$$|P_{\delta_1}(C) - P_{\delta_2}(C)| \leq \delta_1 + \delta_2 + \beta.$$

4. **Local Consistency:** if C has input variables and $\mathrm{Fix}_b(C)$ fixes the last bit to b,

$$\left|P_\delta(C) - \tfrac{1}{2}\left(P_\delta(\mathrm{Fix}_0(C)) + P_\delta(\mathrm{Fix}_1(C))\right)\right| \leq 2\delta + \beta.$$

Remarks

$\mathbf{APX_1}$ extends the language of PV with the new function symbol $P(C, \Delta)$.

Cobham's axioms: $P(C, \Delta)$ can be used when introducing new function symbols.

Over the standard model $\mathbb{N}$, $\mathbf{APX_1}$ functions correspond to $\mathrm{FP}^{P(\cdot)}$ computations.

$P(C, \Delta)$ can **only** be applied to (standard) circuits: not to P-oracle circuits.

Soundness / correctness of the axioms

- Let $\mathbb{N}$ be the standard model of PV. Consider a length-bounded $[0,1]$-valued interpretation $\widetilde{P}$ of $P(C,\Delta)$ as a correct approximate counting procedure

$$\widetilde{P}(C,\Delta) \ \in p(C) \pm 1/|\Delta|$$

  that is exact on syntactically constant circuits. Then $\langle \mathbb{N}, \widetilde{P} \rangle$ is a model of APX_1.

- Conversely, if $\langle \mathbb{N}, \widehat{P} \rangle$ is a model of APX_1, then

$$\mathbb{N} \models \widehat{P}(C,\Delta) \ \in p(C) \pm 1/|\Delta|.$$

- **Consequence:** the axioms characterize the intended notion of **approximate counting** (over the standard model $\mathbb{N}$).

Organization

Prelude: Quick Recap of Bounded Arithmetic

Part I: Theory APX_1

Part II: Feasible Probabilistic Reasoning

Part III: Pigeonhole Principles and Unprovability in APX_1

Probabilistic toolkit in APX_1

From the axioms, APX_1 derives:

- **Invariance principles (P_δ behaves well):**
  - semantic invariance (equivalent circuits have close P_δ values),
  - permutation invariance (relabelling inputs barely changes P_δ).
- **Probabilistic method:** if $P_\delta(C) \geq \delta + \beta$ for some $\delta^{-1}, \beta^{-1} \in \mathsf{Log}$ then $\exists x\, C(x) = 1$.
- Useful notions for **events**, **random variables** and **expectation**.
- **Standard inequalities in approximate form:** union bound, Markov, Chebyshev, one-sided error reduction, restricted version of the Chernoff bound, among other results.

Example: Feasible random variables and approximate expectation

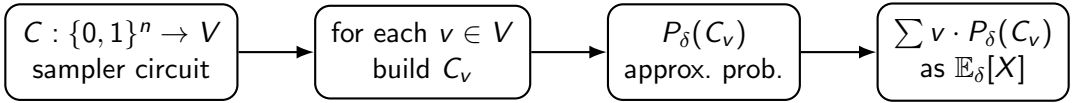
A **feasible random variable** X is specified by:

$$X = (V, n, C), \qquad C : \{0,1\}^n \to V \subseteq \mathbb{Q},$$

where V is an explicit set of size $\mathrm{poly}(n)$.

Consider **indicator circuits** $C_v(x) \triangleq \mathbb{1}[C(x) = v]$, and define **approximate expectation**:

$$\mathbb{E}_\delta[X] \triangleq \sum_{v \in V} v \cdot P_\delta(C_v).$$



Formalizing TCS theorems in APX_1

APX_1 is strong enough to formalize several nontrivial results, including:

- **Yao's distinguisher-to-predictor transformation.**
- **Schwartz–Zippel lemma** (via the alternative proof technique from [AT'25]).
- **Blum–Luby–Rubinfeld (BLR) linearity testing.**
- **Circuit lower bounds:** average-case AC^0 lower bounds for parity.

Upshot: APX_1 enables probabilistic reasoning **without relying on a pigeonhole principle**.

