Unprovability of circuit upper bounds in Cook's theory PV

Igor Carboni Oliveira

Faculty of Mathematics and Physics, Charles University in Prague.

– Based on joint work with **Jan Krajíček** (Prague).

[Dagstuhl Workshop "Computational Complexity of Discrete Problems", March/2017]

Motivation

Question. Is there $f \in \mathsf{P}$ such that f does not admit non-uniform circuits of size $O(n^k)$?

Natural candidates:

- The ℓ-clique problem on n-vertex graphs?
- Languages obtained by diagonalization in the time hierarchy theorem?

Motivation

Question. Is there $f \in \mathrm{P}$ such that f does not admit non-uniform circuits of size $O(n^k)$?

Natural candidates:

- The ℓ-clique problem on n-vertex graphs?
- Languages obtained by diagonalization in the time hierarchy theorem?

As far as we know, every problem in P might admit linear size circuits.

Motivation

Question. Is there $f \in \mathsf{P}$ such that f does not admit non-uniform circuits of size $O(n^k)$?

Natural candidates:

- The ℓ-clique problem on n-vertex graphs?
- Languages obtained by diagonalization in the time hierarchy theorem?

As far as we know, every problem in P might admit linear size circuits.

Can we at least show that some formal theories cannot prove that $\mathsf{P} \subseteq \mathsf{SIZE}(n^k)$?

Previous Work

- Several works on barriers and on the difficulty of proving lower bounds.

  (important results, but often conditional, or restricted to a limited set of techniques.)

Previous Work

- Several works on barriers and on the difficulty of proving lower bounds.

  (important results, but often conditional, or restricted to a limited set of techniques.)

- We obtain results on the unprovability of upper bounds in a reasonably general and established framework (unconditionally).

Previous Work

- Several works on barriers and on the difficulty of proving lower bounds.

  (important results, but often conditional, or restricted to a limited set of techniques.)

- We obtain results on the unprovability of upper bounds in a reasonably general and established framework (unconditionally).

The closest reference seems to be

S. Cook and J. Krajíček, "*Consequences of the provability of* $\mathrm{NP} \subseteq \mathrm{P/poly}$", 2007.

where conditional independence results were obtained for the theories PV, S^1_2, and S^2_2.

Summary of the talk

1. Explain idea behind the formalization of a circuit upper bound as a formal sentence.

Summary of the talk

1. Explain idea behind the formalization of a circuit upper bound as a formal sentence.

2. Discuss a theory (PV) that "understands" this sentence, and mention results that can be formulated and proved in PV.

Summary of the talk

1. Explain idea behind the formalization of a circuit upper bound as a formal sentence.

2. Discuss a theory (PV) that “understands” this sentence, and mention results that can be formulated and proved in PV.

3. Sketch the ideas behind the argument that PV cannot prove that $\mathsf{P} \subseteq \mathsf{SIZE}(n^k)$, formalized as in **1.** above.

Summary of the talk

1. Explain idea behind the formalization of a circuit upper bound as a formal sentence.

2. Discuss a theory (PV) that "understands" this sentence, and mention results that can be formulated and proved in PV.

3. Sketch the ideas behind the argument that PV cannot prove that P $\subseteq$ SIZE(n^k), formalized as in **1.** above.

4. Discussion and open problems.

1. Formalizing non-uniform circuit upper bounds

Informal statement

For a function symbol f and $k, c \geq 1$,

we write a sentence to express that the language $L_f \subseteq \{0, 1\}^*$ computed by f has circuits of size $\leq cn^k$:

Informal statement

For a function symbol f and $k, c \geq 1$,

we write a sentence to express that the language $L_f \subseteq \{0, 1\}^*$ computed by f has circuits of size $\leq cn^k$:

Informally,

$\forall n \in \mathbb{N}$

Informal statement

For a function symbol f and $k, c \geq 1$,

we write a sentence to express that the language $L_f \subseteq \{0, 1\}^*$ computed by f has circuits of size $\leq cn^k$:

Informally,

$$\forall n \in \mathbb{N} \;\; \exists \text{ circuit } C_n$$

Informal statement

For a function symbol f and $k, c \geq 1$,

we write a sentence to express that the language $L_f \subseteq \{0,1\}^*$ computed by f has circuits of size $\leq cn^k$:

Informally,

$$\forall n \in \mathbb{N} \;\; \exists \text{ circuit } C_n \;\; \forall x \in \{0,1\}^n$$

Informal statement

For a function symbol f and $k, c \geq 1$,

> we write a sentence to express that the language $L_f \subseteq \{0,1\}^*$ computed by f has circuits of size $\leq cn^k$:

Informally,

$$\forall n \in \mathbb{N} \;\; \exists \text{ circuit } C_n \;\; \forall x \in \{0,1\}^n \;\; \big(\text{size}(C_n) \leq cn^k \wedge (f(x) \neq 0 \leftrightarrow C_n(x) = 1)\big).$$

Informal statement

For a function symbol f and $k, c \geq 1$,

> we write a sentence to express that the language $L_f \subseteq \{0,1\}^*$ computed by f has circuits of size $\leq cn^k$:

Informally,

$$\forall n \in \mathbb{N} \ \ \exists \text{ circuit } C_n \ \ \forall x \in \{0,1\}^n \ \ \big(\text{size}(C_n) \leq cn^k \wedge (f(x) \neq 0 \leftrightarrow C_n(x) = 1)\big).$$

- What is $\mathbb{N}$? What about $\{0,1\}^n$? A circuit? Symbol "$\in$"? Etc.

