On the consistency of circuit lower bounds for nondeterministic time

Moritz Müller

Universität Passau

joint work with Albert Atserias and Sam Buss

On the consistency of circuit lower bounds for nondeterministic time

Moritz Müller

Universität Passau

joint work with Albert Atserias and Sam Buss

Main result $\mathsf{NEXP} \not\subseteq \mathsf{P}/\mathsf{poly}$ is consistent with V^0_2.

Bounded arithmetics

Language PV: $<$ plus symbols for polynomial time functions

Theory $\forall$PV (DeMillo, Lipton 1979)

universal sentences true in the standard model

Theory PV (Cook 1975) is an axiomatized fragment of $\forall$PV

Bounded arithmetics

Language PV: $<$ plus symbols for polynomial time functions

Theory $\forall$PV (DeMillo, Lipton 1979)

universal sentences true in the standard model

Theory PV (Cook 1975) is an axiomatized fragment of $\forall$PV

- PV eliminates sharply bounded quantifiers $\exists y{<}|t(\bar{x})|$, $\forall y{<}|t(\bar{x})|$
- sharply bounded formulas define precisely the sets in P
- Σ^b_1-formulas define precisely the sets in NP
  i.e. form $\exists y{<}t\ \psi$ for ψ sharply bounded.
- PV proves induction for quantifier free formulas

$$\varphi(0) \wedge \neg\varphi(x) \ \rightarrow\ \exists y\big(\varphi(y) \wedge \neg\varphi(y{+}1)\big)$$

Bounded arithmetics

Language PV: $<$ plus symbols for polynomial time functions

Theory $\forall$PV (DeMillo, Lipton 1979)

universal sentences true in the standard model

Theory PV (Cook 1975) is an axiomatized fragment of $\forall$PV

Herbrand

If PV $\vdash \exists y\ \varphi(y, \bar{x})$ and $\varphi(y, \bar{x})$ is quantifier free,

then PV $\vdash \varphi(f(\bar{x}), \bar{x})$ for some $f \in$ PV.

Bounded arithmetics

Language PV: $<$ plus symbols for polynomial time functions

Theory $\forall$PV (DeMillo, Lipton 1979)

universal sentences true in the standard model

Theory PV (Cook 1975) is an axiomatized fragment of $\forall$PV

Herbrand

If PV $\vdash \exists y\ \varphi(y, \bar{x})$ and $\varphi(y, \bar{x})$ is quantifier free,

then PV $\vdash \varphi(f(\bar{x}), \bar{x})$ for some $f \in$ PV.

Intuition PV formalizes polynomial time reasoning.

Cook 1975

> *if one believes that feasibly constructive arguments can be formalized in* PV*, then it is worthwhile seeing which parts of mathematics can be so formalized.*

Bounded arithmetics

Buss' hierarchy

$$\mathsf{PV} \subseteq \mathsf{S}^1_2 \subseteq \mathsf{T}^1_2 \subseteq \mathsf{S}^2_2 \subseteq \mathsf{T}^2_2 \subseteq \cdots \mathsf{T}_2$$

PV+ quantifier-free induction	PV+ bounded induction
P induction	PH induction

Bounded arithmetics

Buss' hierarchy

$$\mathsf{PV} \;\subseteq\; \mathsf{S}_2^1 \;\subseteq\; \mathsf{T}_2^1 \;\subseteq\; \mathsf{S}_2^2 \;\subseteq\; \mathsf{T}_2^2 \;\subseteq \cdots \mathsf{T}_2$$

$\mathsf{PV} + \Sigma_1^b$ length induction

$\varphi(0) \wedge \forall y(\varphi(y) \to \varphi(y{+}1)) \to \varphi(|x|)$

NP induction for small numbers

Σ_1^b-definable functions: P

Buss' Witnessing 1985

If $\mathsf{S}_2^1 \vdash \exists y\ \varphi(y, \bar{x})$ and $\varphi(y, \bar{x})$ quantifier free,

then $\mathsf{PV} \vdash \varphi(f(\bar{x}), \bar{x})$ for some $f(\bar{x}) \in \mathsf{PV}$.