Example: Parity vs AC^0

- **Average-case lower bound in $\mathbf{APX_1}$.** For constants $k, d \geq 1$, $\mathbf{APX_1}$ proves:
  For every $n \in \mathrm{Log}$, any depth-d AC^0 circuit C of size $\leq n^k$ agrees with $\oplus_n$ on at most

$$\tfrac{1}{2} + \tfrac{1}{n^k} + \delta + \beta$$

  fraction of inputs (measured via P_δ using circuit $T_C(x) \triangleq \mathbb{1}[C(x) = \oplus_n(x)]$).

As a byproduct of our refined treatment of AC^0 circuits in bounded arithmetic, we also show:

- **Worst-case lower bound in PV.** For constants $k, d \geq 1$, **PV** proves:
  For every $n \in \mathrm{Log}$ and depth-d AC^0 circuit C of size $\leq n^k$,

$$\exists x \in \{0,1\}^n \text{ such that } C(x) \neq \oplus_n(x).$$

Previous formalizations used pigeonhole principles and were only known in $\mathbf{APC_1}$ [K'95, MP'20].

The $\mathbf{APX_1}$ proof precisely isolated what needed to be accomplished in **PV**.

From Local Consistency to Probabilistic Reasoning:

A Useful Technique

The pointwise-to-global technique

Consider Boolean circuits $C_1, C_2 \colon \{0,1\}^n \to \{0,1\}$, where $C_1 \triangleq \neg C_2$.

Q. Does APX_1 prove that complementation is consistent, i.e., $P_\delta(C_1) + P_\delta(C_2) \approx 1$?

Not obvious: $P_\delta(\cdot)$ satisfies **"consistency"** constraints, while this statement is **"global"**.

The **pointwise-to-global technique** allows us to connect a global statement to a local, pointwise statement:

For **every fixed string** $a \in \{0,1\}^n$, let $C[a]$ be circuit C fixed (hardwired) with input a.

Using the **boundary axiom**, $\mathrm{APX}_1 \vdash P_\delta(C_1[a]) + P_\delta(C_2[a]) = 1$.

Therefore, the desired statement holds **pointwise**.

The pointwise-to-global technique, cont'd

Now to an example of a **global consequence**: Suppose towards a contradiction that

$$P_\delta(C_1) + P_\delta(C_2) \leq 0.99.$$

By **local consistency** of $P_\delta(\cdot)$ and **averaging**, we can fix variable x_n to a bit a_n such that:

$$P_\delta(\mathrm{Fix}_{a_n}(C_1)) + P_\delta(\mathrm{Fix}_{a_n}(C_2)) \lesssim P_\delta(C_1) + P_\delta(C_2).$$

Repeating n times, we get a fixed string $a \in \{0,1\}^n$ such that:

$$P_\delta(C_1[a]) + P_\delta(C_2[a]) \lesssim P_\delta(C_1) + P_\delta(C_2) \leq 0.99.$$

But this **contradicts the pointwise statement** for a. □

(The formal proof proceeds by induction on n (available in APX_1), and employs **precision consistency** and the slack parameter β to handle the cumulative error from each "$\lesssim$".)

Further applications

Through extensions of the **pointwise-to-global technique**, we recover many useful results from probability:

Approximate Union Bound:

$$P_\delta\Big(C_1(x) \vee \ldots \vee C_m(x)\Big) \leq P_\delta(C_1(x)) + \ldots + P_\delta(C_m(x)) + (2\delta + \beta) \cdot m.$$

Approximate Linearity of Expectation: ...

Then, building on these tools, we derive **Markov's Inequality**, **Chebyshev's Inequality**, etc., followed by more elaborate results from probability theory.

Organization

Prelude: Quick Recap of Bounded Arithmetic

Part I: Theory APX_1

Part II: Feasible Probabilistic Reasoning

Part III: Pigeonhole Principles and Unprovability in APX_1

Relative strength of APX_1

- Trivially: $\mathbf{PV} \subseteq \mathbf{APX_1}$ (i.e., $\mathbf{APX_1}$ extends $\mathbf{PV}$).
- Every PV-sentence provable in $\mathbf{APX_1}$ **is also provable** in $\mathbf{APC_1}$.
- Under plausible assumptions, $\mathbf{APX_1}$ is **strictly weaker** than $\mathbf{APC_1}$:

  Assume subexp-secure $i\mathcal{O}$ and coNP $\not\subseteq$ i.o.NP/poly. Then there is a $\forall\Sigma_2^b$ PV-sentence provable in $\mathbf{APC_1}$ but unprovable in $\mathbf{APX_1}$.

