Bounded Arithmetic and a Consistency Result for NEXP vs $\mathrm{P/poly}$

Sam Buss

Logic Seminar

Mathematics Institute
Czech Academy of Sciences
April 8, 2024

$$\mathrm{L} \subseteq \mathrm{NL}{=}\mathrm{coNL} \subseteq \mathrm{P} \subseteq \mathrm{NP} \subseteq \mathrm{(N)PSPACE} \subseteq \mathrm{EXP} \subseteq \mathrm{NEXP}$$

"L" = "logspace" "N" = "nondeterministic"

"P" = "polynomial (time)" "EXP" = "exponential time"

"PH" = "polynomial time hierarchy"

"P/poly" = "p-time + polynomial advice; i.e., polynomial size circuits"

$$\mathrm{L} \subseteq \mathrm{NL}{=}\mathsf{co}\mathrm{NL} \subseteq \mathrm{P} \subseteq \mathrm{NP} \subseteq \mathsf{(N)}\mathrm{PS}\textsc{pace} \subseteq \mathrm{E}\textsc{xp} \subseteq \mathrm{NE}\textsc{xp}$$

"L" = "logspace"

"N" = "nondeterministic"

"P" = "polynomial (time)"

"Exp" = "exponential time"

"PH" = "polynomial time hierarchy"

"P/poly" = "p-time + polynomial advice; i.e., polynomial size circuits"

$$\mathrm{L} \subseteq \mathrm{NL}{=}\mathsf{co}\mathrm{NL} \subseteq \mathrm{P} \subseteq \mathrm{NP} \subseteq \mathsf{(N)}\mathrm{PS{\small PACE}} \subseteq \mathrm{E{\small XP}} \subseteq \mathrm{NE{\small XP}}$$

"L" = "logspace" "N" = "nondeterministic"

"P" = "polynomial (time)" "EXP" = "exponential time"

"PH" = "polynomial time hierarchy"

"P/poly" = "p-time + polynomial advice; i.e., polynomial size circuits"

$$\mathrm{L} \subseteq \mathrm{NL}{=}\mathrm{coNL} \subseteq \mathrm{P} \subseteq \mathrm{NP} \subseteq \mathrm{(N)PSPACE} \subseteq \mathrm{EXP} \subseteq \mathrm{NEXP}$$

$$\mathrm{P} \subsetneq \mathrm{P/poly}$$

"L" = "logspace" "N" = "nondeterministic"

"P" = "polynomial (time)" "EXP" = "exponential time"

"PH" = "polynomial time hierarchy"

"P/poly" = "p-time + polynomial advice; i.e., **polynomial size circuits**"

$$\begin{array}{c} \mathrm{L} \subseteq \mathrm{NL}{=}\mathrm{coNL} \subseteq \mathrm{P} \subseteq \mathrm{NP} \subseteq (\mathrm{N})\mathrm{PSpace} \subseteq \mathrm{Exp} \subseteq \mathrm{NExp} \end{array}$$

$$\begin{array}{c} \mathrm{P} \\ \rotatebox{90}{$\subsetneq$} \\ \mathrm{P/poly} \end{array}$$

Thm: $\mathrm{NP} \subset \mathrm{P/poly} \quad \Rightarrow \quad \mathrm{PH}{\downarrow} = \Sigma_2^p$. [Karp-Lipton '82]

Thm: $\mathrm{Exp} \subset \mathrm{P/poly} \quad \Rightarrow \quad \mathrm{Exp} = \mathrm{PH} = \Sigma_2^p = \mathrm{MA}$. [Meyer; BFL'91]

Thm: $\mathrm{NExp} \subset \mathrm{P/poly} \quad \Leftrightarrow \quad \mathrm{NExp} = \mathrm{PH} = \Sigma_2^p = \mathrm{MA}$. via Easy Witness Thm [IKW '02]

