Another quantifier-elimination result in arithmetic under negated induction

Tin Lok Wong

Ongoing joint work with
David Belanger, C.T. Chong, Wei Li, Yue Yang

National University of Singapore

31 May, 2022

> Most of the interesting theories which arise in mathematics are undecidable (e.g., number theory, set theory, groups, fields, partial order), and the method of elimination of quantifiers does not work for these theories.
>
> Chang–Keisler (1973)

This talk

a quantifier-elimination result in first-order arithmetic that is both non-trivial and useful

- How can it look like?
- How can one use it?

Plan

1. introduction
2. quantifier elimination
3. consequences
4. discussion

> Most of the interesting theories which arise in mathematics are undecidable (e.g., number theory, set theory, groups, fields, partial order), and the method of elimination of quantifiers does not work for these theories.
>
> Chang–Keisler (1973)

First-order arithmetic

$n \in \mathbb{N}$

- $\mathcal{L}_1 = \{0, 1, +, \times, <, =\}$.
- A quantifier is *bounded* if it is of the form $\forall v < t$ or $\exists v < t$.
- An $\mathcal{L}_1$ formula is Δ_0 if all its quantifiers are bounded.
- $\Sigma_n = \{\exists \bar{v}_1\ \forall \bar{v}_2\ \cdots\ \mathrm{Q}\bar{v}_n\ \theta : \theta \in \Delta_0\}$ and $\Pi_n = \{\forall \bar{v}_1\ \exists \bar{v}_2\ \cdots\ \mathrm{Q}'\bar{v}_n\ \theta : \theta \in \Delta_0\}$.
- $\mathrm{I}\Sigma_n$ consists of the axioms of PA^- and for every $\theta \in \Sigma_n$,
$$\theta(0) \wedge \forall x\ \big(\theta(x) \to \theta(x+1)\big) \to \forall x\ \theta(x).$$
- $\mathrm{PA} = \bigcup_{m \in \mathbb{N}} \mathrm{I}\Sigma_m$.
- exp asserts the totality of $x \mapsto 2^x$ over $\mathrm{I}\Sigma_0$.
- $\mathrm{B}\Sigma_n$ consists of the axioms of $\mathrm{I}\Sigma_0$ and for every $\theta \in \Sigma_n$,
$$\forall a\ \big(\forall x < a\ \exists y\ \theta(x, y) \to \exists b\ \forall x < a\ \exists y < b\ \theta(x, y)\big).$$
- Σ_{n+1} and Π_{n+1} are both closed under bounded quantification over $\mathrm{B}\Sigma_{n+1}$.

Theorem (Paris–Kirby 1978)

$\mathrm{I}\Sigma_0 + \mathrm{exp} \dashv \mathrm{B}\Sigma_1 + \mathrm{exp} \dashv \mathrm{I}\Sigma_1 \dashv \mathrm{B}\Sigma_2 \dashv \mathrm{I}\Sigma_2 \dashv \mathrm{B}\Sigma_3 \dashv \mathrm{I}\Sigma_3 \dashv \mathrm{B}\Sigma_4 \dashv \mathrm{I}\Sigma_4 \dashv \cdots$ and none of the converses holds.

Global properties of local theories

$n \in \mathbb{N}$

Theorem (Kaye 1997)

$\mathrm{B}\Sigma_{n+1} + \exp + \neg\mathrm{I}\Sigma_{n+1}$ proves that there is no *definable* injection from the universe to a bounded set.

- Kaye's proof used κ-like models, where κ is a singular cardinal, i.e., models of cardinality κ all of whose proper initial segments are of strictly smaller cardinality.
- Kołodziejczyk–Kowalik–Yokoyama (2021+) gave an alternative proof using the automorphisms from Kossak (1990).
- By the Completeness Theorem, there *must be* a syntactic proof.
- *Quantifier elimination* is the obvious approach for a syntactic proof.