Can APX_1 prove the $\forall\Sigma^b_1$ consequences of APC_1?

A natural candidate is **rwPHP**, the **retraction weak pigeonhole principle**:

$$\forall n \in \mathrm{Log} \quad \forall \,\text{circuits} \quad E\colon \{0,1\}^n \to \{0,1\}^{n-1},$$
$$D\colon \{0,1\}^{n-1} \to \{0,1\}^n,$$
$$\exists x \in \{0,1\}^n \quad D(E(x)) \neq x.$$

By Thapen (2002), the question in the title is equivalent to $\mathbf{APX_1} \vdash^? \mathbf{rwPHP}$.

Can APX_1 prove rwPHP?

Under computational assumptions, $\mathbf{APX_1} \nvdash \mathbf{wPHP}$ and $\mathbf{APX_1} \nvdash \mathbf{dwPHP}$

But **rwPHP** is more delicate: it is **easy** as a total search problem!

To gain more insight, we consider whether $\mathbf{APX_1} \vdash^{?} \mathbf{rwPHP}$ in the **relativized setting**.

Relativization of APX_1 and rwPHP

We consider fresh function symbols $\boldsymbol{f}, \boldsymbol{g}$ and define the relativized theory $\mathbf{APX_1}(\boldsymbol{f}, \boldsymbol{g})$.

This is just $\mathbf{PV}(\boldsymbol{P}, \boldsymbol{f}, \boldsymbol{g})$ + approximate counting axioms for $\boldsymbol{P}_\delta(\boldsymbol{C})$.

The circuit $\boldsymbol{C}$ has oracle access to $\boldsymbol{f}$ and $\boldsymbol{g}$.

The principle $\mathbf{rwPHP}(\boldsymbol{f}, \boldsymbol{g})$ is defined in the natural way.

Question. Does $\mathbf{APX_1}(\boldsymbol{f}, \boldsymbol{g}) \vdash \mathbf{rwPHP}(\boldsymbol{f}, \boldsymbol{g})$?

Unprovability of rwPHP(f, g)

In ongoing work with **O. Korten**, **J. Li**, and **H. Ren** (with help from GPT 5.6), we show that

$$\mathbf{APX}_1(f, g) \nvdash \mathbf{rwPHP}(f, g) .$$

Key Point: We must show that polynomial many queries of the form $P_\delta(C^{f,g})$ cannot be used to find x such that $g(f(x)) \neq x$.

Much easier to show unprovability for relativized **wPHP**(f) and **dwPHP**(g): one can define an **"honest"** adversary for that.

In the case of **rwPHP**(f, g), the adversary's answers to $P_\delta(C^{f,g})$ must deviate from the intended interpretation of $P(\cdot)$ as approximate counting!

Concluding remarks

There might be "feasible" extensions of the base theory $\mathbf{APX_1}$, such as

$$\mathbf{APX_1} + \mathbf{rwPHP}\ .$$

Similarly, we can explore natural extensions of the 4 approx. counting axioms of $\mathbf{APX_1}$. Consider the following principle:

(Invariance) Let $S, T \subseteq \{0,1\}^n$ be defined by Boolean circuits. If circuits $F\colon S \to T$ and $G\colon T \to S$ compute mutually inverse maps, then

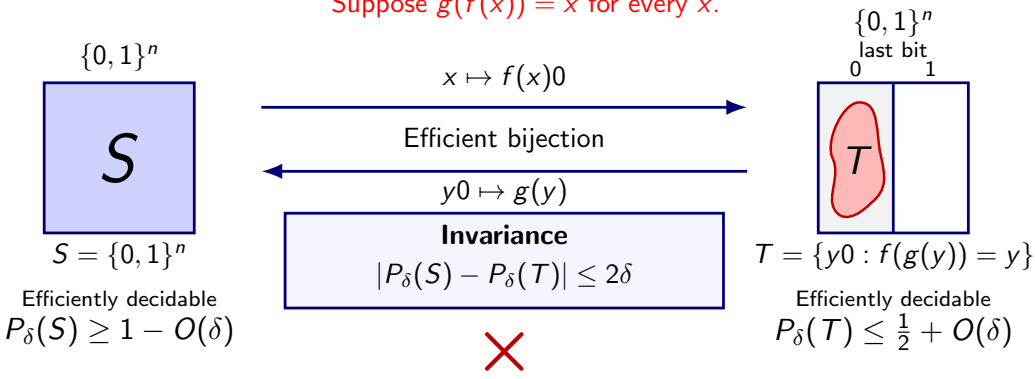
$$|P_\delta(S) - P_\delta(T)| \leq 2\delta.$$

It is not hard to show that $\mathbf{APX_1}$ + **Invariance** $\vdash$ **rwPHP**.