Thm: $\mathrm{NExp} \not\subset \mathrm{ACC}^0$. [Williams '14]

"L" = "logspace"

"N" = "nondeterministic"

"P" = "polynomial (time)"

"Exp" = "exponential time"

"PH" = "polynomial time hierarchy"

"P/poly" = "p-time + polynomial advice; i.e., polynomial size circuits"

$$\mathrm{L} \subseteq \mathrm{NL}{=}\mathsf{co}\mathrm{NL} \subseteq \mathrm{P} \subseteq \mathrm{NP} \subseteq \mathsf{(N)}\mathrm{PS{\small PACE}} \subseteq \mathrm{E{\small XP}} \subseteq \mathrm{NE{\small XP}}$$

$$\begin{array}{c} \mathrm{P} \\ \nmid\!\cap \\ \mathsf{P/poly} \end{array}$$

Thm: $\mathrm{NP} \subset \mathrm{P/poly} \quad \Rightarrow \quad \mathrm{PH}{\downarrow} = \Sigma_2^p.$ [Karp-Lipton '82]

Thm: $\mathrm{E{\small XP}} \subset \mathrm{P/poly} \quad \Rightarrow \quad \mathrm{E{\small XP}} = \mathrm{PH} = \Sigma_2^p = \mathrm{MA}.$ [Meyer; BFL'91]

Thm: $\mathrm{NE{\small XP}} \subset \mathrm{P/poly} \quad \Leftrightarrow \quad \mathrm{NE{\small XP}} = \mathrm{PH} = \Sigma_2^p = \mathrm{MA}.$ via Easy Witness Thm [IKW '02]

Thm: $\mathrm{NE{\small XP}} \not\subset \mathrm{ACC}^0.$ [Williams '14]

This talk:
"NExp $\not\subset$ P/poly" is consistent with the bounded arithmetic theory V_2^0.

"L" = "logspace" "N" = "nondeterministic"

"P" = "polynomial (time)" "EXP" = "exponential time"

"PH" = "polynomial time hierarchy"

"P/poly" = "p-time + polynomial advice; i.e., polynomial size circuits"

• Oracle Separations •

First: an oracle separation:

Theorem: There is also an oracle Ω such that $\mathrm{P}^\Omega \neq \mathrm{NP}^\Omega$.
[Baker-Gill-Solovay'75]

Can be recast as:

Theorem: There is an oracle Ω so that $\mathrm{NP}^\Omega \not\subset \mathrm{P}^\Omega/\mathrm{poly}$.

Further: there is an Ω so that $\mathrm{NExp}^{\Omega[\mathrm{poly}]} \not\subset \mathrm{P}^\Omega/\mathrm{poly}$.

There is an oracle such that $\mathrm{NExp}^{\Omega[\mathrm{poly}]} = \mathrm{P}^\Omega$.

Moral: Separation proofs have to use non-relativizing techniques.

Disadvantage: Relativization.

• Natural Proofs •

[Razborov-Rudich'97]

A proof of $\mathcal{C} \not\subset \mathrm{P/poly}$ is "**natural**" if it is

- Useful (Effective)
- Constructive
- Large (applies to many Boolean functions)

Theorem: There are no natural proofs that $\mathrm{NP} \not\subset \mathrm{P/poly}$ if a (generally believed) strong pseudorandom number generator (SPRNG) conjecture holds. [RR'07]

Natural proofs operate on truth tables to identify Boolean functions that require large circuits.

Disadvantage: The result is conditional on SPRNG.

• ALGEBRIZATION •

[Fortnow'94; Aaronson-Wigderson'08; Impagliazzo-Kabanets-Kolokolova'09]
Work with "algebrizing oracles — Boolean oracles Ω and their extensions $\tilde{\Omega}$ to low-degree polynomials.