Bounded arithmetics

Buss' hierarchy

$$\mathsf{PV} \subseteq \mathsf{S}^1_2 \subseteq \mathsf{T}^1_2 \subseteq \mathsf{S}^2_2 \subseteq \mathsf{T}^2_2 \subseteq \cdots \mathsf{T}_2$$

$\mathsf{PV} + \Sigma^b_1$ induction

$\varphi(0) \wedge \forall y(\varphi(y) \to \varphi(y+1)) \to \varphi(x)$

NP induction for all numbers

Σ^b_1-definable functions: PLS

Bounded arithmetics

Buss' hierarchy

$$\mathsf{PV} \;\subseteq\; \mathsf{S}^1_2 \;\subseteq\; \mathsf{T}^1_2 \;\subseteq\; \mathsf{S}^2_2 \;\subseteq\; \mathsf{T}^2_2 \;\subseteq \cdots \mathsf{T}_2$$

$\mathsf{PV} + \Sigma^b_2$ length induction

$\varphi(0) \wedge \forall y(\varphi(y) \to \varphi(y{+}1)) \to \varphi(|x|)$

$\mathsf{NP}^{\mathsf{NP}}$ induction for small numbers

Σ^b_2-definable functions: P^{NP}

Buss' Witnessing 1985

If $\mathsf{S}^2_2 \vdash \exists y\ \varphi(y, \bar{x})$ and $\varphi(y, \bar{x}) \in \Pi^b_1$,

then given $\bar{x}$ a suitable y is computable in P^{NP}.

Bounded arithmetics

Buss' hierarchy

$$\mathsf{PV} \subseteq \mathsf{S}^1_2 \subseteq \mathsf{T}^1_2 \subseteq \mathsf{S}^2_2 \subseteq \mathsf{T}^2_2 \subseteq \cdots \mathsf{T}_2$$

$\mathsf{PV} + \Sigma^b_2$ length induction

$\varphi(0) \wedge \forall y(\varphi(y) \to \varphi(y+1)) \to \varphi(|x|)$

$\mathsf{NP}^{\mathsf{NP}}$ induction for small numbers

Σ^b_2-definable functions: P^{NP}

Buss' Witnessing 1985

If $\mathsf{S}^2_2 \vdash \exists y\ \varphi(y, \bar{x})$ and $\varphi(y, \bar{x}) \in \Pi^b_1$,

then given $\bar{x}$ a suitable y is computable in P^{NP}.

Krajíček 1993 For S^1_2, $O(\log n)$ many witness queries suffice.

Bounded arithmetics

Buss' hierarchy

$$\mathsf{PV} \subseteq \mathsf{S}_2^1 \subseteq \mathsf{T}_2^1 \subseteq \mathsf{S}_2^2 \subseteq \mathsf{T}_2^2 \subseteq \cdots \mathsf{T}_2$$

Müller, Pich 2020
formalizes many known circuit lower bounds.

Furst-Saxe-Sipser on AC_0
Razborov-Smolensky on $\mathsf{AC}_0[p]$ (almost)
Razborov on monotone circuits

Krajíček, Oliveira 2017

> PV *or its mild extensions seem to formalize most of contemporary complexity theory*

Formalizations

- Direct formalization for a Σ_1^b-formula $\varphi(x)$: $\exists N \ 1 < n = |N|$

$$\alpha_\varphi^c \ := \ \forall n \in Log_{>1} \ \exists C < 2^{n^c} \ \forall x < 2^n \ \ (C(x) = 1 \leftrightarrow \varphi(x))$$

Formalizations

- Direct formalization for a Σ_1^b-formula $\varphi(x)$: $\exists N\ 1 < n = |N|$

$$\alpha_\varphi^c \ := \ \forall n \in Log_{>1}\ \exists C < 2^{n^c}\ \forall x < 2^n\ \ (C(x) = 1 \leftrightarrow \varphi(x))$$

- Direct formalization for an NP-machine M:

$$\alpha_M^c \ := \ \forall n \in Log_{>1}\ \exists C < 2^{n^c}\ \forall x < 2^n$$
$$(C(x) = 1 \leftrightarrow \ \exists y < 2^{n^d} \text{“}y \text{ is an accepting computation of } M \text{ on } x\text{”})$$

Formalizations

- Direct formalization for a Σ^b_1-formula $\varphi(x)$: $\exists N\ 1 < n = |N|$

$$\alpha^c_\varphi \ := \ \forall n \in Log_{>1}\ \exists C < 2^{n^c}\ \forall x < 2^n \ \ (C(x) = 1 \leftrightarrow \varphi(x))$$

- Direct formalization for an NP-machine M:

$$\alpha^c_M \ := \ \forall n \in Log_{>1}\ \exists C < 2^{n^c}\ \forall x < 2^n$$
$$(C(x) = 1 \leftrightarrow \ \exists y < 2^{n^d} \text{ "}y\text{ is an accepting computation of } M \text{ on } x\text{"})$$

