Learning from Equivalence Queries and Unprovability of Circuit Upper Bounds

Igor Carboni Oliveira

University of Warwick

Mathematical Approaches to Lower Bounds: Complexity of Proofs and Computation

ICMS, Edinburgh July 2022

Based on joint papers with **J. Krajíček**, **J. Bydžovský**, **M. Carmosino**, **V. Kabanets, and A. Kolokolova**

Limited progress in understanding the limits of algorithms and Boolean circuits

Are we asking the right questions?

Complexity Theory: seeks to rule out algorithms that compute in time T

(it doesn't consider the **difficulty of proving their correctness**)

Circuit Complexity Theory: seeks to rule out circuits of size S

(it doesn't consider the **difficulty of proving their existence and correctness**)

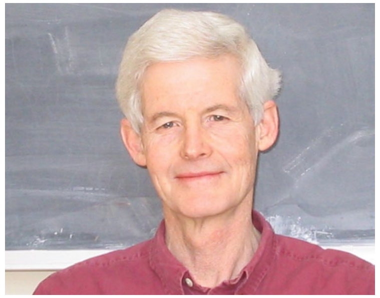
Interested in a refined complexity theory that also considers **provability**

Want to rule out efficient algorithms/circuits **with respect to a logical theory T**

Relax our goal of showing that $\mathbf{P \neq NP}$, $\mathbf{NP \not\subseteq SIZE[n^3]}$, etc. to

Theory T does not prove that P = NP

Theory T does not prove that $\mathbf{NP \subseteq SIZE[n^3]}$




Necessary before showing corresponding lower bounds

Initiated by S. Cook and J. Krajíček: Stephen A. Cook, Jan Krajícek: **Consequences of the provability of** $NP \subseteq P/poly$. J. Symb. Log. 72(4): 1353-1371 (2007)

Theories of Bounded Arithmetic

- Fragments of Peano Arithmetic (PA).
- Intended model is $\mathbb{N}$, but numbers can encode binary strings and other objects.

Example: **Theory $I\Delta_0$** [Parikh'71].

$I\Delta_0$ employs the language $\mathcal{L}_{PA} = \{0, 1, +, \cdot, <\}$.

14 axioms governing these symbols, such as:

1. $\forall x \;\; x + 0 = x$
2. $\forall x \, \forall y \;\; x + y = y + x$
3. $\forall x \;\; x = 0 \lor 0 < x$

$\ldots$

Induction Axioms. $I\Delta_0$ also contains the induction principle

$$\psi(0) \wedge \forall x\,(\psi(x) \to \psi(x+1)) \to \forall x\,\psi(x)$$

for each **bounded formula** $\psi(x)$ (additional free variables are allowed in ψ).

A **bounded formula** only contains quantifiers of the form $\forall y \leq t$ and $\exists y \leq t$, where t is a term not containing y. Abbreviations for $\forall y\,(y \leq t \to \ldots)$ and $\exists y\,(y \leq t \wedge \ldots)$.

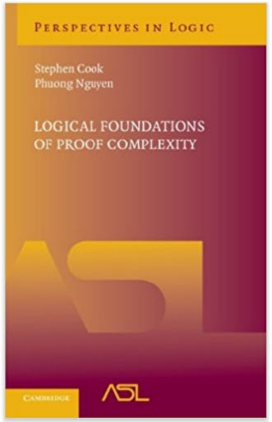
- [Cook'75] and [Buss'86] introduced theories more closely related to levels of PH:

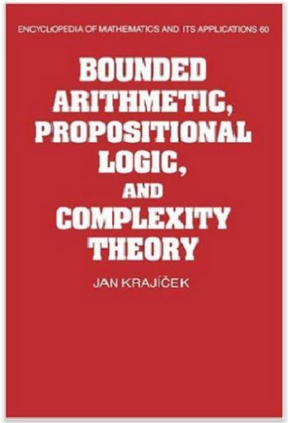
Ex.: T^1_2 uses induction scheme for bounded formulas corresponding to NP-predicates.