Theorem: [AW'08]

- $\mathrm{IP} = \mathrm{PS}{\small\mathrm{PACE}}$ (e.g.) has an algebrizing proof.
- $\mathrm{NP} \subset \mathrm{P/poly}$ and $\mathrm{NE}{\small\mathrm{XP}} \subset \mathrm{P/poly}$ cannot be proved with algebrizing techniques.
  E.g. for some Ω, $\mathrm{NE}{\small\mathrm{XP}}^{\tilde{\Omega}[\text{poly size}]} \not\subset \mathrm{P}^{\Omega}/\mathrm{poly}$.

Moral: Separation proofs have to use non-algebrizing techniques.

Disadvantage: Relativization.

Part II: Quick review of witness circuits

Witnessing for NP

Let $Q(x) \Leftrightarrow (\exists y \le t(x)) P(x, y)$ be an NP predicate.
Here, $P(\cdot, \cdot)$ is p-time and $t(x)$ is poly-growth rate.
A **witness circuit** for $Q(x)$ is a multi-output Boolean circuit $D(x)$ such that $\forall x$,

$$Q(x) \quad \Leftrightarrow \quad P(x, D(x)).$$

I.e. $(\forall x \le b)(\forall y \le t(b))[P(x, y) \rightarrow P(x, D(x))]$.

Theorem

If NP *has polynomial-size circuits* $(\mathrm{NP} \subset \mathrm{P/poly})$, *then* NP *has polynomial-size witness circuits.*

Proof idea: $D(x)$ uses poly-size subcircuits to query the bits of a minimal y one at a time.

— — —

The property of being a witness circuit is Π_1^b. With $Q := SAT$, this can be exploited to prove the Karp-Lipton theorem.

Witnessing for $\mathrm{NE{\scriptsize XP}}$

Let $Q(x) \Leftrightarrow (\exists^2 X {\le} 2^{p(|x|)}) P(x, X)$ be an $\mathrm{NE{\scriptsize XP}}$ predicate.
Here,

$X \in \{0,1\}^{2^{p(|x|)}}$ - an exponentially long bit string (or, oracle)

and

$P(x, X) \ \in \ \mathrm{E{\scriptsize XP}} := \mathrm{T{\scriptsize IME}}(2^{q(|x|)})$

p, q are polynomials.

Easy Witness Theorem: [Impagliazzo-Kabanets-Wigderson'02]
Suppose $\mathrm{NE{\scriptsize XP}} \subset \mathrm{P/poly}$. Then there are polynomial size circuits $D(\cdot)$ so that, for all x,

$$(\exists^2 X {\le} t(x)) P(x, X) \quad \Leftrightarrow \quad P(x, D(x)).$$

That is, $D(x) := D(x, i)$ outputs the value of $X(i)$.

Results reported in this talk:

- Describe second-order fragments of bounded arithmetic, including V_2^i, $i \geq 0$.
- Formulate "$\mathrm{NE}\textsc{xp} \not\subset \mathrm{P/poly}$" as second-order formula. Two forms are formulated.
- Prove that $\mathrm{NE}\textsc{xp} \subset \mathrm{P/poly}$ is not provable in V_2^0.
  Equivalently: $\mathrm{NE}\textsc{xp} \not\subset \mathrm{P/poly}$ is consistent with V_2^0.
  Equivalently: $\mathrm{NE}\textsc{xp} \not\subset \mathrm{P/poly}$ is true in some model of V_2^0.
- Sketch of the proof.

  and

- A "hardness magnification" lifting hardness for $\mathrm{S}_2^1(\alpha)$ to hardness for $\mathrm{V}_2^1(\alpha)$

Part III. Theories of Bounded Arithmetic (subtheories of PRA)

$$\begin{array}{lll}
\text{PV} & & \text{Equational} \\
\cap & & \\
\mathrm{S}^1_2 \subseteq \mathrm{T}^1_2 \subseteq \mathrm{S}^2_2 \subseteq \mathrm{T}^2_2 \subseteq \cdots \subseteq \mathrm{T}_2 & := \bigcup_i \mathrm{T}^i_2 & \text{First-order} \\
\qquad\qquad\qquad\qquad\qquad\qquad \not\cap & & \\
\qquad\qquad\qquad\qquad\qquad\qquad V^0_2 \subseteq \mathrm{V}^1_2 \subseteq \mathrm{V}^2_2 \subseteq \cdots & & \text{Second-order}
\end{array}$$

All theories include second-order objects X (essentially oracles).