Formal statement: The sentence $\mathrm{UP}_{k,c}(f)$

$\mathrm{UP}_{k,c}(f)$:

$$\forall z\, \exists C\, \forall x\, \left[\mathrm{Circuit}(C) \wedge \mathrm{size}(C) \leq c|z|^k \wedge \Big(|x| = |z| \rightarrow (f(x) \neq 0 \leftrightarrow \mathrm{CircEval}(C, x) = 1)\Big)\right].$$

Formal statement: The sentence $\mathrm{UP}_{k,c}(f)$

$\mathrm{UP}_{k,c}(f)$:

$$\forall z\, \exists C\, \forall x\, \left[\mathrm{Circuit}(C) \wedge \mathrm{size}(C) \leq c|z|^k \wedge \Big(|x| = |z| \to (f(x) \neq 0 \leftrightarrow \mathrm{CircEval}(C, x) = 1)\Big)\right].$$

z, C, x are first-order variables (quantified over the same domain).

Formal statement: The sentence $\mathrm{UP}_{k,c}(f)$

$\mathrm{UP}_{k,c}(f)$:

$$\forall z\, \exists C\, \forall x\, \Big[\mathrm{Circuit}(C) \wedge \mathrm{size}(C) \leq c|z|^k \wedge \Big(|x| = |z| \to (f(x) \neq 0 \leftrightarrow \mathrm{CircEval}(C, x) = 1)\Big)\Big].$$

z, C, x are first-order variables (quantified over the same domain).

$|\cdot|$ is a function symbol, and one should think of $|z|$ as the parameter n.

Formal statement: The sentence $\mathrm{UP}_{k,c}(f)$

$\mathrm{UP}_{k,c}(f)$:

$$\forall z\, \exists C\, \forall x\, \Big[\mathrm{Circuit}(C) \wedge \mathrm{size}(C) \leq c|z|^k \wedge \Big(|x| = |z| \rightarrow (f(x) \neq 0 \leftrightarrow \mathrm{CircEval}(C, x) = 1)\Big)\Big].$$

z, C, x are first-order variables (quantified over the same domain).

$|\cdot|$ is a function symbol, and one should think of $|z|$ as the parameter n.

$\mathrm{size}(\cdot)$, $\mathrm{CircEval}(\cdot,\cdot)$, $\leq$, and $f(\cdot)$ are predicate/function symbols.

Formal statement: The sentence $\mathrm{UP}_{k,c}(f)$

$\mathrm{UP}_{k,c}(f)$:

$$\forall z\, \exists C\, \forall x\, \Big[\mathrm{Circuit}(C) \wedge \mathrm{size}(C) \leq c|z|^k \wedge \Big(|x| = |z| \rightarrow (f(x) \neq 0 \leftrightarrow \mathrm{CircEval}(C, x) = 1)\Big)\Big].$$

z, C, x are first-order variables (quantified over the same domain).

$|\cdot|$ is a function symbol, and one should think of $|z|$ as the parameter n.

$\mathrm{size}(\cdot)$, $\mathrm{CircEval}(\cdot,\cdot)$, $\leq$, and $f(\cdot)$ are predicate/function symbols.

$|z|^k$ means $|z| \times \ldots \times |z|$, etc. (we have function symbols $+$ and $\times$).

$\mathrm{UP}_{k,c}(f)$

$\mathrm{UP}_{k,c}(f)$:

$$\forall z\ \exists C\ \forall x\ \left[\mathrm{Circuit}(C) \wedge \mathrm{size}(C) \leq c|z|^k \wedge \left(|x| = |z| \rightarrow (f(x) \neq 0 \leftrightarrow \mathrm{CircEval}(C, x) = 1)\right)\right].$$

- This is just a sequence of symbols. In order to manipulate the symbols and derive true statements involving formulas of this form, we use a first-order theory.

$\mathsf{UP}_{k,c}(f)$

$\mathsf{UP}_{k,c}(f)$:

$$\forall z\, \exists C\, \forall x\, \Big[\mathsf{Circuit}(C) \wedge \mathsf{size}(C) \leq c|z|^k \wedge \Big(|x| = |z| \rightarrow (f(x) \neq 0 \leftrightarrow \mathsf{CircEval}(C, x) = 1)\Big)\Big].$$

- This is just a sequence of symbols. In order to manipulate the symbols and derive true statements involving formulas of this form, we use a first-order theory.

- We need a theory that is connected to uniform polynomial time computations, and that can use first-order quantifiers.

2. The first-order theory PV

(informal discussion)

Background

- PV (“Polynomially Verifiable”) introduced as an equational theory by S. Cook in 1975:
  “Feasibly constructive proofs and the propositional calculus”.

Based on work of Cobham (1965) characterizing p-time functions by a function algebra.

Motivation: Formalizes feasible reasoning, connection to NP vs. coNP problem (propositional translations).

Background

- PV ("Polynomially Verifiable") introduced as an equational theory by S. Cook in 1975: *"Feasibly constructive proofs and the propositional calculus".*

Based on work of Cobham (1965) characterizing p-time functions by a function algebra.

Motivation: Formalizes feasible reasoning, connection to NP vs. coNP problem (propositional translations).

