Теоремы об ускорении для арифметики Пресбургера

Федор Пахомов
ВШЭ. Факультет математики
Математический институт им. В.А. Стеклова
pakhfn@gmail.com

Междисциплинарный семинар «Математика, компьютерные технологии и информационные технологии»
ВШЭ. Факультет компьютерных наук
12 декабря 2017

Abstract Proof Systems

Abstract polynomial proof system $\mathcal{S} = (\mathcal{L}, \mathcal{P}, \mathrm{Prf})$:

- $\mathcal{L}$ is the set of formulas
- $\mathcal{P}$ is the set of proofs
- relation $\mathrm{Prf}(p, \varphi)$, for $\varphi \in \mathcal{L}$ and $p \in \mathcal{P}$
- here $\mathcal{L}$ and $\mathcal{P}$ are set of strings in finite alphabet
- $\mathrm{Prf}(p, \varphi)$ is `PTIME`-decidable property

We will be interested in the situations when $\mathcal{L}$ is propositional language $\mathcal{L}_{PC}$ or set of sentences $\mathcal{L}_{\mathsf{T}}$ of the language of some first-order theory T.

Speed-up

Suppose $\mathcal{S} = (\mathcal{L}, \mathcal{P}, \mathrm{Prf})$ is a proof system.
We write $\mathcal{S} \vdash^n \varphi$ if $\varphi \in \mathcal{L}$ and there exists $p \in \mathcal{P}$ such that $\mathrm{Prf}(p, \varphi)$ and $|p| \leq n$.

Suppose $\mathcal{S}_1 = (\mathcal{L}_1, \mathcal{P}_1, \mathrm{Prf}_1)$ and $\mathcal{S}_2 = (\mathcal{L}_2, \mathcal{P}_2, \mathrm{Prf}_2)$.
We say that there is $f : \mathbb{N} \to \mathbb{N}$ speed-up of $\mathcal{S}_1$ over $\mathcal{S}_2$ if there are sequences

$$\varphi_1, \varphi_2, \ldots \in \mathcal{L}_1 \cap \mathcal{L}_2 \qquad n_1 < n_2 < \ldots$$

$$\mathcal{S}_1 \vdash \varphi_i \qquad \mathcal{S}_2 \vdash \varphi_i$$

$$\mathcal{S}_1 \vdash^{n_i} \varphi_i \qquad \mathcal{S}_2 \nvdash^{f(n)} \varphi_i$$

Propositional and First-order Proof System

Proof systems	Propositional	language of PA
typical speed-up	super-polynomial at most exponential	super-exponential or arbitrary recursive
methods to prove speed-up	various combinatorial	digitalization and Gödel's 2nd incompleteness

Theorem (Cook and Reckhow '79)

There exists a propositional proof system $\mathcal{S}$ such that if $\mathtt{NP} = \mathtt{co\text{-}NP}$ *then there is a polynomial $p(x)$:*

$$\mathcal{S} \vdash \varphi \Rightarrow \mathcal{S} \vdash^{p(n)} \varphi$$

Arbitrary recursive speed-up

Theorem (Gödel '36)

For Peano arithmetic PA *and any recursive* $f : \mathbb{N} \to \mathbb{N}$ *there is a sequence of formulas*

$$\varphi_1, \varphi_2, \ldots \in \mathcal{PA} \quad \mathsf{PA} \vdash \varphi_i \quad \mathsf{PA} \nvdash^{f(|\varphi_i|)} \varphi_i.$$

Theorem (Ehrenfeucht and Mycielski '71)

If theory $\mathsf{T} + \neg\varphi$ *is undecidable then* $\mathsf{T} + \varphi$ *have arbitrary recursive speed-up over* T.

Conservative extensions

$$\exp^*(0) = 1 \quad \exp^*(n+1) = 2^{\exp^*(n)}$$

NBG (von Neumann, Bernays, Gödel set-theory) is a set-theory with classes as explicit objects. NBG is a conservative extension of ZFC, i.e. they prove the same theorems in the language of pure set-theory (without classes).

Theorem (Pudlák '86)

NGB *have* $\exp^*(x^\varepsilon)$ *speed-up over* ZFC, *for some* $\varepsilon > 0$.
ACA_0 *have* $\exp^*(x^\varepsilon)$ *speed-up over* PA, *for some* $\varepsilon > 0$.

Theorem (Pudlák)

Sequent calculus for first-order logic with cuts $\mathsf{LK}_{\mathrm{cut}}$ *have* $\exp^*(x^\varepsilon)$ *speed-up over cut-free* $\mathsf{LK}_{\mathrm{cut\text{-}free}}$, *for some* $\varepsilon > 0$.

Gödel's 2-nd incompleteness on finite domain

Robinson's arithmetic Q is essentially PA $-$ Induction.

Theorem (Gödel '31 (with further improvments))

Any consistent extension of Robinson's arithmetic Q *couldn't prove its own (Hilbert) consistency.*

Let us denote by $\mathrm{Con}(\mathsf{T}) \restriction n$ the arithmetization of statement that $\mathsf{S} \nvdash^n \varphi \wedge \neg\varphi$, for any φ.
Note that we use binary numerals and hence
$|\mathrm{Con}(\mathsf{T}) \restriction n| = \mathcal{O}(\log(n))$.

