Speedup for Presburger Arithmetic

Julien Daoud
Fedor Pakhomov

University of Gent

September 2025

Context

Examples of speedup:

- Let T be a recursively axiomatized theory containing Robinson Arithmetic Q. Then any proper extension of T has arbitrary recursive speed-up over T, corollary of Ehrenfeucht and Mycielski 1971
- There is a non elementary speedup of GB over ZFC, Pudlak 1986
- There is a non elementary speedup of $I\Sigma_1$ over Primitive Recursive Arithmetic, Ignjatovic 1990

Purpose

$2^{2^{x^\epsilon}}$ speedup between the two ***natural axiomatizations*** of Presburger arithmetic, and of real closed fields, using a sequence of sentences with some ***natural meaning***

The axiomatizations for Presburger arithmetic

Definition

Let $\mathcal{L}_{\mathsf{PrA}}$ be the language of Presburger arithmetic, i.e. the language of first order logic with equality, constants 0 *and* 1*, and the binary function symbol* $+$.

Definition

Let the theory PrA^- *be the theory with the following axioms.*

1. *Axioms of cancellative Abelian semigroup with neutral element* 0
2. $\forall x\ x+1 \neq 0$
3. $\forall x\ x \neq 0 \ \rightarrow \exists y\ x = y+1$
4. $\forall x, y\ x \leq y \vee y \leq x$,

where $x \leq y$ *is a shorthand for the formula* $\exists z\ x+z=y$

The axiomatizations for Presburger arithmetic

Definition

Let PrA *be the theory* PrA^- *with the scheme of induction.*
i.e. For all formulas $\phi(x)$ *with at least one free variable* x*, we have the axiom*

$$(\phi(0) \wedge \forall x(\phi(x) \to \phi(x+1))) \to \forall x \phi(x)$$

Definition

Let PrA_{alt} *be the theory* PrA^- *with the following axioms.*
For each prime p *we have the axiom*

$$\forall x \; x \equiv_p 0 \vee \ldots \vee x \equiv_p p-1,$$

where $x \equiv_n s$ *is a shorthand for the formula*

$$\exists z \; (\underbrace{z + \ldots + z}_{n\text{-times}} + s = x \vee \underbrace{z + \ldots + z}_{n\text{-times}} + x = s).$$

The sentences

- $Mul_0(x, y, z)$ defined as

$$(y = 0 \to z = 0) \wedge (y = 1 \to z = x) \wedge (y = 2 \to z = x + x)$$
$$\wedge \neg(y \neq 0 \wedge y \neq 1 \wedge y \neq 2)$$

- $Mul_n(x, y, z)$ defined as

$$\exists y_1, y_2, y_3, y_4, z_1, z_2, z_4 (y = y_3 + y_4 \wedge Mul_{n-1}(y_1, y_2, y_3)$$
$$\wedge Mul_{n-1}(x, y_1, z_1) \wedge Mul_{n-1}(z_1, y_2, z_2)$$
$$\wedge Mul_{n-1}(x, y_4, z_4) \wedge z = z_2 + z_4)$$

- It does have the intended meaning (by induction on n).
- Mul_n accepts y up to $\sim 2^{2^n}$ since $2^{2^{n-1}}.2^{2^{n-1}} = 2^{2^n}$.

The sentences

Theorem (Rackoff, Solovay75)

Let $\mathcal{L}$ *be a first-order language, where* $\neg$ *and at least one of the three logical connectives* $\rightarrow$, $\vee$, $\wedge$ *are present. Furthermore* $\mathcal{L}$ *should contain the equality symbol and constants* $0, 1$. *Let* $\phi_0(\vec{a}, \vec{b})$ *and* $\Phi(R, \vec{a}, \vec{b})$ *be given, with* $\vec{a}$ *being free variables,* $\vec{b}$ *being parameters (defined in* $\mathcal{L}$*), and* $R(\vec{a})$ *being a relation symbol outside of* $\mathcal{L}$.
Then it is possible to construct a sequence of formulas $\phi_1(\vec{a}, \vec{b})$, $\phi_2(\vec{a}, \vec{b})$, … *such that the formulas*

$$\phi_{n+1}(\vec{a}, \vec{b}) \leftrightarrow \Phi(\phi_n, \vec{a}, \vec{b})$$

have polynomial (in n*) proofs in* QPC *from the axiom* $0 \neq 1$.

The sentences

- We then take the Mul_n to be of polynomial size in n by Solovay's theorem.
- $\forall x Div_n(x)$ defined as

$$\forall x \forall y (Hyp_n(x, y) \rightarrow$$
$$(y = 0) \vee \exists a_1, b_1, b_2(Mul_n(a_1, y, b_1) \wedge x = b_1 + b_2 \wedge b_2 < y))$$

  Where $Hyp_n(x, y)$ are some hypotheses on the size of y and on the behaviour of the Mul_n predicate.
- This sentence states that, given any x, it is dividable (with remainder) by all y up to 2^{2^n}.
- Div_n is hence of polynomial size in n since Mul_n is.

Theorem

Theorem

There is a $2^{2^{x^{\epsilon}}}$ *speedup of* PrA *over* PrA_{alt}.

- Short proofs in PrA using the induction
- Long proofs in PrA_{alt} because of the size of the axioms necessary
- We show this last fact by constructing some appropriate model, and then invoking Gödel's completeness theorem

The model

The model M_p whose elements are the naturals $\mathbb{N}$ *and* all polynomials of the following form:

$$a_q.X^q + a_{q-1}.X^{q-1} + ... + a_0$$

where $q > 0$,
a_0 is an integer (in $\mathbb{Z}$),
and for $i \neq 0$, the a_i are of the form

$$\frac{z}{p_0^{x_0}.p_1^{x_1}. \dots p_t^{x_t}}$$

with z an integer, the x_i's natural numbers and $p_0, ..., p_t$ the primes strictly smaller than p.

Extra sweet sweetie

The key idea for the Rackoff-Solovay's theorems:

$$\mathcal{R}(\overline{x}_1) \wedge \ldots \wedge \mathcal{R}(\overline{x}_t)$$

is equivalent to

$$\forall \overline{z}(\ (\overline{x}_1 = \overline{z} \vee \ldots \vee \overline{x}_t = \overline{z}) \rightarrow \mathcal{R}(\overline{z})\ )$$