Speedups for elementary geometry and Presburger arithmetic

Fedor Pakhomov
Institute of Mathematics of the Czech Academy of Sciences, Prague
Steklov Mathematical Institute of the Russian Academy of Sciences, Moscow

pakhomov@math.cas.cz

Tribute to Kurt Gödel
Brno Observatory and Planetarium
Brno, Czech Republic
January 15th 2020

Gödel's speedup theorem

For a first-order theory T and formula φ we write $T \vdash^k \varphi$ if φ is provable from axioms of T by a proof that (as binary string) consists of at most k symbols.

Let PA_n be n-th order arithmetic, i.e. first order theory with n sorts, where the sort 0 is for natural numbers and the sorts $i+1$ are for sets of objects of sort i that has scheme of comprehension for all sorts.

Theorem (Gödel '36)

For any $n > 0$ and any computable $f : \mathbb{N} \to \mathbb{N}$ there is a sequence of formulas

$$\varphi_1, \varphi_2, \ldots \in \mathcal{L}_{\mathrm{PA}} \textit{ s.t. } \mathrm{PA}_{n+1} \vdash^{k_i} \varphi_i \textit{ and } \mathrm{PA}_n \nvdash^{f(|k_i|)} \varphi_i, \quad \textit{for all } i \textit{ and some } k_i\textit{'s.}$$

Generally, given proof systems T_1 and T_2 we say that there is $f : \mathbb{N} \to \mathbb{N}$ speedup of T_1 over T_2 if there are

$$\varphi_1, \varphi_2, \ldots \in \mathcal{L}_{T_2} \text{ s.t. } \mathrm{T}_1 \vdash^{k_i} \varphi_i \text{ and } \mathrm{T}_2 \nvdash^{f(|k_i|)} \varphi_i,$$

Some other speedup theorems

Theorem (Ehrenfeucht and Mycielski '71)

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

Let $\exp^*$ be the hyperexponentiation function, i.e. $\exp^*(0) = 0$ and $\exp^*(x+1) = 2^{\exp^*(x)}$.

Theorem (Pudlák '86)

NGB *has* $\exp^*(x^\varepsilon)$ *speedup over* ZFC*, for some* $\varepsilon > 0$*.*
ACA_0 *has* $\exp^*(x^\varepsilon)$ *speedup over* PA*, for some* $\varepsilon > 0$*.*

Theorem (Statman '78)

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

Theorem (Haken '85)

There is 2^{x^ε} *speedup of resolution over Frege.*

Some decidable first-order theories

Theorem (Presburger '29)

The elementary theory $\mathrm{Th}(\mathbb{N}, 0, 1, +)$ *is decidable.*

Theorem (Tarski '31)

The elementary theories $\mathrm{Th}(\mathbb{R}, 0, 1, +, \times)$ *and Euclidian plane are decidable.*

Here Euclidian plane $\mathbb{R}^2$ is in the Tarski's signature, i.e. with betweenness $B(x, y, z)$ and congruence relation $xy \equiv zw$.

Theory PrA^-

The language $\mathcal{L}_{\mathsf{PrA}}$ is the first order language with constants $0, 1$ and binary function $+$.

We use the following shorthands:

1. $x \leq y \overset{\text{def}}{\Longleftrightarrow} \exists z\; x + z = y$;
2. $\underline{0} \overset{\text{def}}{=} 0$, $\underline{n+1} \overset{\text{def}}{=} \underline{n} + 1$;
3. $x\underline{\times 0} \overset{\text{def}}{=} 0$, $x\underline{\times (n+1)} \overset{\text{def}}{=} x\underline{\times n} + x$;
4. $x \equiv_n y \overset{\text{def}}{\Longleftrightarrow} \exists z (z\underline{\times n} + x = y \vee z\underline{\times n} + y = z)$.

Theory PrA^-:

1. axioms of cancellative Abelian semigroup with neutral element 0 for $+$;
2. $x + 1 \neq 0$;
3. $x \neq 0 \to \exists y\; x = y + 1$;
4. $x \leq y \vee y \leq x$;

Two alternative axiomatizations of PrA^-

Let PrA be PrA^- plus the induction scheme:

$$\varphi(0) \land \forall x\, (\varphi(x) \to \varphi(x+1)) \to \forall x\, \varphi(x).$$

Let $\mathrm{PrA}_{\mathrm{alt}}$ be PrA^- plus the axioms:

$$x \equiv_n \underline{0} \lor \ldots \lor x \equiv_n \underline{n-1}, \text{ for } n \geq 1.$$

Since cut-elemination works even over $\mathrm{PrA}_{\mathrm{alt}}$, both $\mathrm{PrA}_{\mathrm{alt}}$ and PrA prove all true sentnences.