Concluding remarks, cont'd

$f : \{0,1\}^n \to \{0,1\}^{n-1}, \qquad g : \{0,1\}^{n-1} \to \{0,1\}^n$

Suppose $g(f(x)) = x$ for every x.



These results suggest a rich class of natural theories between $\mathbf{APX_1}$ and $\mathbf{APC_1}$.

Open Problems

- Is **APX_1** conversative over **PV**?

  “Can we derandomize every feasible proof?”

- Is **prBPP ⊆ prP** **“**feasibly provable”**?**

  Is there ***f*** in L(PV) such that PV ⊢ 4 approximate counting axioms for ***f*** ?

- If we can **derandomize proofs**, can we **derandomize computations**?

  If **APX_1** is conversative over **PV**, does it follow that **prBPP ⊆ prP** ?

Summary

- $\mathbf{APX_1}$ axiomatizes approximate counting with a **remarkably limited set of axioms**.
- From these axioms, it builds a convenient **probability toolkit** (expectation, inequalities, ...).
- Strong enough to formalize several nontrivial results, yet plausibly weaker than $\mathbf{APC_1}$.
- $\mathbf{APX_1}$ motivates several research directions, including improved formalizations, unprovability results, reverse mathematics, and the feasible provability of derandomization.

Thanks!

Appendix

Formalization of Parity $\notin \mathrm{AC}^0$ in APX_1 and PV_1

Parity $\notin \mathrm{AC}^0$

- **Average-case lower bound in $\mathbf{APX_1}$.** For constants $k, d \geq 1$, $\mathbf{APX_1}$ proves:
  For every $n \in \mathrm{Log}$, any depth-d AC^0 circuit C of size $\leq n^k$ agrees with $\oplus_n$ on at most

$$\tfrac{1}{2} + \tfrac{1}{n^k} + \delta + \beta$$

  fraction of inputs (measured via P_δ using circuit $T_C(x) \triangleq \mathbb{1}[C(x) = \oplus_n(x)]$).

- **Worst-case lower bound in $\mathbf{PV_1}$.** For constants $k, d \geq 1$, $\mathbf{PV_1}$ proves:
  For every $n \in \mathrm{Log}$ and depth-d AC^0 circuit C of size $\leq n^k$,

$$\exists x \in \{0,1\}^n \text{ such that } C(x) \neq \oplus_n(x).$$

Approach

We must avoid encoding-based arguments that rely on pigeonhole principles (or frameworks that build on them), since they are unavailable.

We use instead the classical **Furst-Saxe-Sipser [FSS'84]** random restriction argument:

- their technique seems more "averaging" friendly;
- the refinement by **Agrawal et al. [AAIPR'01]** gives a deterministic algorithm producing a good restriction.

We formalize:

- the probabilistic counting/averaging needed in the **[FSS'84]**-style analysis;
- the correctness of the **[AAIPR'01]** deterministic restriction-finding algorithm.

(Derandomized) Random Restrictions in APX_1 and PV_1

Subset Selection Lemma: We choose a set $T \subseteq [n]$ of variables.

- T is constructed and proved correct in $\mathbf{PV_1}$ using a **potential-function argument** that simulates the method of derandomization via conditional expectations.

Restriction Selection Lemmas: We choose values for variables in T.

- In $\mathbf{APX_1}$, we consider a **random assignment of bits**. The analysis relies on the pointwise-to-global averaging argument for expectation.
- In $\mathbf{PV_1}$, we derandomize the same choice.
  - Implemented by a potential argument that simulates the method of conditional expectations.
  - Relevant expectations depend on $O(\log n)$ coordinates and can be computed by PV_1-terms.

The $\mathbf{APX_1}$ proof precisely isolated what needed to be accomplished in **$\mathbf{PV_1}$**.