PV & S^1_2 - Theories for polynomial time. [Cook'75; B'86]

T^i_2 - Theories for the levels of the polynomial time hierarchy (PH). [B'86]

V^1_2 - Theory for exponential time. [B'86]

Language for bounded arithmetic:

Basic functions: 0, S, $+$, $\cdot$, $\#$, $\lfloor \frac{1}{2}x \rfloor$, $<$.

Polynomial time functions. Every p-time function (and relation).

First-order variables and quantifiers. $\forall x$, $\exists x$ - range over integers.

Second-order variables and quantifiers. $\exists^2 X$, $\forall^2 X$ - range over (finite) sets of integers, i.e., over "oracles" or exponentially long binary strings.

Axioms for bounded arithmetic:

Defining axioms for basic functions and p-time symbols.

Boundedness and Extensionality for second-order objects.

Induction/Minimization for second-order objects.
Length-induction (PIND/LIND) or usual induction (IND).

Comprehension for some class Φ of formulas.

V_2^0 has $\Sigma_0^{1,B}$-comprehension. Essentially PH-comprehension.

Complexity results provable in bounded arithmetic

The theory T_2 can formulate many complexity results:

- Cook-Levin Theorem. [Cook'75; B'86]
- Karp-Lipton Theorem. [B'86]
- Hastad Switching Lemma. [Razborov'95]
- $\textsc{Parity} \notin \mathrm{AC}^0$. [Krajíček'95]
- Rabin test for primality. [Jeřábek'04]
- $\mathsf{BPP} \in \mathrm{P/poly}$ [Jeřábek'04]
- $\mathsf{BPP} \in \Sigma_2^p \cap \Pi_2^p$ [Jeřábek'07]
- $\mathsf{MA} = \mathsf{MAM}$ (Merlin-Arthur). [Jeřábek'07]
- PCP Theorem [Pich'15]
- and more ...

Prior Consistency Results (selected)

Razborov'95: If the SPRNG conjecture holds, S^2_2 cannot prove (slightly) superpolynomial lower bounds on circuit size.

Theorem: [Cook-Krajíček'07]

- If $\mathrm{PH} \not\subset \mathrm{P}^{\mathrm{NP}[\log]}$, then $\mathrm{NP} \not\subset \mathrm{P/poly}$ is consistent with S^1_2.
- If $\mathrm{PH} \not\subset \mathrm{P}^{\mathrm{NP}}$, then $\mathrm{NP} \not\subset \mathrm{P/poly}$ is consistent with S^2_2.

Theorem: [Krajíček-Oliviera'17],[Carmosino-Kabanets-Kolkolova-Olviera'21]
For fixed c,

- $\mathrm{NP} \not\subset \textsc{Size}(n^c)$ is consistent with S^1_2.
- $\mathrm{P}^{\mathrm{NP}} \not\subset \textsc{Size}(n^c)$ is consistent with S^2_2.
- $\mathrm{ZPP}^{\mathrm{NP}} \not\subset \textsc{Size}(n^c)$ is consistent with APC_2.

[Bydŏvský-Müller'20], [Bydŏvský-Krajíček-Müller'20], [Pich'15], [Pich-Santhanan'21], [Li-Oliviera'23] have other unconditional independence results.

For example,

Theorem: [Pich-Santhanan'21] For $\delta < 1$

- It is consistent with PV and $T^0_{\mathrm{APC}_1}$ that NP-predicates cannot be approximated by co-nondeterministic circuits of size $2^{\delta n}$.