Plan

Extract a quantifier-elimination result from Kossak's back-and-forth system for his automorphisms.

Theorem (Paris–Kirby 1978)

$\mathrm{I}\Sigma_0 + \exp \dashv \mathrm{B}\Sigma_1 + \exp \dashv \mathrm{I}\Sigma_1 \dashv \mathrm{B}\Sigma_2 \dashv \mathrm{I}\Sigma_2 \dashv \mathrm{B}\Sigma_3 \dashv \mathrm{I}\Sigma_3 \dashv \mathrm{B}\Sigma_4 \dashv \mathrm{I}\Sigma_4 \dashv \cdots$ and none of the converses holds.

Shrinking the domains of quantification to a cut

nonempty initial segment with no maximum

$n \in \mathbb{N}$

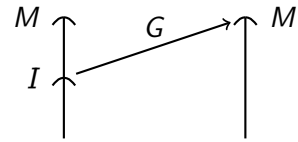
Let $M \models \mathrm{B}\Sigma_{n+1} + \exp + \neg\mathrm{I}\Sigma_{n+1}$.

(1) Use $\neg\mathrm{I}\Sigma_{n+1}$ to obtain a Σ_{n+1}-definable proper cut I of M.

(2) Say $I = \{i \in M : M \models \exists x\ \theta(i,x)\}$, where $\theta \in \Pi_n$. Define

$$G(i) = \min\{x \in M : M \models \theta(i,x)\} \quad \text{for each } i \in I,$$

so that the range of G is cofinal in M.



(3) Then $M \models \exists \bar{v}\ \theta(\bar{v}) \leftrightarrow \exists i \in I\ \exists \bar{v} < G(i)\ \ \theta(\bar{v})$ for any $\mathcal{L}_1$ formula θ.

(4) Let $\alpha(\bar{i}, \bar{u}, \bar{z})$ *is a* Δ_{n+1} *formula for* $\bar{i} \in I$ *in* M, i.e., $\alpha \in \Sigma_{n+1}$ and for some $\alpha'(\bar{i}, \bar{u}, \bar{z}) \in \Pi_{n+1}$,

$$M \models \forall \bar{i} \in I\ \ \forall \bar{u}, \bar{z}\ \big(\alpha(\bar{i}, \bar{u}, \bar{z}) \leftrightarrow \alpha'(\bar{i}, \bar{u}, \bar{z})\big).$$

Then $M \models \forall a, \bar{z}\ \big(\forall \bar{u} < a\ \ \exists \bar{i} \in I\ \ \alpha(\bar{i}, \bar{u}, \bar{z}) \leftrightarrow \exists j \in I\ \ \forall \bar{u} < a\ \ \exists \bar{i} < j\ \ \alpha(\bar{i}, \bar{u}, \bar{z})\big)$.

	$\ldots$		$\exists v_2$		$\forall u_1$		$\exists v_1$	$\alpha_0(\bar{u}, \bar{v}, \bar{z})$	
$\Leftrightarrow$	$\ldots$	$\exists j_2 \in I$	$\exists v_2 < G(j_2)$	$\forall i_1 \in I$	$\forall u_1 < G(i_1)$	$\exists j_1 \in I$	$\exists v_1 < G(j_1)$	$\alpha_0(\bar{u}, \bar{v}, \bar{z})$	by (3);
$\Leftrightarrow$	$\ldots$	$\exists j_2 \in I$		$\forall i_1 \in I$		$\exists j_1 \in I$		$\alpha_1(\bar{i}, \bar{j}, \bar{z})$	by (4).

Skolemization

$n \in \mathbb{N}$

Let $M \models \mathrm{B}\Sigma_{n+1} + \exp + \neg\mathrm{I}\Sigma_{n+1}$ and I be a Σ_{n+1}-definable proper cut of M.