- First-order formulation (PV_1) presented in Krajíček, Pudlák, Takeuti (1991) as a conservative extension of the equational theory.

Background, cont.

- Definition of PV is technical. Some details not particularly important in our argument.

- Indeed, our unprovability results extends to the theory containing all true (in $\mathbb{N}$) universal sentences in the vocabulary $\mathcal{L}_{\mathsf{PV}}$ of PV.

Background, cont.

- Definition of PV is technical. Some details not particularly important in our argument.

- Indeed, our unprovability results extends to the theory containing all true (in $\mathbb{N}$) universal sentences in the vocabulary $\mathcal{L}_{\mathsf{PV}}$ of PV.

We shall give a brief (and incomplete) introduction to PV on the next few slides.
(A formal treatment appears in Section 5.3 of Krajíček's red book.)

An essentially equivalent formulation of the theory (perhaps more accessible) appears in:

E. Jeřábek, *The strength of sharply bounded induction*, 2006.

PV and its vocabulary $\mathcal{L}_{\mathsf{PV}}$

- Intended structure interpreting the symbols of PV is $\mathbb{N}$, together with p-time functions $\tilde{f}\colon \mathbb{N}^\ell \to \mathbb{N}$ interpreting each function symbol ("p-time algorithm") $f \in \mathcal{L}_{\mathsf{PV}}$.

PV and its vocabulary $\mathcal{L}_{\mathsf{PV}}$

- Intended structure interpreting the symbols of PV is $\mathbb{N}$, together with p-time functions $\tilde{f}\colon \mathbb{N}^{\ell} \to \mathbb{N}$ interpreting each function symbol ("p-time algorithm") $f \in \mathcal{L}_{\mathsf{PV}}$.

- Informally, we view $\{0,1\}^{\star} \leftrightarrow \mathbb{N}$, with the intention that $\forall z$, $\exists C$, $\forall x$ quantify over the same domain (numbers represent Boolean circuits, input strings, etc.).

PV and its vocabulary $\mathcal{L}_{\mathsf{PV}}$

- Intended structure interpreting the symbols of PV is $\mathbb{N}$, together with p-time functions $\tilde{f}\colon \mathbb{N}^{\ell} \to \mathbb{N}$ interpreting each function symbol ("p-time algorithm") $f \in \mathcal{L}_{\mathsf{PV}}$.

- Informally, we view $\{0,1\}^{\star} \leftrightarrow \mathbb{N}$, with the intention that $\forall z, \exists C, \forall x$ quantify over the same domain (numbers represent Boolean circuits, input strings, etc.).

- The function symbols in $\mathcal{L}_{\mathsf{PV}}$ and (part of) the axioms of PV are introduced simultaneously, based on Cobham's characterization of FP.

PV and its vocabulary $\mathcal{L}_{\mathrm{PV}}$: Cobham's Theorem (1965)

Cobham's Theorem. FP is equivalent to the set of functions in $\mathbb{N}^k \to \mathbb{N}$, $k \geq 1$, obtained from the base functions below by composition and limited iteration on notation.

Base functions. 0, S, $\lfloor \frac{x}{2} \rfloor$, $2x$, $x \leq y$, $\mathrm{Choice}(x, y, z)$. (i.e. simple AC^0 functions)

PV and its vocabulary $\mathcal{L}_{\mathrm{PV}}$: Cobham's Theorem (1965)

Cobham's Theorem. FP is equivalent to the set of functions in $\mathbb{N}^k \to \mathbb{N}$, $k \geq 1$, obtained from the base functions below by composition and limited iteration on notation.

Base functions. $0, \quad S, \quad \lfloor \frac{x}{2} \rfloor, \quad 2x, \quad x \leq y, \quad \text{Choice}(x, y, z).$ (i.e. simple AC^0 functions)

Limited iteration on notation.

$$
\begin{aligned}
f(\vec{x}, 0) &= g(\vec{x}) \\
f(\vec{x}, y) &= h(\vec{x}, y, f(\vec{x}, \lfloor \frac{y}{2} \rfloor)),
\end{aligned}
$$

PV and its vocabulary $\mathcal{L}_{\mathsf{PV}}$: Cobham's Theorem (1965)

Cobham's Theorem. FP is equivalent to the set of functions in $\mathbb{N}^k \to \mathbb{N}$, $k \geq 1$, obtained from the base functions below by composition and limited iteration on notation.

Base functions. 0, S, $\lfloor \frac{x}{2} \rfloor$, $2x$, $x \leq y$, $\text{Choice}(x, y, z)$. (i.e. simple AC^0 functions)

Limited iteration on notation.

$$\begin{aligned} f(\vec{x}, 0) &= g(\vec{x}) \\ f(\vec{x}, y) &= h(\vec{x}, y, f(\vec{x}, \lfloor \frac{y}{2} \rfloor)), \end{aligned}$$

provided that $|f(\vec{x}, y)| \leq q(|\vec{x}|, |y|)$ for a fixed polynomial q and for all $\vec{x}, y \in \mathbb{N}$, where $|x| \stackrel{\text{def}}{=} \lceil \log(x + 1) \rceil$ is the length of the binary representation of x.

PV and its vocabulary $\mathcal{L}_{\mathsf{PV}}$, cont.