These proofs nearly all use the KPT version of the Herbrand witnessing theorem. Some of them use the randomization technique of the Nisen-Wigderson theorem [Nisan-Wigderson'94], extending [Krajíček'12].

Part IV: Formalizations of $\mathrm{NExp} \not\subset \mathrm{P}/\mathrm{poly}$

Let $M(x)$ be a canonical NExp-complete predicate.

Formalization #1: For each $c \in \mathbb{N}$, let α^c be the formula

$$\forall 2^n \;\; \exists \, \text{circuit } C{<}2^{n^c} \;\; \forall x < 2^n \; [$$

$$C(x) = 1 \rightarrow \exists^2 Y (Y \text{ codes an accepting computation of } M(x)) \wedge$$

$$C(x) = 0 \rightarrow \neg\exists^2 Y (Y \text{ codes an accepting computation of } M(x)) \;]$$

- n is a size parameter.
- Inputs x are strings of length n.
- C ranges over Boolean circuits of size $\approx n^c$.
- $C(x) = 1 \Leftrightarrow M$ accepts x.

Part IV: Formalizations of $\mathrm{NEXP} \not\subset \mathrm{P/poly}$

Let $M(x)$ be a canonical NEXP-complete predicate.

Formalization #1: For each $c \in \mathbb{N}$, let α^c be the formula

$$\forall 2^n \;\exists \text{circuit } C{<}2^{n^c} \;\; \forall x < 2^n \; [$$
$$C(x) = 1 \rightarrow \exists^2 Y(Y \text{ codes an accepting computation of } M(x)) \wedge$$
$$C(x) = 0 \rightarrow \neg\exists^2 Y(Y \text{ codes an accepting computation of } M(x)) \;]$$

Formalization #2: For each $c \in \mathbb{N}$, let β^c be the formula

$$\forall 2^n \;\exists \text{circuits } C, D{<}2^{n^c} \;\; \forall x < 2^n \; [$$
$$C(x) = 1 \rightarrow (D(x, \cdot) \text{ codes an accepting computation of } M(x)) \;\; \wedge$$
$$C(x) = 0 \rightarrow \neg\exists^2 Y(Y \text{ codes an accepting computation of } M(x)) \;]$$

$\bigvee_c \alpha^c$: Exactly states "$\mathrm{NEXP} \subset \mathrm{P/poly}$".
$\bigvee_c \beta^c$: Equivalent to "$\mathrm{NEXP} \subset \mathrm{P/poly}$" by Easy Witness Lemma.

$\{\neg\alpha^c\}_{c\in\mathbb{N}}$: Exactly states "$\mathrm{NE{\small XP}} \not\subset \mathrm{P/poly}$".
$\{\neg\beta^c\}_{c\in\mathbb{N}}$: Equivalent to "$\mathrm{NE{\small XP}} \not\subset \mathrm{P/poly}$"
via Easy Witness Lemma.

The implications $\beta_c \to \alpha_c$ are trivial
(via comprehension on $\{y : D(x,y)\}$).

Theorem (Atserias-B.-Müller'23)

- *$\mathrm{V}^0_2 + \{\neg\alpha^c\}_{c\in\mathbb{N}}$ is consistent.*
- *$\mathrm{V}^0_2 + \{\neg\beta_c\}_{c\in\mathbb{N}}$ is consistent.*

I.e., $\mathrm{V}^0_2 +$ "$\mathrm{NE{\small XP}} \not\subset \mathrm{P/poly}$" is consistent.

Proof sketch

Proof is by contradiction.