- These are $\forall\Sigma^b_3$. Can get a $\forall\Sigma^b_2$-formula

$$\beta^c_M \ := \ \forall n \in Log_{>1}\ \exists C, D < 2^{n^c}\ \forall x < 2^n\ \forall y < 2^{n^d}$$
$$(C(x) = 0 \rightarrow \ \neg \text{ "}y\text{ is an accepting computation of } M \text{ on } x\text{"}) \wedge$$
$$(C(x) = 1 \rightarrow \ \text{"}D(x)\text{ is an accepting computation of } M \text{ on } x\text{"})$$

"NP $\not\subseteq$ P/poly" $:= \left\{\neg\beta^c_{M_0} \mid c \in \mathbb{N}\right\}$ for a universal NP-machine M_0.

The consistency question

$$\alpha_M^c \;=\; \forall n{\in}Log_{>1}\ \exists C{<}2^{n^c}\ \forall x{<}2^n$$
$$(C(x)=1 \leftrightarrow\ \exists y{<}2^{n^d}\text{ “}y\text{ is an accepting computation of }M\text{ on }x\text{”})$$
$$\beta_M^c \;=\; \forall n{\in}Log_{>1}\ \exists C,D{<}2^{n^c}\ \forall x{<}2^n\ \forall y{<}2^{n^d}$$
$$(C(x)=0 \rightarrow\ \neg\text{ “}y\text{ is an accepting computation of }M\text{ on }x\text{”})\ \wedge$$
$$(C(x)=1 \rightarrow\ \text{“}D(x)\text{ is an accepting computation of }M\text{ on }x\text{”})$$

Central question   Is “NP $\not\subseteq$ P/poly” consistent with PV?

Krajíček 1995 / 2019

> *[Such models are] not ridiculously pathological structures, and a part of the difficulty in constructing them stems exactly from the fact that it is hard to distinguish these structures, by the studied properties, from natural numbers*
>
> *The consistency counts towards the validity of H: it is true in a model of the theory, a structure very close to the standard model from the point of view of complexity theory.*

Earlier consistency results

$$\begin{aligned}
\alpha^c_M \;&=\; \forall n{\in}Log_{>1}\ \exists C{<}2^{n^c}\ \forall x{<}2^n \\
&\quad (C(x)=1 \leftrightarrow\ \exists y{<}2^{n^d}\ \text{“}y \text{ is an accepting computation of } M \text{ on } x\text{”}) \\
\beta^c_M \;&=\; \forall n{\in}Log_{>1}\ \exists C,D{<}2^{n^c}\ \forall x{<}2^n\ \forall y{<}2^{n^d} \\
&\quad (C(x)=0 \rightarrow\ \neg\ \text{“}y \text{ is an accepting computation of } M \text{ on } x\text{”}) \wedge \\
&\quad (C(x)=1 \rightarrow\ \text{“}D(x) \text{ is an accepting computation of } M \text{ on } x\text{”})
\end{aligned}$$

Cook, Krajíček 2007

“NP $\not\subseteq$ P/poly” is consistent with S^1_2 if PH $\neq$ P^{NP}_{tt}.

“NP $\not\subseteq$ P/poly” is consistent with S^2_2 if PH $\neq$ P^{NP}.

Earlier consistency results

$$\alpha^c_M \;=\; \forall n{\in}Log_{>1}\ \exists C{<}2^{n^c}\ \forall x{<}2^n$$
$$(C(x)=1 \leftrightarrow\ \exists y{<}2^{n^d}\ \text{"}y \text{ is an accepting computation of } M \text{ on } x\text{"})$$

$$\beta^c_M \;=\; \forall n{\in}Log_{>1}\ \exists C,D{<}2^{n^c}\ \forall x{<}2^n\ \forall y{<}2^{n^d}$$
$$(C(x)=0 \rightarrow\ \neg\ \text{"}y \text{ is an accepting computation of } M \text{ on } x\text{"}) \wedge$$
$$(C(x)=1 \rightarrow\ \text{"}D(x) \text{ is an accepting computation of } M \text{ on } x\text{"})$$

Cook, Krajíček 2007

"NP $\not\subseteq$ P/poly" is consistent with S^1_2 if PH $\neq$ P^{NP}_{tt}.

"NP $\not\subseteq$ P/poly" is consistent with S^2_2 if PH $\neq$ P^{NP}.