Theorem (H. Friedman (unpublished), Pudlák '85)

For any extension T *of* Q *there is* $\varepsilon > 0$ *such that*

$$\mathsf{T} \nvdash^{n^\varepsilon} \mathrm{Con}(\mathsf{T}) \restriction n.$$

Pudlák's Conjecture

Theorem (Pudlák '85)

For any "reasonable" $\mathsf{T} \supseteq \mathsf{Q}$ *(this includes finitely axiomatizable theories and natural schematic theories like* $\mathsf{PA}, \mathsf{ZFC}$*, etc.) there exist polynomial* $p(x)$ *such that*

$$\mathsf{T} \vdash^{p(n)} \mathrm{Con}(\mathsf{T}) \restriction n.$$

Conjecture (Pudlák '17)

1. *For any theory* $\mathsf{T} \supseteq \mathsf{Q}$ *there exists theory* $\mathsf{S} \supset \mathsf{T}$ *such that for any polynomial* $p(x)$ *there exists* n *such that*

$$\mathsf{T} \nvdash^{p(n)} \mathrm{Con}(\mathsf{S}) \restriction n.$$

2. *Conjecture 1. holds for* $\mathsf{S} = \mathsf{T} + \mathrm{Con}(\mathsf{T})$.

Propositional proofs and 2n incompleteness

Any arithmetical first-order theory naturally gives a (very strong) propositional proof system since propositional language could be naturally embedded in arithmetic.

Note that $|(\mathrm{Con}(\mathrm{T}) \upharpoonright n)^{\mathrm{Prop}}| = \mathcal{O}(n)$.

Essentially, Pudlak's conjecture provides propositional tautologies $(\mathrm{Con}(\mathrm{T}) \upharpoonright n)^{\mathrm{Prop}}$ that could be use to separate propositional proof system of increasing strength.

More on Pudlák's Conjecture

Theorem (Hrubeš '17)

There exists Π_1*-sentence* F *unprovable in* PA *such that for some polynomial* $p(x)$*:*

$$\mathrm{PA} \vdash^{p(n)} \mathrm{Con}(\mathrm{PA} + \mathrm{F}) \restriction n.$$

Theorem (Freund, P. '17)

For slow consistency statement $\mathrm{Con}^*(\mathrm{PA})$ *for* PA *(due to S. Friedman, Rathjen, Weiermann '13) there exists polynomial* $p(x)$*:*

$$\mathrm{PA} \vdash^{p(n)} \mathrm{Con}(\mathrm{PA} + \mathrm{Con}^*(\mathrm{PA})) \restriction n.$$

Moreover there is total recursive function $F^*_{\varepsilon_0}$ *which totality isn't provable in* PA *such that for some polynomial* $p(x)$*:*

$$\mathrm{PA} \vdash^{p(n)} \mathrm{Con}(\mathrm{PA} + \text{“}F^*_{\varepsilon_0} \text{ is total”}) \restriction n.$$

Presburger Arithmetic

Presburger arithmetic PrA is a theory in the language $\langle =, 0, 1, + \rangle$.

Axioms of PrA are

1. $\neg(0 = x + 1)$
2. $x + 1 = y + 1 \to x = y$
3. $x + 0 = x$
4. $x + (y + 1) = (x + y) + 1$
5. $\mathrm{F}(0) \to (\forall x\, (\mathrm{F}(x) \to \mathrm{F}(x + 1)) \to \forall x\, \mathrm{F}(x))$, for all formulas $\mathrm{F}(x)$ of the language of PrA

Theorem (Presburger '29)

Theory PrA *is decidable and complete.*

We consider $\mathcal{L}_{\mathrm{PrA}} \subset \mathcal{L}_{\mathrm{PA}}$.

Speed-up in Presburger Arithmetic

Theorem

For some $\varepsilon > 0$ *there is* $\exp^*(x^\varepsilon)$ *speed-up of* Q *over Presburger arithmetic.*

Note that however Q is very weak system that is not able to prove some theorem of PrA, in particular commutativity and associativity of $+$.

Moreover,

Theorem

For any consistent $\mathsf{T}, \mathsf{S} \supset \mathsf{Q}$, *if* $\mathsf{S} \vdash \mathrm{Con}(\mathsf{T})$ *then for some* $\varepsilon > 0$ *there is* $\exp^*(x^\varepsilon)$ *speed-up of* S *over* T *in the language of* PrA.

On the other hand there exists polynomial $p(x)$:

$$\mathsf{PrA} \vdash^{\exp(\exp(\exp(p(|\mathsf{F}|))))} \mathsf{F}.$$

More on Presburger Arithmetic

Theorem (Presburger '29)

Theory PrA *is decidable and complete.*

Theorem

In S^1_2 *completeness and decidability of* PrA *is equivalent to totality of exponentiation.*

Спасибо!