- Suppose $\mathrm{V}_2^0 \vDash \alpha^c$ for some $c \in \mathbb{N}$.
  (For sake of a contradiction.)
- We'll show that V_2^0 proves PHP_n^{n+1} in this case.

$$\mathrm{PHP}_x^{x+1} \quad := \quad \text{Pigeonhole principle on } x \text{ many pigeons.}$$

- But this is impossible, because the Paris-Wilkie translation would then imply that there are quasipolynomial size, constant-depth Frege proofs of PHP_n^{n+1}. These are known not to exist, [Beame-Impagliazzo-Krajíček-Pitassi-Pudlák-Woods'92]
- In second-order arithmetic, the statement $\neg\mathrm{PHP}_x^{x+1}$ can be expressed as

$$\begin{aligned}\exists^2 Z\ [\quad & \forall u \le x\,(Z(u) < x) \wedge \\ & (\forall u < v \le x)(Z(u) \ne Z(v))\ ]\end{aligned}$$

- Note that $\neg\mathrm{PHP}_x^{x+1}$ is a $\mathrm{NE{\scriptstyle XP}}$-predicate.
- Since we suppose $\mathrm{V}_2^0 \vDash \alpha^c$, there is a family of polynomial size Boolean circuits $C_n(x)$ such that $C_{|x|}(i)$ outputs *True* iff there is a Z violating the pigeonhole principle PHP_i^{i+1} (for $i \le x$).
- Then, similar to the Cook-Rechhow ['79] proof of PHP, this allows V_2^0 to prove the pigeon hole principle holds for all x. Namely, from a Z violating PHP_i^{i+1}, it is easy to construct (in V_2^0) a Z' violating PHP_{i-1}^{i}.
- From this, induction — on the values of $C_{|x|}(i)$ — allows V_2^0 to prove $\forall x\, \neg\mathrm{PHP}_x^{x+1}$
- This gives the desired contradiction.

A similar proof gives a stronger result:

Theorem (Atserias-B.-Müller'23)

$\mathrm{V}_2^0 +$ "$\mathrm{NE{\scriptstyle XP}} \not\subset \mathrm{PH}/\mathit{poly}$" *is consistent.*

Theorem (Atserias-B.-Müller'23)

For the $\{\neg\beta^c\}$ formalization:

- *If* $\mathrm{S}^1_2 \nvdash \mathrm{NE{\small XP}} \not\subset \mathrm{P/poly}$, *then* $\mathrm{V}^1_2 \nvdash \mathrm{NE{\small XP}} \not\subset \mathrm{P/poly}$.
- *If* $\mathrm{V}^1_2 \vdash \mathrm{NE{\small XP}} \not\subset \mathrm{P/poly}$, *then* $\mathrm{S}^1_2 \vdash \mathrm{NE{\small XP}} \not\subset \mathrm{P/poly}$.

This is an intriguing result since the theory V^1_2 is so strong.

Indeed, Razborov['95] identifies V^1_2 as a strong theory for which independence results will be highly indicative.

Proof sketch:

A model $\mathcal{M}$ of $\mathrm{S}^1_2 + \beta^c$ can be enlarged to be a model $\mathcal{N}$ of $\mathrm{S}^1_2 + \beta^c$ plus $\exists^2\Pi^b_1$-comprehension for formulas without free second-order parameters. Namely, by taking the second-order objects of $\mathcal{N}$ to be those definable by 2^{n^c}-size circuits in $\mathcal{M}$. This is also a model of $\mathrm{V}^1_2 + \beta^c$.

Open Questions

- Is $\mathrm{V}_2^0 + \neg\alpha^{\log\log x}$ consistent? (Or, slower growing value for c?)
- Is $\mathrm{V}_2^0 +$ "$\mathrm{EXP} \not\subset \mathrm{P/poly}$" consistent?
  Is $\mathrm{V}_2^0 +$ "$\mathrm{PSPACE} \not\subset \mathrm{P/poly}$" consistent?
- Is $\mathrm{V}_2^0 +$ "$\mathrm{NP} \subset \mathrm{P/poly}$" consistent?
- Do V_2^0 or V_2^1 prove the Easy Witness Lemma?
- Independence results for V_2^1?

Thank you!