- As a new algorithm f is defined from previous ones:
  - We add a new function symbol f to $\mathcal{L}_{\mathsf{PV}}$,
  - The corresponding defining equations are added to PV as new axioms.

PV and its vocabulary $\mathcal{L}_{\mathsf{PV}}$, cont.

- As a new algorithm f is defined from previous ones:
  - We add a new function symbol f to $\mathcal{L}_{\mathsf{PV}}$,
  - The corresponding defining equations are added to PV as new axioms.

- PV has also a form of induction axiom that simulates binary search.

PV and its vocabulary $\mathcal{L}_{\mathrm{PV}}$, cont.

- As a new algorithm f is defined from previous ones:
  - We add a new function symbol f to $\mathcal{L}_{\mathrm{PV}}$,
  - The corresponding defining equations are added to PV as new axioms.

- PV has also a form of induction axiom that simulates binary search.

- We use first-order predicate calculus to reason and prove theorems in PV.

PV and its vocabulary $\mathcal{L}_{\mathrm{PV}}$, cont.

- As a new algorithm f is defined from previous ones:
  - We add a new function symbol f to $\mathcal{L}_{\mathrm{PV}}$,
  - The corresponding defining equations are added to PV as new axioms.

- PV has also a form of induction axiom that simulates binary search.

- We use first-order predicate calculus to reason and prove theorems in PV.

Remark. PV can be axiomatized by universal formulas (i.e., $\forall \vec{w}\ \phi(\vec{w})$, where ϕ is quantifier-free).

$\mathsf{UP}_{k,c}(f)$ as a sentence in $\mathcal{L}_{\mathsf{PV}}$

Recall $\mathsf{UP}_{k,c}(f)$:

$$\forall z\ \exists C\ \forall x\ \Big[\mathsf{Circuit}(C) \wedge \mathsf{size}(C) \leq c|z|^k \wedge \Big(|x| = |z| \rightarrow (f(x) \neq 0 \leftrightarrow \mathsf{CircEval}(C, x) = 1)\Big)\Big].$$

- Circuit(·), size(·), CircEval(·), etc. are poly-time algorithms which can be associated to well-behaved function symbols in $\mathcal{L}_{\mathsf{PV}}$.

$\mathsf{UP}_{k,c}(f)$ as a sentence in $\mathcal{L}_{\mathsf{PV}}$

Recall $\mathsf{UP}_{k,c}(f)$:

$$\forall z\, \exists C\, \forall x\, \Big[\mathrm{Circuit}(C) \wedge \mathrm{size}(C) \leq c|z|^k \wedge \Big(|x| = |z| \rightarrow (f(x) \neq 0 \leftrightarrow \mathrm{CircEval}(C, x) = 1)\Big)\Big].$$

► Circuit($\cdot$), size($\cdot$), CircEval($\cdot$), etc. are poly-time algorithms which can be associated to well-behaved function symbols in $\mathcal{L}_{\mathsf{PV}}$.

Question. Given $k \geq 1$, is there a function symbol $h \in \mathcal{L}_{\mathsf{PV}}$ such that

$$\mathsf{PV} \nvdash \mathsf{UP}_{k,c}(h) \quad ? \quad \text{(no matter the choice of c)}$$

$\mathsf{UP}_{k,c}(f)$ as a sentence in $\mathcal{L}_{\mathsf{PV}}$

Recall $\mathsf{UP}_{k,c}(f)$:

$$\forall z\, \exists C\, \forall x\, \Big[\mathrm{Circuit}(C) \wedge \mathrm{size}(C) \le c|z|^k \wedge \Big(|x| = |z| \to (f(x) \neq 0 \leftrightarrow \mathrm{CircEval}(C, x) = 1)\Big)\Big].$$

- Circuit$(\cdot)$, size$(\cdot)$, CircEval$(\cdot)$, etc. are poly-time algorithms which can be associated to well-behaved function symbols in $\mathcal{L}_{\mathsf{PV}}$.

Question. Given $k \ge 1$, is there a function symbol $h \in \mathcal{L}_{\mathsf{PV}}$ such that

$$\mathsf{PV} \nvdash \mathsf{UP}_{k,c}(h) \;\;?$$ (no matter the choice of c)

(By construction, the definition of $h \in \mathcal{L}_{\mathsf{PV}}$ contains in its description the specification of a poly-time algorithm for h.)

The strength of PV

- Many combinatorial and complexity-theoretic statements have been formalized and proved in PV (or in theories believed to be strictly weaker than PV).

The strength of PV

- Many combinatorial and complexity-theoretic statements have been formalized and proved in PV (or in theories believed to be strictly weaker than PV).

- This often involves clever adaptations of the original arguments, approximations of probabilistic statements, discovering alternative proofs, etc.

The strength of PV, cont.

- A recent substantial formalization obtained in PV:

J. Pich, "*Logical strength of complexity theory and a formalization of the PCP Theorem in Bounded Arithmetic*, 2015.

The strength of PV, cont.

- A recent substantial formalization obtained in PV:

J. Pich, "*Logical strength of complexity theory and a formalization of the PCP Theorem in Bounded Arithmetic*, 2015.

"*The aim of this paper is to show that a lot of complexity theory can be formalized in low fragments of arithmetic like Cook's theory PV_1.*

Our motivation is to demonstrate the power of bounded arithmetic as a counterpart to the unprovability results we already have or want to obtain . . ."

The strength of PV, cont.