Bydžovský, Krajíček, Oliveira 2020 Let $c \in \mathbb{N}$.

$\neg\alpha^c_M$ is consistent with S^1_2 for some NP-machine M.

$\neg\alpha^c_M$ is consistent with S^2_2 for some P^{NP}-machine M.

Two sorted theories

Add set sort variables $X, Y, \ldots$ and atoms $x \in X$.

$\Sigma_0^{1,b}$: bounded number sort quantifiers, no set sort quantifiers.

$\Sigma_1^{1,b}$: form $\exists X \psi$ for $\psi \in \Sigma_0^{1,b}$. Define the problems in NEXP.

$$\mathsf{PV} \ \subseteq \ \mathsf{S}_2^1 \ \subseteq \ \mathsf{T}_2^1 \ \subseteq \cdots \mathsf{T}_2 \ \subseteq \ \mathsf{V}_2^0 \subseteq \ \mathsf{V}_2^1$$

$\mathsf{T}_2 + \Sigma_0^{1,b}$ comprehension

$\exists Y \ \forall y \ (y \in Y \leftrightarrow y \leq z \wedge \varphi(\bar{X}, \bar{x}, y))$

Set boundedness $\quad \exists y \ \forall x \ (x \in X \rightarrow x \leq y)$

Extensionality $\quad \forall x (x \in X \leftrightarrow x \in Y) \rightarrow X = Y$

Same number sort consequences as T_2

Two sorted theories

Add set sort variables $X, Y, \ldots$ and atoms $x \in X$.

$\Sigma_0^{1,b}$: bounded number sort quantifiers, no set sort quantifiers.

$\Sigma_1^{1,b}$: form $\exists X \psi$ for $\psi \in \Sigma_0^{1,b}$. Define the problems in NEXP.

$$\mathsf{PV} \subseteq \mathsf{S}_2^1 \subseteq \mathsf{T}_2^1 \subseteq \cdots \mathsf{T}_2 \subseteq \mathsf{V}_2^0 \subseteq \mathsf{V}_2^1$$

$\mathsf{T}_2 + \Sigma_1^{1,b}$ comprehension

$\exists Y \ \forall y \ (y \in Y \leftrightarrow y \leq z \wedge \varphi(\bar{X}, \bar{x}, y))$

Set boundedness $\exists y \ \forall x \ (x \in X \rightarrow x \leq y)$

Extensionality $\forall x (x \in X \leftrightarrow x \in Y) \rightarrow X = Y$

$\Sigma_1^{1,b}$-definable functions: EXP.

Core idea

Direct formalization:

$$\alpha_\varphi^c := \forall n \in Log_{>1}\ \exists C < 2^{n^c}\ \forall x < 2^n \quad (C(x) = 1 \leftrightarrow \varphi(x)).$$

Proposition

$\{\neg\alpha_\varphi^c \mid c \in \mathbb{N}\}$ is consistent with V_2^0 for some $\Sigma_1^{1,b}$-formula $\varphi(x)$.

Core idea

Direct formalization:

$$\alpha_\varphi^c := \forall n{\in}Log_{>1}\ \exists C{<}2^{n^c}\ \forall x{<}2^n\ \ (C(x) = 1 \leftrightarrow \varphi(x)).$$

Proposition

$\{\neg\alpha_\varphi^c \mid c \in \mathbb{N}\}$ is consistent with V_2^0 for some strict $\Sigma_1^{1,b}$-formula $\varphi(x)$.

Proof sketch Let $\mathsf{PHP}(x)$ be

$$\neg\ \exists X\ \text{“}X \text{ codes a bijection from } x+1 \text{ onto } x\text{”}.$$

V_2^0 proves $\mathsf{PHP}(x)$ is inductive: $\mathsf{PHP}(0) \wedge (\mathsf{PHP}(u) \rightarrow \mathsf{PHP}(u+1))$.

Assume $\mathsf{V}_2^0 \vdash \alpha_{\neg\mathsf{PHP}}^c$.

Then $\mathsf{PHP}(u)$ is equivalent to $C(u) = 0$ for some circuit C.

Quantifier free induction gives $\mathsf{PHP}(x)$. Contradiction. $\square$

Core idea

Direct formalization:

$$\alpha^c_\varphi := \forall n{\in}Log_{>1}\ \exists C{<}2^{n^c}\ \forall x{<}2^n\ \ (C(x) = 1 \leftrightarrow \varphi(x)).$$

Proposition

$\{\neg\alpha^c_\varphi \mid c \in \mathbb{N}\}$ is consistent with V^0_2 for some strict $\Sigma^{1,b}_1$-formula $\varphi(x)$.

