

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:

“ $\text{NEXP} \not\subseteq \text{P/poly}$ ” 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

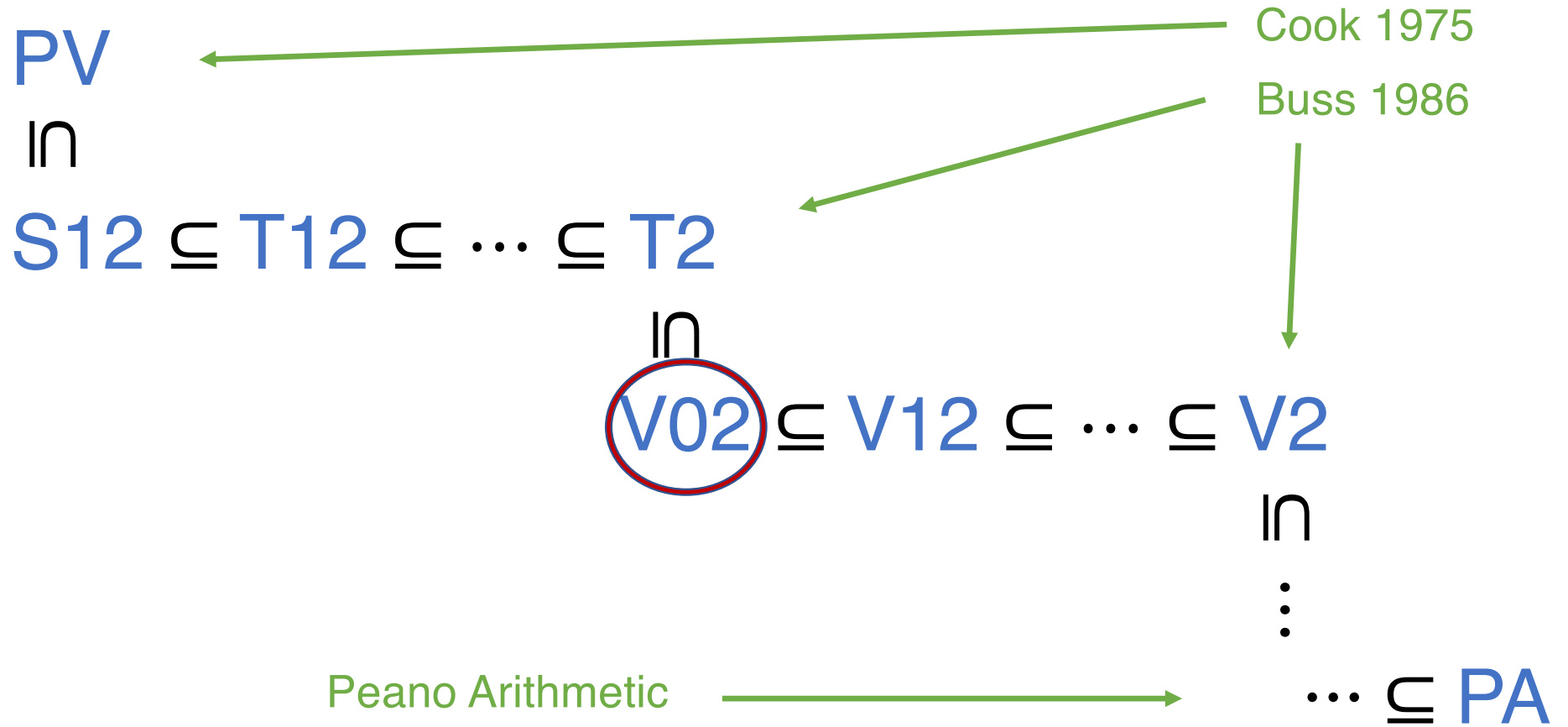
 Cook-Krajicek 07

Consistency Approach

- (a) Formalize the statement $A \notin P/\text{poly}$: the quotes in “ $A \notin P/\text{poly}$ ”
- (b) Prove: “ $A \notin P/\text{poly}$ ” is consistent with T ,
i.e., “ $A \notin P/\text{poly}$ ” is true in some model of T ,
i.e., “ $A \in P/\text{poly}$ ” is unprovable in T .
- } equivalent statements

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

Theories of Arithmetic



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
	- $BPP \subseteq \Sigma_2P \cap \Pi_2P$	J07
	- Graph Isomorphism is in co-AM	J07
	- $AM = MAM = AMAM = MAMAM = \dots$	J07
	- [...]	