Theorem

There is $2^{2^{x^{\varepsilon}}}$ speeedup of PrA *over* $\mathrm{PrA}_{\mathrm{alt}}$*.*

Note that by formalization of Cooper's cut-elimination procedure for PrA there is $C > 0$ such that any true sentence $\varphi \in \mathcal{L}_{\mathrm{PrA}}$ has a proof in $\mathrm{PrA}_{\mathrm{alt}}$ of the length $\leq 2^{2^{2^{|\varphi|^{C}}}}$.

Idea of proof

It is possible to define formulas $\mathrm{Mul}_n(x, y, z)$ of polynomial in n sizes that express that $y < 2^{2^n}$ and $xy = z$.
Using $\mathrm{Mul}_n(x, y, z)$ we could formulate the formulas $\mathrm{Div}_n(x)$ that expresses that number x is divisible with remainder by all $y < 2^{2^n}$.

The formulas $\forall x\ \mathrm{Div}_n(x)$ have simple proofs by induction on x in PrA. The lengths of those proofs are polynomial in n.

However, for $n \geq 1$, it is possible to show that in order to prove $\forall x\ \mathrm{Div}_n(x)$ in $\mathrm{PrA}_{\mathrm{alt}}$ we need to use at least one instance of $x \equiv_k \underline{0} \lor \ldots \lor x \equiv_k \underline{k-1}$, for some $k \geq 2^{2^n-1}$.

This yields the $2^{2^{x^\varepsilon}}$ speedup of PrA over $\mathrm{PrA}_{\mathrm{alt}}$.

Proof systems for elementary geometry

Let TARSKI be Tarski's axiomatization of elementary geometry. Recall that it consists of finitely many axioms plus the scheme of continuity, i.e. "if a subsets (given by a formula) of a ray has an upper bound, it has the greatest upper bound".

RCF theory of real closed fields

1. axioms of fields;
2. axioms of linear order for $\leq$, where $x \leq y$ is a shorthand for $\exists z \; y = y + z^2$;
3. axioms that state that all polynomial of odd degree have roots, i.e. axioms O_n:

$$\forall a_0, \ldots, a_{n-1} \exists x \; x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0.$$

Note that elementary geometry is interpretable in the field of real numbers and vice versa. Due to this, both TARSKI and RCF could be considered as proof systems for both the theories of elementary geometry and the field of reals.

Speedup for elementary geometry

Theorem

There is $2^{2^{x^{\varepsilon}}}$ *speedup of* TARSKI *over* RCF*.*

Idea of proof:

We define formulas $\mathrm{Pow}_n(x, y, z)$ of the polynomial in n length that express that y is a natural number $< 2^{2^n}$ and $z = x^y$.

This allows us to formulate sentences R_n that express that for all natural $y < 2^{2^n}$ the equation $x^y = 2$ has a solution. By continuity axiom we have polynomial in n proofs of R_n in TARSKI.

However, R_n implies axioms O_k, for all odd $k < 2^{2^n}$. It is possible to show that for $n \geq 1$ any proof of R_n in RCF need to use some axiom O_k, for $k \geq 2^{2^n - 1}$.

Speedup for stronger theories

Theorem

Suppose $T \supseteq \mathsf{EA}$*,* $U \supseteq \mathsf{PrA}^-$ *are* $\mathtt{NP}$*-axiomatizable theories and* T *proves consistency of* U*. Then there is* 2^{x^ε} *speedup of* T *over* U *in* $\mathcal{L}_{\mathsf{PrA}}$*.*

Theorem

Suppose $T \supseteq \mathsf{EA}$*,* $U \supseteq \mathsf{RCF}$ *are* $\mathtt{NP}$*-axiomatizable theories,* ι *is an interpretation of* RCF *in* T*, and* T *proves consistency of* U*. Here* T *is regarded as a proof system for* $\mathcal{L}_{\mathsf{RCF}}$ *via interpretation* ι*. Then there is* 2^{x^ε} *speedup of* T *over* U *in* $\mathcal{L}_{\mathsf{RCF}}$*.*

Thank you!