- A recent substantial formalization obtained in PV:

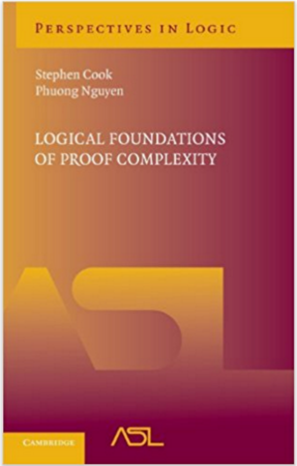
J. Pich, "*Logical strength of complexity theory and a formalization of the PCP Theorem in Bounded Arithmetic*, 2015.

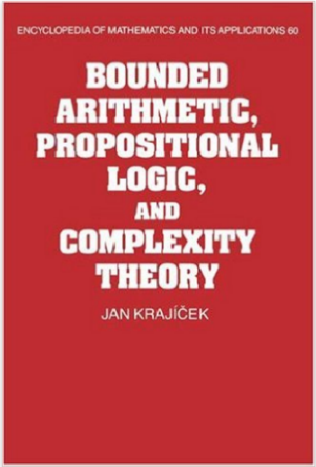
"*The aim of this paper is to show that a lot of complexity theory can be formalized in low fragments of arithmetic like Cook's theory* PV_1.

Our motivation is to demonstrate the power of bounded arithmetic as a counterpart to the unprovability results we already have or want to obtain . . ."

- Includes formalization of many other results, such as the Cook-Levin Theorem, expander graphs, etc.

For more information and background:





3. The unconditional unprovability result

(main ideas and the associated difficulties)

Main Theorem

Theorem. For every $k \geq 1$ there is a unary PV function symbol h such that for no constant $c \geq 1$ PV proves the sentence $\mathrm{UP}_{k,c}(h)$.

Theorem. For every $k \geq 1$ there is a unary PV function symbol h such that for no constant $c \geq 1$ PV proves the sentence $\mathrm{UP}_{k,c}(h)$.

Remark. $\mathrm{UP}_{k,c}(h)$ is a $\forall\exists\forall$-sentence in $\mathcal{L}_{\mathrm{PV}}$, and can be written as:

$$\mathrm{UP}_{k,c}(h) \;\equiv\; \forall z\, \exists C\, \forall x\; \phi_h(z, C, x), \text{ where } \phi_h \text{ is quantifier-free.}$$

The basic idea

- Logic/Provability as a bridge between non-uniform and uniform circuit complexity.

If PV $\vdash$ $\mathrm{UP}_{k,c}(h)$ using a proof π (list of symbols), extract from π computational information about sequence C_n of circuits computing h.

The basic idea

- Logic/Provability as a bridge between non-uniform and uniform circuit complexity.

If PV $\vdash$ $\mathrm{UP}_{k,c}(h)$ using a proof π (list of symbols), extract from π computational information about sequence C_n of circuits computing h.

- Since PV is sound, provability of a sentence implies that the sentence is true in the usual sense (in $\mathbb{N}$).

The basic idea

- Logic/Provability as a bridge between non-uniform and uniform circuit complexity.

If PV $\vdash$ $\mathrm{UP}_{k,c}(h)$ using a proof π (list of symbols), extract from π computational information about sequence C_n of circuits computing h.

- Since PV is sound, provability of a sentence implies that the sentence is true in the usual sense (in $\mathbb{N}$).

- Perhaps contradict known (unconditional) lower bounds in uniform circuit complexity ?

The basic idea

- Logic/Provability as a bridge between non-uniform and uniform circuit complexity.

If PV $\vdash$ $\mathrm{UP}_{k,c}(h)$ using a proof π (list of symbols), extract from π computational information about sequence C_n of circuits computing h.

- Since PV is sound, provability of a sentence implies that the sentence is true in the usual sense (in $\mathbb{N}$).

- Perhaps contradict known (unconditional) lower bounds in uniform circuit complexity ?

(We will later explain why this natural approach is problematic.)

Techniques

Standard tools from logic and complexity, which build on other important results:

- Uniform circuit lower bounds (Santhanam-Williams, 2014).
- Formalization of the argument from Santhanam-Williams in PV.
- Axiomatization of PV as a universal theory.
- Herbrand's Theorem from mathematical logic.
- Krajicek-Pudlak-Takeuti Theorem (KPT) from bounded arithmetic.
- (Non-constructive) Inductive argument.

The uniform lower bound

R. Santhanam and R. Williams, "*On uniformity and circuit lower bounds*", 2014.

Theorem. For every $k \geq 1$, there is $L \in \mathsf{P}$ such that $L \notin$ P-uniform-SIZE(n^k).

The uniform lower bound

R. Santhanam and R. Williams, "*On uniformity and circuit lower bounds*", 2014.

Theorem. For every $k \geq 1$, there is $L \in \mathrm{P}$ such that $L \notin$ P-uniform-SIZE(n^k).

Why is this result so special?

$L \in \mathrm{DTIME}(n^\ell)$, but P-uniform generating algorithm can run in time n^{2^ℓ}, $n^{2^{2^{\ell \cdot k}}}$, etc.

The uniform lower bound

R. Santhanam and R. Williams, "*On uniformity and circuit lower bounds*", 2014.

Theorem. For every $k \geq 1$, there is $L \in \mathsf{P}$ such that $L \notin$ P-uniform-SIZE(n^k).