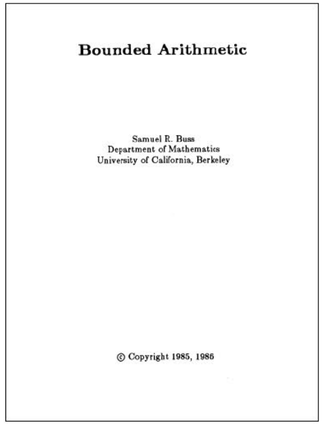
Contributions

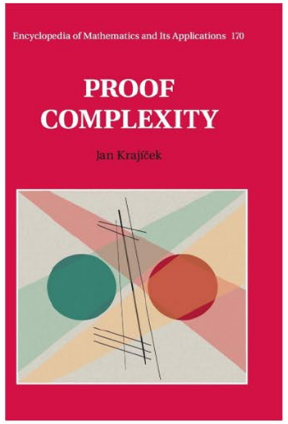
We consider several established theories of bounded arithmetic:

$$\mathsf{PV},\quad \mathsf{S}^1_2,\quad \mathsf{T}^1_2,\quad \mathsf{APC}^1$$









Many interesting algorithms and complexity results can be formalized in such theories.

Randomized Matching Algorithms in APC^1 [TriManLe-Cook'11]

PCP Theorem in PV [Pich'15].

Parity $\notin \mathsf{AC}^0$, k-Clique $\notin \mathsf{mSIZE}[n^{\sqrt{k}/1000}]$ in APC^1 [Muller-Pich'19].

Arnold Beckman's survey on Friday

Azza Gaysin's talk on formalizing Dmitriy Zhuk's CSP algorithm in S^1_2

In contrast, we show that several **circuit upper bounds cannot be proved in these theories**.

Unprovability Results

Related work:

Cook-Krajicek'07

Bydzovsky-Muller'20

Recent progress on unprovability of **circuit lower bounds**

[Krajicek-**O**'17] $\mathsf{PV} \nvdash \mathsf{P} \subseteq \mathsf{SIZE}[n^k]$

[Bydzovsky-Krajicek-**O**'20] $\mathsf{S}^1_2 \nvdash \mathsf{NP} \subseteq \mathsf{SIZE}[n^k]$

[Bydzovsky-Krajicek-**O**'20] $\mathsf{T}^1_2 \nvdash \mathsf{P}^{\mathsf{NP}} \subseteq \mathsf{SIZE}[n^k]$

[Carmosino-Kabanets-Kolokolova-**O**'21] $\mathsf{APC}^1 \nvdash \mathsf{ZPP}^{\mathsf{NP}[\mathsf{O}(1)]} \subseteq \mathsf{SIZE}[n^k]$

[CKKO'21]
Unified approach via LEARNING

Remarks: Unconditional

As theories get stronger, we can only rule out stronger inclusions

APC¹: unprovability result is close to known unconditional lower bound

[CKKO'21]: Unprovability via Learning

We argue by contradiction

Suppose theory T can prove that a language L is contained in SIZE$[n^k]$

Non-uniform upper bound:

For every n, there is a small circuit C, for every input x, C(x) = L(x)

This sentence claims the **existence of a sequence of small circuits for L**

A **proof** of the existence of an object often provides more information about the object than just its existence.

We explore standard techniques from logic (**witnessing theorems**) to extract a **learning algorithm** from a proof in bounded arithmetic

To complete the argument:

We argue (outside T) that corresponding learning algorithm that constructs circuits for L **does not exist**.

Learning from **Equivalence Queries** [Angluin'87]

EQ oracle for language L:

Learner selects circuit c of size $\leq$ s $\rightarrow$ $\boxed{\mathrm{EQ}(c)}$

- "yes" if $c \equiv L_n$
- x such that $c(x) \neq L_n(x)$ otherwise

(counterexample)

Definition. We say that L is in **$\mathbf{LEARN}^{\mathbf{EQ[q]}}$-uniform SIZE[s]** if

$\exists$ efficient algorithm $A(1^n)$ that outputs a circuit of size $\leq s(n)$ for L_n after making $\leq q(n)$ EQs.

Example of learning uniformity

If **PRIMES** in $\mathbf{LEARN}^{\mathbf{EQ}[\log n]}$**-uniform SIZE[**$9n^3$**]** then

There is an algorithm A(1^n) that computes as follows:

$\leq \log n$ **queries**

Runs in poly time and produces EQ c_1 (receives **"yes"** or **counterexample** $\boldsymbol{x_1}$)

Runs in poly time and produces EQ c_2 (receives **"yes"** or **counterexample** $\boldsymbol{x_2}$)

...