Theorem (Chong–Mourad 1990). If $\alpha(\bar{i}, \bar{z})$ is a Δ_{n+1} formula for $\bar{i} \in I$ in M, then

$$M \models \forall b\ \exists c\ \forall \bar{i} \in I\ \ \forall \bar{z} < b\ \ \big((\bar{i}, \bar{z}) \in \mathrm{Set}(c) \leftrightarrow \alpha(\bar{i}, \bar{z})\big),$$

where $\mathrm{Set}(c)$ denotes the set coded by c, say, via its binary representation.

From the previous slide, every $\mathcal{L}_1$ formula is equivalent in M to one of the form

$$\begin{aligned}
&\dots\ \forall i_2 \in I\ \ \exists j_2 \in I\ \ \forall i_1 \in I\ \ \exists j_1 \in I\ \ \alpha_1(i_1, j_1, i_2, j_2, \dots) \\
\Leftrightarrow\ &\dots\ \forall i_2 \in I\ \ \exists j_2 \in I\ \ \exists s_1 \colon I \to I\ \forall i_1 \in I\ \ \alpha_1(i_1, s_1(i_1), i_2, j_2, \dots) \\
\Leftrightarrow\ &\dots\ \forall i_2 \in I\ \ \forall s_2 \colon (I \to I) \to (I \to I)\ \exists j_2 \in I\ \ \exists s_1 \colon I \to I\ \alpha_1(s_2(s_1, j_2), s_1(s_2(s_1, j_2)), i_2, j_2, \dots \\
\Leftrightarrow\ &\dots\ \forall i_2 \in I\ \ \forall s_2 \colon \underbrace{(I \to I) \to (I \to I)}_{I \underset{2}{\to} I}\ \exists k_2 \in I\ \ \alpha_2(s_2, i_2, k_2, \dots) \\
\Leftrightarrow\ &\dots\ \exists s_3 \colon (I \underset{2}{\to} I) \to (I \to I)\ \forall i_2 \in I\ \ \forall s_2 \colon I \underset{2}{\to} I\ \alpha_2(s_2, i_2, s_3(s_2, i_2), \dots) \quad \Leftrightarrow\ \dots
\end{aligned}$$

where $\alpha_1, \alpha_2, \dots$ are Δ_{n+1} for $\bar{i}, \bar{j} \in I$ in M, and $s_1, s_2, \dots$ are *coded* in M.

Quantifier elimination

$n \in \mathbb{N}$

Let $M \models \mathrm{B}\Sigma_{n+1} + \exp + \neg\mathrm{I}\Sigma_{n+1}$ and I be a Σ_{n+1}-definable proper cut of M.

Theorem (Chong–Mourad 1990). If $\alpha(\bar{i}, \bar{z})$ is a Δ_{n+1} formula for $\bar{i} \in I$ in M, then

$$M \models \forall b\ \exists c\ \forall \bar{i} \in I\ \ \forall \bar{z} < b\ \ \big((\bar{i}, \bar{z}) \in \mathrm{Set}(c) \leftrightarrow \alpha(\bar{i}, \bar{z})\big),$$

where $\mathrm{Set}(c)$ denotes the set coded by c, say, via its binary representation.

Theorem

Let $m \in \mathbb{N}$. Every Σ_{m+n+3} formula is equivalent in M to one of the form

$$\exists i \in I\ \ \exists \text{coded } s\colon I \xrightarrow[m+1]{} I\ \forall k \in I\ \ \alpha(s, i, k, \bar{z}), \qquad (*)$$

where $\alpha(s, i, k, \bar{z})$ is a Δ_{n+1} formula for $i, k \in I$ in M.

$$I \xrightarrow[m+1]{} I = (I \xrightarrow[m]{} I) \to (I \to I)$$

Note

For every $b \in M$, there is an M-coded set A such that, for all $\bar{z} < b$, the formula $(*)$ above is equivalent in M to

$$\exists i \in I\ \ \exists \text{coded } s\colon I \xrightarrow[m+1]{} I\ \exists k > I\ \ (s, i, k, \bar{z}) \in A.$$

Pigeonhole principles — provability

$m, n \in \mathbb{N}$

Let $M \models \mathrm{B}\Sigma_{n+1} + \exp + \neg\mathrm{I}\Sigma_{n+1}$ and I be a Σ_{n+1}-definable proper cut of M.