Why is this result so special?

$L \in \mathsf{DTIME}(n^\ell)$, but P-uniform generating algorithm can run in time n^{2^ℓ}, $n^{2^{2^{\ell \cdot k}}}$, etc.

▶ Proof is a clever win-win argument by contradiction (non-constructive), and relies on a time hierarchy theorem with advice.

The uniform lower bound

R. Santhanam and R. Williams, "*On uniformity and circuit lower bounds*", 2014.

Theorem. For every $k \geq 1$, there is $L \in \mathrm{P}$ such that $L \notin$ P-uniform-SIZE(n^k).

Why is this result so special?

$L \in \mathrm{DTIME}(n^\ell)$, but P-uniform generating algorithm can run in time n^{2^ℓ}, $n^{2^{2^{\ell \cdot k}}}$, etc.

► Proof is a clever win-win argument by contradiction (non-constructive), and relies on a time hierarchy theorem with advice.

► **Our Approach.** From a PV-proof of $\mathrm{UP}_{k,c}(h)$, we try to extract a poly-time generating algorithm. We can't control its p-time bound, but this is okay with the theorem above!

The KPT Witnessing Theorem

J. Krajíček, P. Pudlák, and G. Takeuti: "*Bounded arithmetic and the polynomial hierarchy*", 1991.

Theorem. Assume T is a universal theory with vocabulary $\mathcal{L}$, ϕ is a quantifier-free $\mathcal{L}$-formula, and

$$T \vdash \forall z \, \exists C \, \forall x \;\; \phi(z, C, x) \; .$$

Then there exist a constant $d \geq 1$ and a finite sequence $t_1, \ldots, t_d$ of $\mathcal{L}$-terms such that

$$T \vdash \phi(z, t_1(z), x_1) \; \vee \; \phi(z, t_2(z, x_1), x_2) \; \vee \; \ldots \; \vee \; \phi(z, t_d(z, x_1, \ldots, x_{d-1}), x_d).$$

The KPT Witnessing Theorem

J. Krajíček, P. Pudlák, and G. Takeuti: "*Bounded arithmetic and the polynomial hierarchy*", 1991.

Theorem. Assume T is a <u>universal</u> theory with vocabulary $\mathcal{L}$, ϕ is a quantifier-free $\mathcal{L}$-formula, and

$$T \vdash \forall z \, \exists C \, \forall x \;\; \phi(z, C, x) \; .$$

Then there exist a constant $d \geq 1$ and a finite sequence $t_1, \ldots, t_d$ of $\mathcal{L}$-terms such that

$$T \vdash \phi(z, t_1(z), x_1) \;\vee\; \phi(z, t_2(z, x_1), x_2) \;\vee\; \ldots \;\vee\; \phi(z, t_d(z, x_1, \ldots, x_{d-1}), x_d).$$

- The result can be established using proof theory or model theory.

Applying the KPT Theorem to PV and $\mathrm{UP}_{k,c}(f)$

- Fix $k \geq 1$, and assume that for every $f \in \mathcal{L}_{\mathrm{PV}}$ we have $c \geq 1$ such that

$$\mathrm{PV} \vdash \mathrm{UP}_{k,c}(f) \qquad \text{Recall that this is } \forall z\, \exists C\, \forall x\, \phi_f(z, C, x).$$

Applying the KPT Theorem to PV and $\mathrm{UP}_{k,c}(f)$

- Fix $k \geq 1$, and assume that for every $f \in \mathcal{L}_{\mathrm{PV}}$ we have $c \geq 1$ such that

$$\mathrm{PV} \vdash \mathrm{UP}_{k,c}(f) \qquad \text{Recall that this is } \forall z\, \exists C\, \forall x\, \phi_f(z, C, x).$$

- Assume we get $d = 1$ after applying the KPT statement, i.e.,

$$\mathrm{PV} \vdash \phi_f(z, t_1^f(z), x_1)\ , \qquad \text{where } t_1^f(z) \text{ is an } \mathcal{L}_{\mathrm{PV}}\text{-term.}$$

Applying the KPT Theorem to PV and $\mathrm{UP}_{k,c}(f)$

- Fix $k \geq 1$, and assume that for every $f \in \mathcal{L}_{\mathrm{PV}}$ we have $c \geq 1$ such that

$$\mathrm{PV} \vdash \mathrm{UP}_{k,c}(f) \qquad \text{Recall that this is } \forall z\, \exists C\, \forall x\; \phi_f(z, C, x).$$

- Assume we get $d = 1$ after applying the KPT statement, i.e.,

$$\mathrm{PV} \vdash \phi_f(z, t_1^f(z), x_1)\;, \qquad \text{where } t_1^f(z) \text{ is an } \mathcal{L}_{\mathrm{PV}}\text{-term.}$$

- Then, by the soundness of PV, if we set z to be some n-bit integer $1^{(n)}$,

$$\mathbb{N} \models \forall x_1\; \phi_f(1^{(n)}, t_1^f(1^{(n)}), x_1).$$

Applying the KPT Theorem to PV and $\mathrm{UP}_{k,c}(f)$

- Fix $k \geq 1$, and assume that for every $f \in \mathcal{L}_{\mathrm{PV}}$ we have $c \geq 1$ such that

$$\mathrm{PV} \vdash \mathrm{UP}_{k,c}(f) \qquad \text{Recall that this is } \forall z\, \exists C\, \forall x\; \phi_f(z, C, x).$$