Outputs a correct circuit of size $\leq$ $9n^3$ **for PRIMES**$_n$

Example of Formalization [KO'17]

PV cannot prove that **P is contained in SIZE[n^k]**

For a **function symbol *f*** in the language of PV (polynomial-time algorithms) and **constant c in $\mathbb{N}$**,

$$\mathsf{UP}_{k,c}(f) \text{ asserts that } L_f \in \mathsf{SIZE}[cn^k]:$$

$$\forall 1^{(n)} \exists \text{circuit } C_n (|C_n| \leq cn^k) \forall x (|x| = n),\ f(x) \neq 0 \leftrightarrow C_n(x) = 1$$

Theorem. *For every $k \geq 1$ there is a unary PV function symbol h such that for no constant $c \geq 1$ PV proves the sentence* $\mathrm{UP}_{k,c}(h)$.

Remark: UP$_{k,c}$ (*f*) is a $\forall\exists\forall$ sentence

From logic to learning via KPT Witnessing

Theorem. Assume T is a universal theory with vocabulary $\mathcal{L}$, ϕ is a quantifier-free $\mathcal{L}$-formula, and

$$T \vdash \forall z \exists C \forall x \;\; \phi(z, C, x) \; .$$

Then there exist a constant $d \geq 1$ and a finite sequence $t_1, \ldots, t_d$ of $\mathcal{L}$-terms such that

$$T \vdash \phi(z, t_1(z), x_1) \;\vee\; \phi(z, t_2(z, x_1), x_2) \;\vee\; \ldots \;\vee\; \phi(z, t_d(z, x_1, \ldots, x_{d-1}), x_d).$$

From logic to learning via KPT Witnessing

Theorem. Assume T is a universal theory with vocabulary $\mathcal{L}$, ϕ is a quantifier-free $\mathcal{L}$-formula, and

$$T \vdash \forall z \exists C \forall x \ \phi(z, C, x) \ .$$

Then there exist a constant $d \geq 1$ and a finite sequence $t_1, \ldots, t_d$ of $\mathcal{L}$-terms such that

$$T \vdash \phi(z, t_1(z), x_1) \ \vee \ \phi(z, t_2(z, x_1), x_2)$$

From logic to learning via KPT Witnessing

Theorem. Assume T is a universal theory with vocabulary $\mathcal{L}$, ϕ is a quantifier-free $\mathcal{L}$-formula, and

$$T \vdash \forall z \exists C \forall x \ \phi(z, C, x) \ .$$

Then there exist a constant $d \geq 1$ and a finite sequence $t_1, \ldots, t_d$ of $\mathcal{L}$-terms such that

$$T \vdash \phi(z, t_1(z), x_1) \ \vee \ \phi(z, t_2(z, x_1), x_2) \ \vee \ \ldots \ \vee \ \phi(z, t_d(z, x_1, \ldots, x_{d-1}), x_d).$$

From logic to learning via KPT Witnessing

Theorem. Assume T is a universal theory with vocabulary $\mathcal{L}$, ϕ is a quantifier-free $\mathcal{L}$-formula, and

$$T \vdash \forall z \exists C \forall x \;\; \phi(z, C, x) \; .$$

Then there exist a constant $d \geq 1$ and a finite sequence $t_1, \ldots, t_d$ of $\mathcal{L}$-terms such that

$$T \vdash \phi(z, t_1(z), x_1) \;\vee\; \phi(z, t_2(z, x_1), x_2) \;\vee\; \ldots \;\vee\; \phi(z, t_d(z, x_1, \ldots, x_{d-1}), x_d).$$

Key point: Applying this result to **UP$_{k,c}$(*f*)** and **PV,** we get a **LEARN-uniform** construction of circuits of size cn^k for ***f***.