Faithful?

is there an NEXP-machine not simulated by small circuits in this model?

$$\begin{aligned}\alpha^c_M \quad := \quad & \forall n{\in}Log_{>1}\ \exists C{<}2^{n^c}\ \forall x{<}2^n \\ & (C(x) = 1 \leftrightarrow\ \exists Y\ \text{“}Y \text{ is an accepting computation of } M \text{ on } x\text{”})\end{aligned}$$

Core idea

Direct formalization:

$$\alpha_\varphi^c := \forall n \in Log_{>1}\ \exists C < 2^{n^c}\ \forall x < 2^n\ \ (C(x) = 1 \leftrightarrow \varphi(x)).$$

Proposition

$\{\neg\alpha_\varphi^c \mid c \in \mathbb{N}\}$ is consistent with V_2^0 for some strict $\Sigma_1^{1,b}$-formula $\varphi(x)$.

Faithful?

is there an NEXP-machine not simulated by small circuits in this model?

$$\alpha_M^c \ := \ \forall n \in Log_{>1}\ \exists C < 2^{n^c}\ \forall x < 2^n$$
$$(C(x) = 1 \leftrightarrow \ \exists Y \text{ ``}Y \text{ is an accepting computation of } M \text{ on } x\text{''})$$

Surprising?

α_φ^c has existential set quantifiers. Intuitively, V_2^0 only knows trivial sets.

Want

Set-universal formalization for machines.

Easy witness lemma

$$\beta_M^c \quad := \quad \forall n \in Log_{>1}\ \exists C, D < 2^{n^c}\ \forall x < 2^n\ \forall Y$$
$$(C(x) = 0 \rightarrow\ \neg\ \text{“}Y \text{ is an accepting computation of } M \text{ on } x\text{''})\ \wedge$$
$$(C(x) = 1 \rightarrow\ \text{“}\ \mathtt{tt}(D_x) \text{ is an accepting computation of } M \text{ on } x\text{''})$$

Easy witness lemma

$$\beta^c_M \quad := \quad \forall n{\in}Log_{>1}\ \exists C, D{<}2^{n^c}\ \forall x{<}2^n\ \forall Y$$
$$(C(x) = 0 \rightarrow\ \neg\ \text{“}Y \text{ is an accepting computation of } M \text{ on } x\text{”}) \wedge$$
$$(C(x) = 1 \rightarrow\ \text{“ } \mathtt{tt}(D_x) \text{ is an accepting computation of } M \text{ on } x\text{”})$$

Impagliazzo, Kabanets, Wigderson 2002

The following are equivalent

NEXP $\not\subseteq$ P/poly

$\{\neg\alpha^c_\varphi \mid c \in \mathbb{N}\}$ is true for some $\Sigma^{1,b}_1$-formula $\varphi(x)$

$\{\neg\alpha^c_M \mid c \in \mathbb{N}\}$ is true for some for some NEXP-machine M

$\{\neg\alpha^c_{M_0} \mid c \in \mathbb{N}\}$ is true

$\{\neg\beta^c_M \mid c \in \mathbb{N}\}$ is true for some NEXP-machine M

$\{\neg\beta^c_{M_0} \mid c \in \mathbb{N}\}$ is true

Main result

$$\beta^c_M \quad := \quad \forall n{\in}Log_{>1}\ \exists C, D{<}2^{n^c}\ \forall x{<}2^n\ \forall Y$$
$$(C(x) = 0 \to\ \neg\ \text{“}Y \text{ is an accepting computation of } M \text{ on } x\text{”}) \wedge$$
$$(C(x) = 1 \to\ \text{“ } \mathrm{tt}(D_x) \text{ is an accepting computation of } M \text{ on } x\text{”})$$

Theorem

V^0_2 is consistent with

$\{\neg\alpha^c_\varphi \mid c \in \mathbb{N}\}$ for some $\Sigma^{1,b}_1$-formula $\varphi(x)$

$\{\neg\alpha^c_M \mid c \in \mathbb{N}\}$ for some NEXP-machine M

$\{\neg\alpha^c_{M_0} \mid c \in \mathbb{N}\}$

$\{\neg\beta^c_M \mid c \in \mathbb{N}\}$ for some NEXP-machine M

$\{\neg\beta^c_{M_0} \mid c \in \mathbb{N}\} =:$ “NEXP $\not\subseteq$ P/poly”

Proof sketch For all c, φ there are d, e, M such that V^0_2 proves:

$(\beta^c_{M_0} \to \beta^d_M)$ $\quad$ $(\beta^d_M \to \alpha^d_M)$ $\quad$ $(\alpha^d_M \to \alpha^e_\varphi)$ $\quad$ ... $\quad$ □

Slightly superpolynomial time

Theorem

"$\mathsf{NTIME}[n^{O(\log\log\log n)}] \not\subseteq \mathsf{P}/\mathsf{poly}$" is consistent with V^0_2.