Strength (2/2)

- T2**
- Bipartite Perfect Matching is in RNC^2
 - PCP Theorem
 - $PARITY \notin AC^0/poly$
 - $CLIQUE \notin mP/poly$
- LC11
P15
K95
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
“ $NP \not\subseteq P/\text{poly}$ ” is true in a model of **S12**

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



CK07
“witnessing
method”

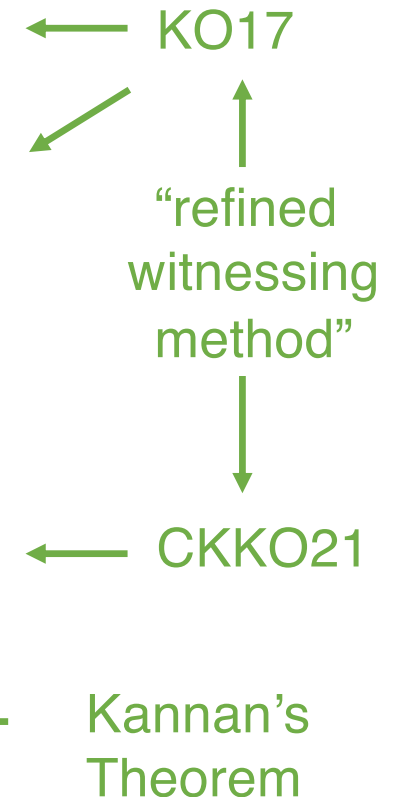
Previous Consistency Results (2/2)

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

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

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

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



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 $S12 \subseteq S22 \subseteq APC2 \subseteq \dots$
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

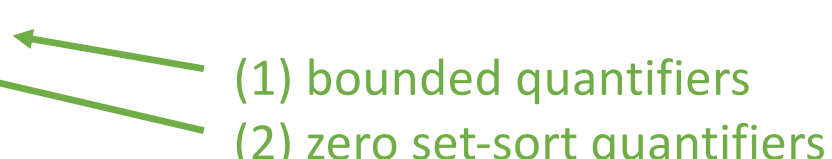
1. **BASIC** axioms for basic arithmetic
2. **Cobham's** definitions for PV-symbols
3. **Boundedness** and **Extensionality** for set sort
4. **Induction** for formulas in class Φ :

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

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:

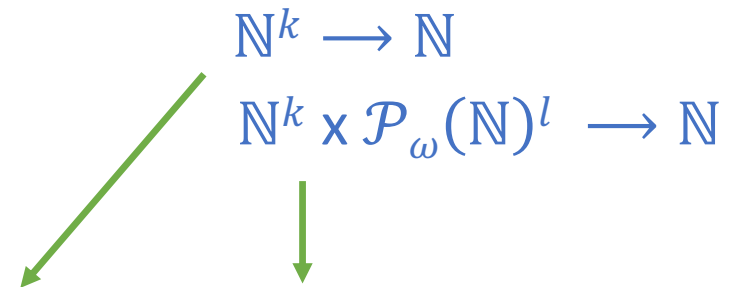
\mathbb{N} in the standard model \mathbb{N}_2

Domain for set sort:

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

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 $\text{NEXP} \not\subseteq \text{P/poly}$

K_0 : a (standard) NEXP -complete problem, e.g., bounded halting
 M_0 : a (standard) explicit NEXP -machine deciding K_0

TFAE: $\text{NEXP} \not\subseteq \text{P/poly}$
 $K_0 \notin \text{P/poly}$
 $\mathbb{N}_2 \models \neg \alpha^c$ for all $c > 0$

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

$C(x) = 1 \rightarrow \exists_2 Y$ “ Y is an acc. comp. of M_0 on x ”

$C(x) = 0 \rightarrow \forall_2 Y$ “ Y is not an acc. comp. of M_0 on x ”

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

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
 $\mathbb{N}_2 \models \neg\beta^c$ for all $c > 0$



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

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



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

$C(x) = 0 \rightarrow \forall_2 Y$ “ Y is not an acc. comp. of M_0 on x ”

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

Main Theorem

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

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

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

i.e.

$$\mathcal{M} \models \text{“NEXP} \not\subseteq \text{P/poly”}$$

Proof Sketch in Four Steps

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

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.

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

More strongly,

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

Step 2 : Get the NEXP machine

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

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 $f \in PV$:

$$\begin{aligned} V02 \vdash \varphi(x) &\leftrightarrow \exists_2 Y \text{ “} Y \text{ is an acc. comp. of } N \text{ on } x\text{”} \\ &\leftrightarrow \exists_2 Y \text{ “} Y \text{ is an acc. comp. of } M_0 \text{ on } f(x)\text{”} \end{aligned}$$

getting V02 here is not entirely trivial

Step 3 : Use the assumption

$$\mathcal{M} \models \neg PHP(x) \leftrightarrow \exists_2 Y \text{ “}Y \text{ is an acc. comp. of } M_0 \text{ on } f(x)\text{”}$$

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

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

Recall

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

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

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

against the quantifier-free induction axiom of **V02**.

QED

Discussion (1/2)

We proved “ $\text{NEXP} \not\subseteq \text{P/poly}$ ” true in some model of V02 .

Might “ $\text{NEXP} \not\subseteq \text{P/poly}$ ” be independent of V02 ?

Magnification Theorem for Unprovability:

If it is unprovable in V02 , then it is also unprovable in V12 !



unprovability in
 $\text{S12}(\alpha)$ suffices



would settle
Razborov's program

Discussion (2/2)

Similar ideas give:

Theorem:

“ $\text{NTIME}(n^{\log \log \dots \log n}) \not\subseteq \text{P/poly}$ ” is true
in a model of V_0^2



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 “ $NEXP^{NP} \not\subseteq P/poly$ ”?

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