Landscape of circuit uniformity notions

P-uniform SIZE[n^k]

Efficiently computable from 1^n

LEARN$^{\text{EQ[q]}}$-uniform-SIZE[n^k]

Stronger theories: corresponding learning algorithms are more expressive (more queries, randomized)

SIZE[n^k]

Essentially equivalent to FZPP$^{\text{NP}}$ uniformity w.r.t. lower bounds:

$$\mathsf{P} \subseteq \mathsf{SIZE}[O(n^k)]$$

$$\Updownarrow \quad \text{[Bsh+96]}$$

$$\mathsf{P} \subseteq \mathsf{FZPP}^{\mathsf{NP}}\text{-uniform } \mathsf{SIZE}[O(n^{k'})]$$

Unconditional LEARN-Uniform Lower Bounds

[Carmosino-Kabanets-Kolokolova-**O**'21]

1. *For all* $k \geq 1$, *there is a language* $L \in \mathsf{P}$ *such that* $L \notin \mathsf{LEARN}^{\mathsf{EQ}[O(1)]}\text{-uniform } \mathsf{SIZE}[n^k]$.

2. *For all* $C \geq 1$ *and* $r(n) = o(\log n / \log\log n)$, $\mathsf{P} \not\subseteq \mathsf{LEARN}^{\mathsf{EQ}[r(n)]}\text{-uniform } \mathsf{SIZE}[n \cdot (\log n)^C]$.

3. *For all* $k \geq 1$, $\mathsf{NP} \not\subseteq \mathsf{LEARN}^{\mathsf{EQ}[n^{o(1)}]}\text{-uniform } \mathsf{SIZE}[n^k]$.

Q. What is the power of a **polynomial number** of equivalence queries?

Learning a SAT Solver

- We consider the problem of learning a **SAT Solver** for formulas of bitlength n:

SAT Solver: A circuit **C** such that, on every SATISFIABLE Boolean formula ϕ,

C(ϕ) outputs a satisfying assignment of ϕ

- We allow the LEARN-uniform construction to make **Search-SAT-EQs**:

Search-SAT-EQs: Given a candidate SAT Solver **D**, either returns **CORRECT** or provides a **counterexample**:

Pair (ψ, w) such that ψ(w) = 1 but **D**(ψ) is **not** a satisfying assignment for ψ

4. For all $k \geq 1$,

$\textsf{Search-SAT} \notin \textsf{LEARN}^{\textsf{Search-SAT-EQ}[n^{O(1)}]}\textsf{-uniform SIZE}[n^k]$ *or* $\textsf{NP} \not\subseteq \textsf{LEARN}^{\textsf{EQ}[n^{O(1)}]}\textsf{-uniform SIZE}[n^k]$

Techniques

Lower bounds for **P** (fewer EQs) and for **NP** (larger number of EQs) rely on different approaches

1. For all $k \geq 1$, *there is a language* $L \in \mathsf{P}$ *such that* $L \notin \mathsf{LEARN}^{\mathsf{EQ}[O(1)]}\text{-uniform } \mathsf{SIZE}[n^k]$.

Indirect diagonalization

Non-trivial: learning procedure can run in larger time than L

Builds on techniques from **[Santhanam-Williams'14]**

3. For all $k \geq 1$, $\mathsf{NP} \not\subseteq \mathsf{LEARN}^{\mathsf{EQ}[n^{o(1)}]}\text{-uniform } \mathsf{SIZE}[n^k]$.

LEARN-uniform construction implies **collapse** of **PH** to **NP/o(n)**

Derive non-uniform circuit lower bounds for NP, contradicting initial assumption.

Builds on techniques from **[Cook-Krajicek'07]**

Summary of (deterministic) learning lower bounds

[Carmosino-Kabanets-Kolokolova-**O**'21]

1. *For all* $k \geq 1$, *there is a language* $L \in \mathsf{P}$ *such that* $L \notin \mathsf{LEARN}^{\mathsf{EQ}[O(1)]}\text{-uniform } \mathsf{SIZE}[n^k]$.

2. *For all* $C \geq 1$ *and* $r(n) = o(\log n / \log\log n)$, $\mathsf{P} \not\subseteq \mathsf{LEARN}^{\mathsf{EQ}[r(n)]}\text{-uniform } \mathsf{SIZE}[n \cdot (\log n)^C]$.

3. *For all* $k \geq 1$, $\mathsf{NP} \not\subseteq \mathsf{LEARN}^{\mathsf{EQ}[n^{o(1)}]}\text{-uniform } \mathsf{SIZE}[n^k]$.