Corollary

$\{0, 1, \ldots, a-1\}$

Let $a, e \in M$ with $e > I$. There is no Σ_{m+n+3}-definable injection $2^e_{m+1}e^2a \to a$ in M.

Proof

$2^{2^{\cdot^{\cdot^{\cdot^{2^e}}}}}$ $\}$ $(m+1)$-many 2's

- Let F be a Σ_{m+n+3}-definable injection $b \to a$.
- Use the quantifier-elimination result to find an M-coded set A such that
$$M \models \forall x, y\ \big(F(x) = y \leftrightarrow \exists i \in I\ \exists\text{coded } s\colon I \xrightarrow[m+1]{} I\ \exists k > I\ (s, i, k, x, y) \in A\big).$$
- Then $\mathrm{graph}(F) = \bigcup_{i,s,k} F_{i,s,k}$, where $F_{i,s,k} := \{(x, y) \in M^2 : (s, i, k, x, y) \in A\}$, and $i \in I$ and $s\colon I \xrightarrow[m+1]{} I$ and $k > I$.
- There are at most $e \times 2^e_{m+1} \times e$ such triples (i, s, k).
- Each $F_{i,s,k} \subseteq \mathrm{graph}(F)$. So $F_{i,s,k}$ is the graph of an injection with codomain a. It must have M-cardinality at most a by the pigeonhole principle for coded injections.
- So $b = \mathrm{card}^M \mathrm{graph}(F) \leqslant 2^e_{m+1}e^2a$. □

Pigeonhole principles — unprovability

$m, n \in \mathbb{N}$

Let $M \models \mathrm{B}\Sigma_{n+1} + \exp + \neg\mathrm{I}\Sigma_{n+1}$ and I be a Σ_{n+1}-definable proper cut of M.

Corollary

$\{0, 1, \ldots, a-1\}$

Let $a, e \in M$ with $e > I$. There is no Σ_{m+n+3}-definable injection $2^{e}_{m+1}e^2a \to a$ in M.

$2^{2^{\cdot^{\cdot^{\cdot^{2^e}}}}}$ } $(m+1)$-many 2's

Theorem (Groszek–Slaman 1994). There is $K \models \mathrm{I}\Sigma_n + \exp + \neg\mathrm{B}\Sigma_{n+1}$ with a Σ_{n+1}-definable bijection $K \to \mathbb{N}$.

Corollary

One cannot prove $\mathrm{I}\Sigma_{n+1}$ from $\mathrm{B}\Sigma_{n+1} + \exp$ plus

for no $a \geqslant 2$ is there a definable injection $a^2 \to a$.

Proof

Apply the previous corollary to a model M in which $\mathbb{N}$ is Σ_{n+1}-definable. □

Second-order arithmetic

$n \in \mathbb{N}$

- $\mathcal{L}_2 := \mathcal{L}_1 \cup \{\in\}$ has a number sort and a set sort.
- We use lowercase letters $a, b, c, \ldots, x, y, z$ for objects of the number sort, and uppercase letters $A, B, C, \ldots, X, Y, Z$ for objects of the set sort.
- We write an $\mathcal{L}_2$ structure as $(M, \mathscr{X})$, where $M, \mathscr{X}$ are universes for the number and set sorts respectively.
- A quantifier is *bounded* if it is of the form $\forall v < t$ or $\exists v < t$.
- An $\mathcal{L}_2$ formula is Δ^0_0 if all its quantifiers are bounded.
- $\Sigma^0_n = \{\exists \bar{v}_1\ \forall \bar{v}_2\ \cdots\ \mathrm{Q}\bar{v}_n\ \theta : \theta \in \Delta^0_0\}$.
- $\mathrm{I}\Sigma^0_n$ and $\mathrm{B}\Sigma^0_n$ are similar to $\mathrm{I}\Sigma_n$ and $\mathrm{B}\Sigma_n$, except that there may be set variables.

