Consistency of NEXP $\not\subseteq$ P/poly in a Strong Theory

Albert Atserias

UPC Barcelona

Joint work with:

Sam Buss, UCSD,

Moritz Müller, U. Passau

Main Result

Theorem:

"$\mathrm{NEXP} \not\subseteq \mathrm{P/poly}$" is true

in a model of V02

Circuit Lower Bounds

The Big Open Problem:
Prove that some explicit problem A
is not solvable by poly-size Boolean circuits,
i.e., $A \notin$ P/poly.

Ideally, the problem A is in NP,
i.e., SAT $\notin$ P/poly.

Approaches

- Enlarge NP, e.g., PSPACE, EXP, NEXP, $NEXP^{NP}$
- Shrink P/poly, e.g., small depth, monotone, symmetric, ...
- Prove that "SAT $\notin$ P/poly" is consistent with a theory T

Cook-Krajicek 07

Consistency Approach

(a) Formalize the statement $A \notin P/poly$: the quotes in "$A \notin P/poly$"

(b) Prove: "$A \notin P/poly$" is consistent with T,
i.e., "$A \notin P/poly$" is true in some model of T,
i.e., "$A \in P/poly$" is unprovable in T.

equivalent statements

The stronger the theory T,
the stronger the evidence for $A \notin P/poly$!

Theories of Arithmetic

Cook 1975

Buss 1986

PV

$\rotatebox[origin=c]{-90}{$\subseteq$}$

S12 $\subseteq$ T12 $\subseteq \cdots \subseteq$ T2

$\rotatebox[origin=c]{-90}{$\subseteq$}$

V02 $\subseteq$ V12 $\subseteq \cdots \subseteq$ V2

$\rotatebox[origin=c]{-90}{$\subseteq$}$

$\vdots$

Peano Arithmetic $\longrightarrow$ $\cdots \subseteq$ PA

Strength (1/2)

T2

- Cook-Levin Theorem — C75, B86
- Karp-Lipton Theorem for NP — B86
- Hastad's Switching Lemma — R95
- BPP $\subseteq$ P/poly — J04
- Rabin test decides (Fermat) Primality — J04
- BPP $\subseteq$ Σ_2P $\cap$ Π_2P — J07
- Graph Isomorphism is in co-AM — J07
- AM = MAM = AMAM = MAMAM = ... — J07
- [...]

Strength (2/2)

T2
- Bipartite Perfect Matching is in RNC^2 — LC11
- PCP Theorem — P15
- PARITY $\notin$ AC^0/poly — K95
- CLIQUE $\notin$ mP/poly — MP19

V02
- PH $\subseteq$ PSPACE $\subseteq$ EXP $\subseteq$ NEXP
- bounded halting for NTMs is NEXP-complete
- Karp-Lipton Theorems for PSPACE and EXP

follow from our work

L: There is a NEXP-machine M_0 s.t. V02 proves that M_0 correctly decides the bounded halting problem for NTMs and also proves that L(M_0) is NEXP-complete.

Open Problem

Is "$NP \not\subseteq P/poly$" true in a model of S12?

Answer is YES
assuming $PH \not\subseteq NP^{NP}$ by Karp-Lipton Theorem
or even $PH \not\subseteq ZPP^{NP}$ by Watanabe's KL Theorem

Previous Consistency Results (1/2)

Thm: If PH $\not\subseteq$ $P^{NP[log]}$, then
"NP $\not\subseteq$ P/poly" is true in a model of S12

CK07
"witnessing
method"

Thm: If PH $\not\subseteq$ P^{NP}, then
"NP $\not\subseteq$ P/poly" is true in a model of S22

Previous Consistency Results (2/2)

Thm: For every $c > 0$,
"NP $\not\subseteq$ SIZE(n^c)" is true in a model of S12 ← KO17

Thm: For every $c > 0$,
"$P^{NP} \not\subseteq$ SIZE(n^c)" is true in a model of S22

"refined witnessing method"

Thm: For every $c > 0$,
"$ZPP^{NP} \not\subseteq$ SIZE(n^c)" is true in a model of APC2 ← CKKO21

Recall: For every $c > 0$, $NP^{NP} \not\subseteq$ SIZE(n^c) ← Kannan's Theorem

Our Main Result

Theorem:

"NEXP $\not\subseteq$ P/poly" is true
in a model of V02

1. MINUS: For NEXP instead of ZPP^{NP}, P^{NP}, NP,
2. PLUS: Against P/poly instead of $SIZE(n^c)$,
3. PLUS: In V02 instead of S12 $\subseteq$ S22 $\subseteq$ APC2 $\subseteq \cdots$
4. PLUS: Unconditional!