4. *For all* $k \geq 1$,

$\mathsf{Search\text{-}SAT} \notin \mathsf{LEARN}^{\mathsf{Search\text{-}SAT\text{-}EQ}[n^{O(1)}]}\text{-uniform } \mathsf{SIZE}[n^k]$ *or* $\mathsf{NP} \not\subseteq \mathsf{LEARN}^{\mathsf{EQ}[n^{O(1)}]}\text{-uniform } \mathsf{SIZE}[n^k]$

Consequences in logic

These results imply unprovability of circuit upper bounds in theories PV, S^1_2, T^1_2

For **APC**^{1}, the provability of circuit upper bounds leads to **RANDOMIZED** learning with **EQs**.

Analyzing circuits constructed with $\underbrace{\textbf{RANDOMNESS + EQs}}$ becomes much more challenging.

P-uniform SIZE$[n^k]$ **LEARN**$^{\mathrm{EQ}[q]}$**-uniform-SIZE**$[n^k]$ **. . .** ★ **SIZE**$[n^k]$

Essentially equivalent to **FZPP**$^{\mathrm{NP}}$ uniformity w.r.t. lower bounds

Theorem 1 (**KPT Witnessing for APC^1**). *Let φ be an open formula in the language of PV. If*

$$\mathsf{APC}^1 \vdash \forall N\, \exists C\, \forall Z\; \varphi(N, C, Z)$$

there are a constant number ℓ of polynomial-time computable functions

$$A_1(N, R_1),\; A_2(N, R_1, Z_1, R_2),\; \dots\;,\; A_\ell(N, R_1, Z_1, \dots, R_{\ell-1}, Z_{\ell-1}, R_\ell)$$

and a constant $c \geq 1$ such that, for every $N \in \mathbb{N}$ and $n = |N| \geq 1$, the following holds.

1. *With probability at least $1/n^c$ over uniform randomness R_1, for $C_1 = A_1(N, R_1)$, either $\mathbb{N} \vDash \forall Z_1\, \varphi(N, C_1, Z_1)$, or for any Z_1 such that $\mathbb{N} \vDash \neg\varphi(N, C_1, Z_1)$, the following holds.*

2. *With probability at least $1/n^c$ over R_2, for $C_2 = A_2(N, R_1, Z_1, R_2)$, either $\mathbb{N} \vDash \forall Z_2\, \varphi(N, C_2, Z_2)$, or for any Z_2 such that $\mathbb{N} \vDash \neg\varphi(N, C_2, Z_2)$, the following holds.*

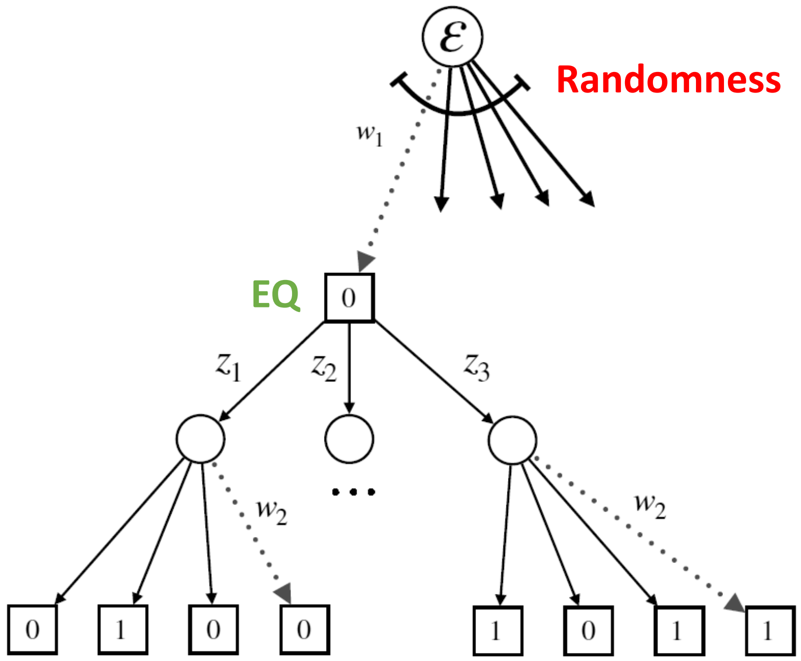
$$\vdots$$

ℓ. *With probability at least $1/n^c$ over R_ℓ, for $C_\ell = A_\ell(N, R_1, Z_1, \dots, R_{\ell-1}, Z_{\ell-1}, R_\ell)$, we have $\mathbb{N} \vDash \forall Z_\ell\, \varphi(N, C_\ell, Z_\ell)$.*