Theorem (Paris–Kirby 1978)

$\mathrm{I}\Sigma^0_0 + \exp \dashv \mathrm{B}\Sigma^0_1 + \exp \dashv \mathrm{I}\Sigma^0_1 \dashv \mathrm{B}\Sigma^0_2 \dashv \mathrm{I}\Sigma^0_2 \dashv \mathrm{B}\Sigma^0_3 \dashv \mathrm{I}\Sigma^0_3 \dashv \mathrm{B}\Sigma^0_4 \dashv \mathrm{I}\Sigma^0_4 \dashv \cdots$ and none of the converses holds.

Expansions

$m, n \in \mathbb{N}$

Let $M \models \mathrm{B}\Sigma_{n+1} + \exp + \neg\mathrm{I}\Sigma_{n+1}$ and I be a Σ_{n+1}-definable proper cut of M.

Corollary. For every Σ^0_{m+n+3} formula $\theta(\bar{z})$ and every $b \in M$, there is an M-coded set A such that, for all $\bar{z} < b$, the formula $\theta(\bar{z})$ is equivalent in $(M, \mathscr{X})$ to

$$\exists i \in I \ \exists \text{coded } s\colon I \xrightarrow[m+1]{} I \ \exists k > I \ (s, i, k, \bar{z}) \in A.$$

Corollary

For any $(M, \mathscr{X}) \models \mathrm{B}\Sigma^0_{n+1}$ and any bounded $S \subseteq M$,

$$S \in \Sigma^0_m\text{-Def}(M, \mathscr{X}) \quad \Rightarrow \quad S \in \Sigma_m\text{-Def}(M).$$

Proof when $m \geqslant n + 3$

The corollary at the top works also in $(M, \mathscr{X})$, but the equivalent formula does not involve $\mathscr{X}$. (The set A is coded by an element of M.) □

Theorem (Towsner 2015 for $n \geqslant 1$). Given any countable $K \models \mathrm{I}\Sigma_n + \exp + \neg\mathrm{B}\Sigma_{n+1}$ and any $S \subseteq K$, one can construct $(K, \mathscr{X}) \models \mathrm{I}\Sigma^0_n$ in which S is Σ^0_{n+1}-definable.

Concluding discussion

$m, n \in \mathbb{N}$

Let $M \models \mathrm{B}\Sigma_{n+1} + \exp + \neg\mathrm{I}\Sigma_{n+1}$ and I be a Σ_{n+1}-definable proper cut of M.

Corollary. For every Σ_{m+n+3} formula $\theta(\bar{z})$ and every $b \in M$, there is an M-coded set A such that, for all $\bar{z} < b$, the formula $\theta(\bar{z})$ is equivalent in M to

$$\exists i \in I \ \exists \text{coded } s\colon I \xrightarrow[m+1]{} I \ \exists k > I \ (s, i, k, \bar{z}) \in A.$$

- Proof: (1) Shrink the domains of quantification to a cut. (2) Skolemize.
- Via an argument from Kossak (1989), our quantifier-elimination result applies to any proper cut of a countable recursively saturated model of PA.
- This (partially) answers Kaye's question from the Kotlarski–Ratajczyk conference in 2012 about the existence of quantifier-eliminable cuts in models of PA.
- Models of arithmetic that expand to a model of $\mathrm{B}\Sigma^0_{n+1} + \exp + \neg\mathrm{I}\Sigma^0_{n+1}$ are nicer; cf. Kossak's notions of ω-property and not-always-semiregular models.
- (Kaye, around 1991) The model-theoretic properties of a model of arithmetic do not only depend on the induction axioms it satisfies, but also on the induction axioms it does *not* satisfy.