Two-Sorted Language

Basic arithmetic:

0 succ(x) $x + y$ $x \times y$ $x \# y$ $\lfloor x/2 \rfloor$ $|x|$ $x < y$

PV symbols: a function symbol for each poly-time clocked algorithm:

EUCLID-GCD(x, y)
AKS-PRIME(x)
BINARY-SEARCH^{Y}(x, l, r)

Quantifiers over number sort: $\exists x\ \varphi$ $\forall x\ \varphi$
Quantifiers over set sort: $\exists_2 Y\ \varphi$ $\forall_2 Y\ \varphi$
Membership relation: $x \in Y$

Axioms

1. BASIC axioms for basic arithmetic
2. Cobham's definitions for PV-symbols
3. Boundedness and Extensionality for set sort
4. Induction for formulas in class Φ:

$$\varphi(0) \wedge \forall z < x \left(\varphi(z) \rightarrow \varphi(z+1)\right) \rightarrow \varphi(x)$$

5. Comprehension for formulas in class Φ:

$$\exists_2 Y \leq z \ \forall x \leq z \ (x \in Y \leftrightarrow \varphi(x))$$

Definition: To define V02 take $\Phi = \Sigma_0^{1,b}$

(1) bounded quantifiers

(2) zero set-sort quantifiers

Models

Domain for number sort:

$\mathbb{N}$ in the standard model $\mathbb{N}_2$

Domain for set sort:

$\mathcal{P}_\omega(\mathbb{N})$ in the standard model $\mathbb{N}_2$

$\mathbb{N}^k \longrightarrow \mathbb{N}$

$\mathbb{N}^k$ x $\mathcal{P}_\omega(\mathbb{N})^l \longrightarrow \mathbb{N}$

Interpretations for PV-symbols:

All polynomial-time computable (type-1 and type-2) functions in the standard model $\mathbb{N}_2$

Standard interpretation for $x \in Y$ in all models.

Formalization of NEXP $\not\subseteq$ P/poly

K$_0$: a (standard) NEXP-complete problem, e.g., bounded halting
M$_0$: a (standard) explicit NEXP-machine deciding K$_0$

TFAE: NEXP $\not\subseteq$ P/poly
K$_0$ $\notin$ P/poly
$\mathbb{N}_2 \models \neg\alpha^c$ for all $c > 0$

$B(\Pi_1^{1,b})$

$$\alpha^c := \forall n \in Log\ \exists C < 2^{n^c}\ \forall x < 2^n$$
$$C(x) = 1 \longrightarrow \exists_2 Y\ \text{"}Y \text{ is an acc. comp. of } M_0 \text{ on } x\text{"}$$
$$C(x) = 0 \longrightarrow \forall_2 Y\ \text{"}Y \text{ is not an acc. comp. of } M_0 \text{ on } x\text{"}$$

A Better Formalization

Easy Witness Lemma
IKW'02

TFAE: NEXP $\not\subseteq$ P/poly
$K_0 \notin$ P/poly
K_0 does not have poly-size witness circuits
$\mathbb{N}_2 \vDash \neg\beta^c$ for all $c > 0$

$\Pi_1^{1,b}$ vs $B(\Pi_1^{1,b})$

$$\beta^c := \forall n \in Log\ \exists C < 2^{n^c}\ \exists D < 2^{n^c}\ \forall x < 2^n$$

$C(x) = 1 \longrightarrow$ "$\{y : D(x,y) = 1\}$ is an acc. comp. of M_0 on x"

$C(x) = 0 \longrightarrow \forall_2 Y$ "Y is not an acc. comp. of M_0 on x"

Note: V02 $\overset{\checkmark}{\vdash} \beta^c \to \alpha^c$ but V02 $\overset{?}{\vdash} \alpha^c \to \beta^{c'}$

Main Theorem

There is a model $\mathcal{M}$ of V02 s.t.

$\mathcal{M} \vDash \neg\alpha^c$ for all $c > 0$

$\mathcal{M} \vDash \neg\beta^c$ for all $c > 0$

i.e.