Randomized LEARN-uniformity

Definition. We say that L is in $\mathbf{FZPP\text{-}LEARN}^{\mathrm{EQ}[q]}$**-uniform SIZE[s]** if

∃ efficient **randomized** algorithm A(1^n) that outputs with probability $\geq 3/4$ a circuit of size ≤ s(n) for L_n after making ≤ q(n) **EQs**.



Our goal: Explicit lower bounds against

$\mathbf{FZPP\text{-}LEARN}^{\mathrm{EQ}[O(1)]}$**-uniform SIZE[O($n^k$)]**

RANDOMNESS + **EQs**

Which circuits can we construct with **randomness only**?

Randomized Uniformity

It seems we are the first to investigate the limits of randomized uniformity

Two potential definitions:

(1) The **same** circuit is produced with probability $\geq 2/3$ (**pseudodeterministic**)

Equivalently, the **direct connection language** is in **ZPP** or **BPP**

$$\textsf{ZPP-uniform SIZE}[n^k]$$

$$\textsf{BPP-uniform SIZE}[n^k]$$

(2) With probability $\geq 2/3$ a correct circuit is produced

Appropriate definition in the learning setting

$$\textsf{FZPP-uniform SIZE}[n^k]$$

$$\textsf{FBPP-uniform SIZE}[n^k]$$

Much harder to analyze!

Lower bounds against randomized uniformity

[Carmosino-Kabanets-Kolokolova-**O**'21]

$\mathbf{FZPP\text{-}LEARN}^{\mathbf{EQ}[0]}$**-uniform SIZE[$n^k$]**

$\shortparallel$

Theorem. promise-ZPP $\not\subseteq$ FZPP-uniform $\mathsf{SIZE}[n^k]$

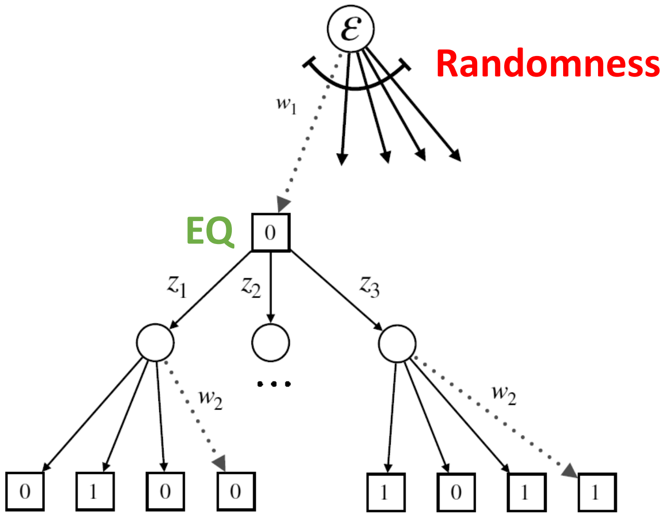
Main ideas: First, we establish that ZPP $\not\subseteq$ ZPP$/n^{\varepsilon}$-uniform $\mathsf{SIZE}[n^k]$

Now reduce the **FZPP** case to the simpler case of **ZPP-uniformity**:

Proof makes use of recent **BPP/1 computable pseudodeterministic PRG** from [Lu-O-Santhanam'21]

(To maintain zero error, we invoke Kabanets' **Easy Witness Method**)

Randomized LEARN-uniformity



RANDOMNESS + **EQs**

Goal: Explicit lower bounds against

$$\mathbf{FZPP\text{-}LEARN}^{\mathbf{EQ}[O(1)]}\text{-}\mathbf{uniform\ SIZE}[O(n^k)]$$