Set-universal formalization based on:

Murray, Williams 2018

$t(n)$ increasing, time-constructible, superpolynomial.

If $\mathsf{NTIME}(t(n)^{O(1)}) \subseteq \mathsf{P}/\mathsf{poly}$,

then $\mathsf{NTIME}(t(n)^{O(1)})$-machines have poly-size witness circuits.

Almost settles the central question on the consistency of "$\mathsf{NP} \not\subseteq \mathsf{P}/\mathsf{poly}$".

General consistency and magnification

Lemma Let $(M, \mathcal{X}) \models \mathsf{S}^1_2(\alpha) + \beta^c_{M_0}$ for some $c \in \mathbb{N}$.

There is $\mathcal{Y} \subseteq \mathcal{X}$ such that $(M, \mathcal{Y}) \models \mathsf{V}^1_2$.

General consistency and magnification

Lemma Let $(M, \mathcal{X}) \models \mathsf{S}^1_2(\alpha) + \beta^c_{M_0}$ for some $c \in \mathbb{N}$.

There is $\mathcal{Y} \subseteq \mathcal{X}$ such that $(M, \mathcal{Y}) \models \mathsf{V}^1_2$.

Proof idea

Consider a weak theory plus $\beta^c_{M_0}$

$\beta^c_{M_0}$ implies that many sets are coded by small circuits

The weak theory can quantify over and reason with these circuits

The weak theory can implicitly reason with many sets

The weak theory can simulate a strong theory

General consistency and magnification

Lemma Let $(M, \mathcal{X}) \models \mathsf{S}^1_2(\alpha) + \beta^c_{M_0}$ for some $c \in \mathbb{N}$.

There is $\mathcal{Y} \subseteq \mathcal{X}$ such that $(M, \mathcal{Y}) \models \mathsf{V}^1_2$.

Proof sketch

$\mathcal{Y} :=$ sets represented by circuits in M

Then $(M, \mathcal{Y}) \models \beta^c_{M_0}$ since $\beta^c_{M_0}$ is set-universal.

And $(M, \mathcal{Y}) \models \mathsf{S}^1_2(\alpha)$.

Suffices to show the existence of sets defined by $\exists X \ \psi(x, \bar{y}, X, \bar{Y})$ for $\psi \in \Pi^b_1$

Key: set parameters $\bar{Y}$ from $\mathcal{Y}$ can be replaced by circuits: number sort!

Then $\beta^c_{M_0}$ implies the the set is given by a circuit. □

General consistency and magnification

Lemma Let $(M, \mathcal{X}) \models \mathsf{S}^1_2(\alpha) + \beta^c_{M_0}$ for some $c \in \mathbb{N}$.

There is $\mathcal{Y} \subseteq \mathcal{X}$ such that $(M, \mathcal{Y}) \models \mathsf{V}^1_2$.

Theorem

Let $\mathsf{S}^1_2(\alpha) \subseteq \mathsf{T}$. Assume T does not prove all number-sort consequences of V^1_2.

Then "NEXP $\not\subseteq$ P/poly" is consistent with T.

General consistency and magnification

Lemma Let $(M, \mathcal{X}) \models \mathsf{S}^1_2(\alpha) + \beta^c_{M_0}$ for some $c \in \mathbb{N}$.

There is $\mathcal{Y} \subseteq \mathcal{X}$ such that $(M, \mathcal{Y}) \models \mathsf{V}^1_2$.

Theorem

Let $\mathsf{S}^1_2(\alpha) \subseteq \mathsf{T}$. Assume T does not prove all number-sort consequences of V^1_2.

Then "NEXP $\not\subseteq$ P/poly" is consistent with T.

Proof

Else $\mathsf{T} \vdash \beta^c_{M_0}$ for some $c \in \mathbb{N}$.