- Assume we get $d = 1$ after applying the KPT statement, i.e.,

$$\mathrm{PV} \vdash \phi_f(z, t_1^f(z), x_1)\,, \qquad \text{where } t_1^f(z) \text{ is an } \mathcal{L}_{\mathrm{PV}}\text{-term.}$$

- Then, by the soundness of PV, if we set z to be some n-bit integer $1^{(n)}$,

$$\mathbb{N} \models \forall x_1\; \phi_f(1^{(n)}, t_1^f(1^{(n)}), x_1).$$

- Now $t_1^f(1^{(n)})$, a term in PV, corresponds in $\mathbb{N}$ to a poly-time computation.
  The assumption that we get this for all $f \in \mathcal{L}_{\mathrm{PV}}$ contradicts Santhanam-Williams.

Applying the KPT Theorem to PV and $\mathrm{UP}_{k,c}(f)$

- Fix $k \geq 1$, and assume that <u>for every</u> $f \in \mathcal{L}_{\mathrm{PV}}$ we have $c \geq 1$ such that

$$\mathrm{PV} \vdash \mathrm{UP}_{k,c}(f) \qquad \text{Recall that this is } \forall z\, \exists C\, \forall x\, \phi_f(z, C, x).$$

- Assume we get $d = 1$ after applying the KPT statement, i.e.,

$$\mathrm{PV} \vdash \phi_f(z, t_1^f(z), x_1)\,, \qquad \text{where } t_1^f(z) \text{ is an } \mathcal{L}_{\mathrm{PV}}\text{-term.}$$

- Then, by the soundness of PV, if we set z to be some n-bit integer $1^{(n)}$,

$$\mathbb{N} \models \forall x_1\, \phi_f(1^{(n)}, t_1^f(1^{(n)}), x_1).$$

- Now $t_1^f(1^{(n)})$, a term in PV, corresponds in $\mathbb{N}$ to a poly-time computation.
  The assumption that we get this for all $f \in \mathcal{L}_{\mathrm{PV}}$ contradicts Santhanam-Williams. $\square$

The general case

- If $d > 1$, we obtain from $\mathsf{PV} \vdash \mathsf{UP}_{k,c}(f)$ the more general scenario:

$$\mathbb{N} \models \phi(z, t_1(z), x_1) \lor \phi(z, t_2(z, x_1), x_2) \lor \ \ldots \ \lor \phi(z, t_d(z, x_1, \ldots, x_{d-1}), x_d).$$

The general case

- If $d > 1$, we obtain from $\mathrm{PV} \vdash \mathrm{UP}_{k,c}(f)$ the more general scenario:

$$\mathbb{N} \models \phi(z, t_1(z), x_1) \vee \phi(z, t_2(z, x_1), x_2) \vee \ldots \vee \phi(z, t_d(z, x_1, \ldots, x_{d-1}), x_d).$$

Either $t_1(1^{(n)})$ outputs a correct circuit for f, or

There is a counter-example $a_1 \in \{0,1\}^n$, and $t_2(1^{(n)}, a_1)$ outputs a correct circuit, or

$\ldots$

The general case

- If $d > 1$, we obtain from $\text{PV} \vdash \text{UP}_{k,c}(f)$ the more general scenario:

$$\mathbb{N} \models \phi(z, t_1(z), x_1) \lor \phi(z, t_2(z, x_1), x_2) \lor \ldots \lor \phi(z, t_d(z, x_1, \ldots, x_{d-1}), x_d).$$

Either $t_1(1^{(n)})$ outputs a correct circuit for f, or

There is a counter-example $a_1 \in \{0,1\}^n$, and $t_2(1^{(n)}, a_1)$ outputs a correct circuit, or

$\ldots$

- Due to the counter-examples, we can only show that $f \in [\text{P-uniform} \,/\, O(n)]\text{-SIZE}(n^k)$.

The general case

- If $d > 1$, we obtain from $\mathsf{PV} \vdash \mathsf{UP}_{k,c}(f)$ the more general scenario:

$$\mathbb{N} \models \phi(z, t_1(z), x_1) \ \vee \ \phi(z, t_2(z, x_1), x_2) \ \vee \ \ldots \ \vee \ \phi(z, t_d(z, x_1, \ldots, x_{d-1}), x_d).$$

Either $t_1(1^{(n)})$ outputs a correct circuit for f, or

There is a counter-example $a_1 \in \{0,1\}^n$, and $t_2(1^{(n)}, a_1)$ outputs a correct circuit, or

$\ldots$

- Due to the counter-examples, we can only show that $f \in$ [P-uniform / $O(n)$]-SIZE(n^k).

- **Contradiction? A difficulty is the lack of super-linear non-uniform lower bounds!**

How to establish an unconditional unprovability result?

- Apply KPT to a specific $\mathsf{UP}_{k,c}(g)$, obtaining a disjunction of $\leq d$ formulas, $d \in \mathbb{N}$.
  (We will eliminate one by one in d stages, until we get a contradiction.)

How to establish an unconditional unprovability result?

- Apply KPT to a specific $\mathrm{UP}_{k,c}(g)$, obtaining a disjunction of $\leq d$ formulas, $d \in \mathbb{N}$.
  (We will eliminate one by one in d stages, until we get a contradiction.)