Theorem. $\text{Search-SAT} \notin \text{FZPP-LEARN}^{\text{Search-SAT-EQ}[O(1)]}\text{-uniform SIZE}[\text{poly}]$

$$or$$

$$\text{ZPP}^{\text{NP}[O(1)]} \not\subset \text{SIZE}[n^k]$$

Corollary. "**APC**[1] does not prove that $\mathbf{ZPP}^{\mathbf{NP[O(1)]}}$ is contained in $\mathbf{SIZE}[n^k]$"

"**APC^1** does not prove that **ZPP$^{\text{NP}[O(1)]}$** is contained in **SIZE$[n^k]$**"

Formally: $\mathsf{APC}^1 \nvdash \mathsf{NP} \subseteq \mathsf{SIZE}[n^k]$ or $\mathsf{ZPP}^{\mathsf{NP}[O(1)]} \not\subseteq \mathsf{SIZE}[n^k]$

Suppose **APC^1** proves that **NP is contained in SIZE$[n^k]$**

→ **CK'07** →

APC^1 proves that there is an efficient SAT solver

→ **KPT Witnessing for APC^1** →

A SAT solver of size n^d is learnable from **r = O(1)** Search-SAT-EQs with **probability 1/poly(n)**

↓ **Amplification Lemma** ↓

Boosted learning procedure that maintains **r** Search-SAT-EQs and has **success probability 1 – 2$^{-\text{poly}(n)}$**.

← **Conversion Lemma** ←

Randomness-First Learner with **r** Search-SAT-EQs

← **Similar to deterministic learning result** ←

Collapse of **PH** to **ZPP$^{\text{NP}[O(1)]}$**

↓

By Kannan's Theorem, **ZPP$^{\text{NP}[O(1)]}$ is not contained in SIZE$[n^k]$**

Summary

We advance a research program that **combines complexity and provability**:

Goal: Theory **T** does not establish upper bounds

(formally necessary before establishing lower bounds)

Learning vs Logic: Each theory **T** leads to a **corresponding notion of learnability**

Essentially all known results can be obtained by investigating **LEARN-uniform constructions**.

Open Problems

P is not contained in LEARN-Uniform SIZE$[n^k]$ with **O(log *n*)** queries

NP is not contained in LEARN-Uniform SIZE$[n^k]$ with **poly(*n*)** queries

Show that $\mathsf{S}^1_2 \nvdash \mathsf{P} \subseteq \mathsf{SIZE}[n^k]$

New lower bounds against **Randomized Uniformity** and **Randomized LEARN-Uniformity**

e.g., show that **promise-BPP** is not contained in **FBPP-uniform SIZE$[n^k]$**

Obtain a stronger unprovability result for **APC**^{1} ?

Thank you

Appendix

Unprovability of i.o. circuit upper bounds [BKO'20]

Our results. For an $L(\mathsf{PV})$-formula $\varphi(x)$ and an integer $k \geq 1$, the $L(\mathsf{PV})$-sentence $\mathsf{UB}_k^{i.o.}(\varphi)$ is defined as follows:

$$\forall 1^{(n)}\, \exists 1^{(m)} (m \geq n)\, \exists C_m(|C_m| \leq m^k)\, \forall x(|x| = m),\ \varphi(x) \equiv (C_m(x) = 1)\ .$$

Theorem 1.1 (Consistency of almost-everywhere circuit lower bounds with bounded theories). *Let $k \geq 1$ be any positive integer. For any of the following pairs of an $L(\mathsf{PV})$-theory T and a uniform complexity class $\mathcal{C}$:*

(a) $T = \mathsf{T}_2^1(\mathsf{PV}) \cup \mathsf{True}_1$ *and* $\mathcal{C} = \mathsf{P}^{\mathsf{NP}}$,
(b) $T = \mathsf{S}_2^1(\mathsf{PV}) \cup \mathsf{True}_0$ *and* $\mathcal{C} = \mathsf{NP}$,
(c) $T = \mathsf{PV} \cup \mathsf{True}_0$ *and* $\mathcal{C} = \mathsf{P}$,

there is an $L(\mathsf{PV})$-formula $\varphi(x)$ defining a language $L \in \mathcal{C}$ such that T does not prove the sentence $\mathsf{UB}_k^{i.o.}(\varphi)$.