Let $\mathsf{V}^1_2 \vdash \psi$ number sort. Let $(M, \mathcal{X}) \models \mathsf{T}$.

To show: $M \models \psi$.

Clear by lemma. □

General consistency and magnification

Lemma Let $(M, \mathcal{X}) \models \mathsf{S}^1_2(\alpha) + \beta^c_{M_0}$ for some $c \in \mathbb{N}$.

There is $\mathcal{Y} \subseteq \mathcal{X}$ such that $(M, \mathcal{Y}) \models \mathsf{V}^1_2$.

Theorem

Let $\mathsf{S}^1_2(\alpha) \subseteq T$. Assume T does not prove all number-sort consequences of V^1_2.

Then "NEXP $\not\subseteq$ P/poly" is consistent with T.

Magnification

If $\mathsf{S}^1_2(\alpha) \nvdash$ "NEXP $\not\subseteq$ P/poly", then $\mathsf{V}^1_2 \nvdash$ "NEXP $\not\subseteq$ P/poly".

General consistency and magnification

Lemma Let $(M, \mathcal{X}) \models \mathsf{S}^1_2(\alpha) + \beta^c_{M_0}$ for some $c \in \mathbb{N}$.

There is $\mathcal{Y} \subseteq \mathcal{X}$ such that $(M, \mathcal{Y}) \models \mathsf{V}^1_2$.

Theorem

Let $\mathsf{S}^1_2(\alpha) \subseteq T$. Assume T does not prove all number-sort consequences of V^1_2.

Then "NEXP $\not\subseteq$ P/poly" is consistent with T.

Magnification

If $\mathsf{S}^1_2(\alpha) \nvdash$ "NEXP $\not\subseteq$ P/poly", then $\mathsf{V}^1_2 \nvdash$ "NEXP $\not\subseteq$ P/poly".

Proof

Say $(M, \mathcal{X}) \models \mathsf{S}^1_2(\alpha) + \beta^c_{M_0}$

Lemma: $(M, \mathcal{Y}) \models \mathsf{V}^1_2$ for some $\mathcal{Y} \subseteq \mathcal{X}$.

But $(M, \mathcal{Y}) \models \beta^c_{M_0}$ since $\beta^c_{M_0}$ is set-universal. $\square$

General consistency and magnification

Lemma Let $(M, \mathcal{X}) \models \mathsf{S}^1_2(\alpha) + \beta^c_{M_0}$ for some $c \in \mathbb{N}$.

There is $\mathcal{Y} \subseteq \mathcal{X}$ such that $(M, \mathcal{Y}) \models \mathsf{V}^1_2$.

Theorem

Let $\mathsf{S}^1_2(\alpha) \subseteq T$. Assume T does not prove all number-sort consequences of V^1_2.

Then "NEXP $\not\subseteq$ P/poly" is consistent with T.

Magnification

If $\mathsf{S}^1_2(\alpha) \nvdash$ "NEXP $\not\subseteq$ P/poly", then $\mathsf{V}^1_2 \nvdash$ "NEXP $\not\subseteq$ P/poly".

Hope to complete Razborov's program.

Question: deterministic computations ?

Open Is "EXP $\not\subseteq$ P/poly" consistent with V^0_2 ?

Formalization

Let M_1 be a suitable EXP-universal machine.

$$\begin{aligned}\beta^c_{M_1} \quad := \quad & \forall n{\in}Log_{>1}\ \exists C, D{<}2^{n^c}\ \forall x{<}2^n\ \forall Y \\ & (C(x) = 0 \rightarrow\ \neg\ \text{“}Y \text{ is an accepting computation of } M_1 \text{ on } x\text{”}) \wedge \\ & (C(x) = 1 \rightarrow\ \text{“ tt}(D_x) \text{ is an accepting computation of } M_1 \text{ on } x\text{”})\end{aligned}$$

Question: deterministic computations ?

Open Is "EXP $\not\subseteq$ P/poly" consistent with V^0_2 ?

Formalization

Let M_1 be a suitable EXP-universal machine.

$$\beta^c_{M_1} \;:=\; \forall n{\in}Log_{>1}\ \exists C, D{<}2^{n^c}\ \forall x{<}2^n\ \forall Y$$
$$(C(x) = 0 \to\ \neg\ \text{“}Y \text{ is an accepting computation of } M_1 \text{ on } x\text{”}) \wedge$$
$$(C(x) = 1 \to\ \text{“ tt}(D_x) \text{ is an accepting computation of } M_1 \text{ on } x\text{”})$$

$$\gamma^c_{M_1} \;:=\; \forall n{\in}Log_{>1}\ \exists D{<}2^{n^c}\ \forall x{<}2^n$$
$$\text{“tt}(D_x) \text{ is a halting computation of } M_1 \text{ on } x\text{”}$$

number sort $\forall\Sigma^b_2$

Proposition The following are equivalent.