- To handle each elimination step, we formalize the SW win-win argument inside PV.

How to establish an unconditional unprovability result?

- Apply KPT to a specific $\mathrm{UP}_{k,c}(g)$, obtaining a disjunction of $\leq d$ formulas, $d \in \mathbb{N}$.
  (We will eliminate one by one in d stages, until we get a contradiction.)

- To handle each elimination step, we formalize the SW win-win argument inside PV.

The following ideas are crucial:

- Using the constructivity of PV and Herbrand's Theorem, it can be shown that the counter-examples that previously caused difficulties can be provably witnessed in PV.

How to establish an unconditional unprovability result?

- Apply KPT to a specific $\mathrm{UP}_{k,c}(g)$, obtaining a disjunction of $\leq d$ formulas, $d \in \mathbb{N}$.
  (We will eliminate one by one in d stages, until we get a contradiction.)

- To handle each elimination step, we formalize the SW win-win argument inside PV.

The following ideas are crucial:

- Using the constructivity of PV and Herbrand's Theorem, it can be shown that the counter-examples that previously caused difficulties can be provably witnessed in PV.

- In the SW win-win analysis, the second case only needs a non-uniform assumption. This allows us to move from d to $d - 1$ (our result is about non-uniform upper bounds!).

How to establish an unconditional unprovability result?

- Apply KPT to a specific $\mathsf{UP}_{k,c}(g)$, obtaining a disjunction of $\leq d$ formulas, $d \in \mathbb{N}$.
  (We will eliminate one by one in d stages, until we get a contradiction.)

- To handle each elimination step, we formalize the SW win-win argument inside PV.

The following ideas are crucial:

- Using the constructivity of PV and Herbrand's Theorem, it can be shown that the counter-examples that previously caused difficulties can be provably witnessed in PV.

- In the SW win-win analysis, the second case only needs a non-uniform assumption. This allows us to move from d to $d - 1$ (our result is about non-uniform upper bounds!).

Check our paper for more details!

4. Remarks and open problems

Consistency of lower bounds

Given k and a "hard" $h \in \mathcal{L}_{\mathsf{PV}}$, by a standard compactness argument over the formulas

$$\mathsf{PV} \ \cup \ \{\neg \mathsf{UP}_{c,k}(h) \mid c \in \mathbb{N}\},$$

Corollary. For every $k \geq 1$ there exists a unary PV function symbol h and a model $\mathfrak{M}_k$ of PV such that for every $c \geq 1$,

$$\mathfrak{M}_k \ \models \ \neg UP_{k,c}(h).$$

Consistency of lower bounds, cont.

- From the point of view of the structure $\mathfrak{M}_k$, there are poly-time computations that require non-uniform circuits of size $\omega(n^k)$.

Consistency of lower bounds, cont.

- From the point of view of the structure $\mathfrak{M}_k$, there are poly-time computations that require non-uniform circuits of size $\omega(n^k)$.

- Thanks to the strength of PV, this means that a reasonable fraction of complex. theory can be developed assuming $\omega(n^k)$ non-uniform lower bounds, without ever producing a contradiction.

Consistency of lower bounds, cont.

- From the point of view of the structure $\mathfrak{M}_k$, there are poly-time computations that require non-uniform circuits of size $\omega(n^k)$.

- Thanks to the strength of PV, this means that a reasonable fraction of complex. theory can be developed assuming $\omega(n^k)$ non-uniform lower bounds, without ever producing a contradiction.

(In the spirit, for instance, of ZF Set Theory and the consistency of the Axiom of Choice.)

Open problems and directions

- Prove a similar independence result for theories stronger than PV.

Example: $\mathsf{APC}_1 \stackrel{\text{def}}{=} \mathsf{PV} + \mathsf{dWPHP}(L_{\mathsf{PV}})$, a theory that formalizes many probabilistic arguments and randomized algorithms (Jeřábek's phd thesis, 2005), including:

Lovász Local Lemma and Goldreich-Levin [DaiTriManLe'14], Parity $\notin \mathsf{AC}^0$ [Krajicek'95], etc.

Open problems and directions

- Prove a similar independence result for theories stronger than PV.

Example: $APC_1 \stackrel{\text{def}}{=} PV + dWPHP(L_{PV})$, a theory that formalizes many probabilistic arguments and randomized algorithms (Jeřábek's phd thesis, 2005), including:

Lovász Local Lemma and Goldreich-Levin [DaiTriManLe'14], Parity $\notin AC^0$ [Krajicek'95], etc.

- Obtain an explicit function symbol h in our result (instead of only an existential proof).

Open problems and directions

- Prove a similar independence result for theories stronger than PV.

Example: $\mathsf{APC}_1 \stackrel{\text{def}}{=} \mathsf{PV} + \mathsf{dWPHP}(L_{\mathsf{PV}})$, a theory that formalizes many probabilistic arguments and randomized algorithms (Jeřábek's phd thesis, 2005), including:

Lovász Local Lemma and Goldreich-Levin [DaiTriManLe'14], Parity $\notin \mathsf{AC}^0$ [Krajicek'95], etc.

- Obtain an explicit function symbol h in our result (instead of only an existential proof).

- Establish the same unprovability result under a $\exists\forall\exists\forall$-formalization of the upper bound statement, which also quantifies over the parameter c in the size bound cn^k.

Thank you.