$\mathcal{M} \vDash$ "NEXP $\not\subseteq$ P/poly"

Proof Sketch in Four Steps

Step 0: Assume otherwise; i.e., for every model $\mathcal{M}$ of V02
there exists $c > 0$ such that $\mathcal{M} \vDash \beta^c$

Step 1: Take a non-standard model $\mathcal{M}$ of V02
where Pigeonhole Principle fails: $Y : [a] \xrightarrow{\text{inj}} [a-1]$

Step 2: Take a NEXP-machine N which, given a as input,
guesses and verifies 1-1 maps, provably in V02

Step 3: Use the assumption to get a contradiction because,
in $\mathcal{M}$, some such 1-1 maps cannot be in P/poly

Step 1: Get the model

Jewel Theorem of Proof Complexity: For every d > 0 and every large m > 0, every depth-d Frege proof of $PHP_{m,m-1}$ has size at least $\exp(m^{-\exp(d)})$.

A88, KPW92, BIP92

Gives a model $\mathcal{M}$ of V02 and $a \in \mathcal{M}$ where $PHP(a)$ fails, i.e.

$$\mathcal{M} \quad \vDash \quad \exists_2 Y \text{ “}Y \text{ is a 1–1 map from } a \text{ to } a-1\text{”}$$

More strongly,

$$\mathcal{M} \quad \vDash \quad PHP(0) \ \wedge \forall z < a \ \big(PHP(z) \rightarrow PHP(z+1)\big) \wedge \ \neg PHP(a)$$

Step 2 : Get the NEXP machine

$\mathcal{M} \vDash \exists_2 Y$ "Y is a 1–1 map from a to $a-1$"

Think of these as:

a: an input of length $n := |a|$ in Log of $\mathcal{M}$

Y: the guess of a NEXP-machine N on input a

L: For every $s\Sigma_1^{b,1}$-formula $\varphi(x)$ there is NEXP-machine N and f ∈ PV:

$$\text{V02} \vdash \varphi(x) \leftrightarrow \exists_2 Y \text{ "}Y\text{ is an acc. comp. of N on }x\text{"}$$
$$\leftrightarrow \exists_2 Y \text{ "}Y\text{ is an acc. comp. of }\mathrm{M}_0\text{ on f}(x)\text{"}$$

getting V02 here is not entirely trivial

Step 3 : Use the assumption

$$\mathcal{M} \vDash \neg PHP(x) \leftrightarrow \exists_2 Y \text{ “}Y \text{ is an acc. comp. of } \mathrm{M}_0 \text{ on } \mathrm{f}(x)\text{”}$$

By assumption $\mathcal{M} \vDash \beta^c$ for some $c > 0$. Hence:

$$\mathcal{M} \vDash \exists C < 2^{|a|^c} \forall x < 2^{|a|} \left(C(x) \leftrightarrow \neg PHP(x)\right)$$

Recall

$$\mathcal{M} \vDash PHP(0) \wedge \forall z < a \left(PHP(z) \rightarrow PHP(z+1)\right) \wedge \neg PHP(a).$$

Therefore, for the above $C \in \mathcal{M}$, we have

$$\mathcal{M} \vDash \neg C(0) \wedge \forall z < a \left(\neg C(z) \rightarrow \neg C(z+1)\right) \wedge C(a)$$

against the quantifier-free induction axiom of V02. $\boxed{\text{QED}}$

Discussion (1/2)

We proved "NEXP $\not\subseteq$ P/poly" true in some model of V02.

Might "NEXP $\not\subseteq$ P/poly" be independent of V02?

Magnification Theorem for Unprovability:
If it is unprovable in V02, then it is also unprovable in V12!

unprovability in
S12(α) suffices

would settle
Razborov's program

Discussion (2/2)

Similar ideas give:

Theorem:
"$\mathsf{NTIME}(n^{\log\log\cdots\log n}) \not\subseteq \mathsf{P/poly}$" is true
in a model of V02

Relies on Murray-Williams' EWL
instead of IKW's EWL

Open Problems

Q1 : Can V02 prove the Easy Witness Lemma? V02 $\vdash \alpha^{c} \rightarrow \beta^{c'}$?

Q2 : Can V02 prove IP = PSPACE or MIP = NEXP?

Q3 : Can V02 prove Polynomial Identity Testing in BPP or P/poly?

Q4 : Can V02 prove "$\mathrm{NEXP}^{\mathrm{NP}} \not\subseteq$ P/poly"?

Q5 : Is "NEXP $\not\subseteq$ P/poly" true in some model of V02 + PHP(x)?

Q6 : Is "EXP $\not\subseteq$ P/poly" true in some model of V02?

Q7 : Is "PSPACE $\not\subseteq$ P/poly" true in some model of V02?

THE END