EXP $\not\subseteq$ P/poly

$\{\neg\beta^c_{M_1} \mid c \in \mathbb{N}\}$ is true

$\{\neg\gamma^c_{M_1} \mid c \in \mathbb{N}\}$ is true

Question: deterministic computations ?

Open Is "EXP $\not\subseteq$ P/poly" consistent with V^0_2 ?

Formalization

Let M_1 be a suitable EXP-universal machine.

$$\beta^c_{M_1} := \forall n{\in}Log_{>1}\ \exists C, D{<}2^{n^c}\ \forall x{<}2^n\ \forall Y$$
$$(C(x) = 0 \rightarrow\ \neg\ \text{“}Y \text{ is an accepting computation of } M_1 \text{ on } x\text{”}) \wedge$$
$$(C(x) = 1 \rightarrow\ \text{“ tt}(D_x) \text{ is an accepting computation of } M_1 \text{ on } x\text{”})$$

$$\gamma^c_{M_1} := \forall n{\in}Log_{>1}\ \exists D{<}2^{n^c}\ \forall x{<}2^n$$
$$\text{“tt}(D_x) \text{ is a halting computation of } M_1 \text{ on } x\text{”}$$

number sort

$\forall\Sigma^b_2$

Theorem The following are equivalent for $T \supseteq T^1_2(\alpha)$:

$\{\neg\beta^c_{M_1} \mid c \in \mathbb{N}\}$ is consistent with T

$\{\neg\gamma^c_{M_1} \mid c \in \mathbb{N}\}$ is consistent with T

Question: deterministic computations ?

Open   Is "EXP $\not\subseteq$ P/poly" consistent with V^0_2 ?

Formalization

Let M_1 be a suitable EXP-universal machine.

$$\beta^c_{M_1} := \forall n{\in}Log_{>1}\ \exists C,D{<}2^{n^c}\ \forall x{<}2^n\ \forall Y$$
$$(C(x)=0 \rightarrow\ \neg\text{ "}Y\text{ is an accepting computation of }M_1\text{ on }x\text{"}) \wedge$$
$$(C(x)=1 \rightarrow\ \text{" tt}(D_x)\text{ is an accepting computation of }M_1\text{ on }x\text{"})$$

$$\gamma^c_{M_1} := \forall n{\in}Log_{>1}\ \exists D{<}2^{n^c}\ \forall x{<}2^n$$
"$\text{tt}(D_x)$ is a halting computation of M_1 on x"

number sort $\forall\boldsymbol{\Sigma}^b_2$

Witnessing

Proposition "EXP $\not\subseteq$ P/poly" is consistent

with S^{17}_2 if EXP $\not\subseteq \Delta^P_{17}$

with S^1_2 if EXP $\not\subseteq P^{NP}_{tt}$

Question: deterministic computations ?

Open Is "EXP $\not\subseteq$ P/poly" consistent with V^0_2 ?

Formalization

Let M_1 be a suitable EXP-universal machine.

$$\beta^c_{M_1} := \forall n{\in}Log_{>1}\ \exists C, D{<}2^{n^c}\ \forall x{<}2^n\ \forall Y$$
$$(C(x) = 0 \to\ \neg\ \text{"}Y \text{ is an accepting computation of } M_1 \text{ on } x\text{"}) \wedge$$
$$(C(x) = 1 \to\ \text{" tt}(D_x) \text{ is an accepting computation of } M_1 \text{ on } x\text{"})$$

$$\gamma^c_{M_1} := \forall n{\in}Log_{>1}\ \exists D{<}2^{n^c}\ \forall x{<}2^n$$
$$\text{"tt}(D_x) \text{ is a halting computation of } M_1 \text{ on } x\text{"}$$

number sort $\forall\boldsymbol{\Sigma}^b_2$

Witnessing

Proposition "EXP $\not\subseteq$ P/poly" is consistent

with S^{17}_2 if EXP $\not\subseteq \Delta^{\mathsf{P}}_{17}$

with S^1_2 if EXP $\not\subseteq \mathsf{P}^{\mathsf{NP}}_{tt}$
if EXP = NEXP