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.

Cook's PV

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

Cook's PV

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 $\exists y{<}|t(\bar{x})|$, $\forall y{<}|t(\bar{x})|$
- PV proves induction for quantifier free formulas
- sharply bounded formulas define precisely the sets in P
- Σ_1^b-formulas define precisely the sets in NP

  i.e. form $\exists y{<}t \ \psi$ for ψ sharply bounded.

Cook's PV

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

Proposition

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 $f(\bar{x}) \in$ PV.

Cook's PV

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

Proposition

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 $f(\bar{x}) \in$ 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.*

Buss' hierarchy

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

PV	quantifier-free induction P induction

Buss' hierarchy

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

PV	quantifier-free induction P induction
S_2^1	Σ_1^b length induction: $\varphi(0) \wedge \forall y(\varphi(y) \rightarrow \varphi(y+1)) \rightarrow \varphi(\lvert x \rvert)$ NP induction for small numbers Σ_1^b-definable functions: P

Buss' hierarchy

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

PV	quantifier-free induction P induction
S^1_2	Σ^b_1 length induction: $\varphi(0) \wedge \forall y(\varphi(y) \to \varphi(y{+}1)) \to \varphi(\lvert x \rvert)$ NP induction for small numbers Σ^b_1-definable functions: P
T^1_2	Σ^b_1 induction NP induction Σ^b_1-definable functions: PLS

Buss' hierarchy

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

PV	quantifier-free induction P induction
S_2^1	Σ_1^b length induction: $\varphi(0) \wedge \forall y(\varphi(y) \to \varphi(y+1)) \to \varphi(\lvert x \rvert)$ NP induction for small numbers Σ_1^b-definable functions: P
T_2^1	Σ_1^b induction NP induction Σ_1^b-definable functions: PLS
T_2	bounded induction PH induction

Buss' hierarchy

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

T^2_2 formalizes

- 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^b_1-formula $\varphi(x)$: $\exists N \; 1 < n = |N|$

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

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_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:

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

- These are $\forall \Sigma_3^b$. Can get a $\forall \Sigma_2^b$-formula

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

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

The consistency question

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

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

Krajíček 2019

> *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 $\neq$ $\mathsf{P}^{\mathsf{NP}}_{tt}$.

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

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 $\neq \mathsf{P}^{\mathsf{NP}}_{tt}$.

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

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 $\exists y \ \forall x \ (x \in X \to x \leq y)$

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

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

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

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

Core idea

Direct formalization:

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

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 PHP(x) be

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

V_2^0 proves 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 PHP(u) is equivalent to $C(u)=0$ for some circuit C.

Quantifier free induction gives 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?

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

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

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

Easy witness lemma

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

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

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

Theorem

V_2^0 is consistent with

- $\{\neg\alpha_\varphi^c \mid c \in \mathbb{N}\}$ for some $\Sigma_1^{1,b}$-formula $\varphi(x)$
- $\{\neg\alpha_M^c \mid c \in \mathbb{N}\}$ for some NEXP-machine M
- $\{\neg\alpha_{M_0}^c \mid c \in \mathbb{N}\}$
- $\{\neg\beta_M^c \mid c \in \mathbb{N}\}$ for some NEXP-machine M
- $\{\neg\beta_{M_0}^c \mid c \in \mathbb{N}\} =:$ “NEXP $\not\subseteq$ P/poly”

Proof sketch For all c, φ, M there are d, e, M^* such that V_2^0 proves:

$$(\beta_{M_0}^c \to \beta_M^d) \qquad (\beta_M^d \to \alpha_M^d) \qquad (\alpha_{M^*}^d \to \alpha_\varphi^e) \qquad \ldots \qquad \square$$

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.
- 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 set is given by a circuit. $\square$

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

Then "$\mathsf{NEXP} \not\subseteq \mathsf{P/poly}$" 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.

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.

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

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.

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

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

number sort

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

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.

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

$$\begin{aligned}\gamma^c_{M_1} \;:=\; & \forall n{\in}Log_{>1}\ \exists D{<}2^{n^c}\ \forall x{<}2^n & \text{number sort} \\ & \text{“tt}(D_x) \text{ is a halting computation of } M_1 \text{ on } x\text{”} & \forall\Sigma^b_2\end{aligned}$$

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

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

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