

Linear fragments of Peano arithmetic

Petr Glivický

petrglivicky@gmail.com

University of Economics, Prague

BPGMTC 2017, Leeds
January 26, 2017

Content

- 1 Linear arithmetics
- 2 Context
 - Primitive positive elimination for ordered modules over rings R_τ
 - A more detailed analysis
- 3 Properties of LA
- 4 Properties of LA_2 and above

Section 1

Linear arithmetics

Linear arithmetic

Recall that:

Presburger arithmetic is the full-induction arithmetic for the language $\langle 0, 1, -, +, \leq \rangle$.

Peano arithmetic is the full-induction arithmetic for the language $\langle 0, 1, -, +, \cdot, \leq \rangle$.

We introduce:

Linear arithmetic (LA) is the full-induction arithmetic for the language $\langle 0, 1, -, +, a \cdot, \leq \rangle$, where $a \cdot$ is a unary function of multiplication by a positive non-standard element.

Higher order linear arithmetics

Similarly, for any cardinal κ , we introduce:

κ -linear arithmetic (LA_κ) is the full-induction arithmetic for the language $\langle 0, 1, -, +, a_\alpha \cdot, \leq \rangle_{\alpha \in \kappa}$, where all “scalars” a_α are non-standard.

Then:

- $Pr = LA_0$,
- $LA = LA_1$.

Models of linear arithmetics can be understood as certain **ordered modules**:

Let $\mathcal{M} = \langle M, 0, 1, -, +, a \cdot, \leq \rangle \models LA$.

Then \mathcal{M} can be equipped with a structure of a (discretely ordered) module over the ring $R_a = \mathbb{Q}[a] \cap M$.

More generally, any $\mathcal{M} = \langle M, 0, 1, -, +, a_\alpha \cdot, \leq \rangle_{\alpha \in \kappa} \models LA_\kappa$ can be understood as a discretely ordered module over the ring $\mathbb{Q}[a_\alpha]_{\alpha \in \kappa} \cap M$.

Section 2

Context

We want to understand definable sets in models of linear arithmetics (certain discretely ordered modules).

There are two closely related, but simpler situations:

$\langle M, 0, -, +, r \rangle_{r \in R}$ and $\langle M, 0, 1, -, +, \leq \rangle = \langle M, 0, 1, -, +, \leq, z \rangle_{z \in \mathbb{Z}}$
(unordered) modules models of Presburger arithmetics =
 = discretely ordered inductive \mathbb{Z} -modules
(forget the ordering) (forget the scalars)

Unordered modules

The following is a classical result in the theory of modules:

Theorem (Baur-Monk)

Let $\mathcal{M} = \langle M, 0, -, +, r \rangle_{r \in R}$ be a (left) module over a ring (associative, with 1) R .

Every formula is in \mathcal{M} equivalent to a boolean combination of primitive positive formulas, i.e. to a boolean combination of formulas of the form $(\exists \bar{z})\psi_i$, where each ψ_i is a system of linear equations.

Remark: A formula in a language L is called **primitive positive**, or **pp-formula**, if it is of the form $(\exists \bar{z}) \bigwedge_{i < n} \chi_i$, where χ_i are atomic formulas.

Models of Pr

For models of Presburger arithmetic, we have:

Theorem (Presburger)

Every formula is in Pr equivalent to a disjunction of primitive positive formulas, i.e. to a formula of the form $\bigvee_{i < n} (\exists \bar{z}) \psi_i$, where each ψ_i is a system of linear inequalities.

Question: Do the pp-elimination results of Baur-Monk and Presburger generalize to arithmetics LA_κ with $\kappa > 0$?

We “show” that the answer is “Yes” if and only if $\kappa = 1$.

Recall that $\mathcal{M} \models LA$ can be understood as a discretely ordered module over the ring $R_a = \mathbb{Q}[a] \cap M$.

We have $\mathbb{Z}[x] \subseteq R_a \subseteq \mathbb{Q}[x]$ and each R_a is (up to isomorphism) uniquely determined by the class τ of remainders of $a \bmod 0 < n \in \mathbb{N}$. R_τ denotes some R_a with a having the remainders τ .

Then, clearly, \mathcal{M} is “integrally-divisible” over R_a , i.e.

$(\exists x, z \in M)(m = rx + z \ \& \ 0 \leq z < r \cdot 1)$ for all $m \in M$, $r \in R_a$.

Let further on $D = R_\tau$ be fixed and $\mathcal{M} = \langle M, 0, 1, -, +, \leq, r \rangle_{r \in D}$ be a fixed discretely ordered (with 1 being the least positive element), integrally-divisible D -module.

In particular, any $\mathcal{M} \models LA$ with $D = R_a$ satisfy these assumptions.

\mathcal{M}' is the expansion of \mathcal{M} by definitions of functions r^{-1} providing integral division by all scalars $0 < r \in D$.

Theorem

For any formula $\varphi(x, \bar{y})$ of \mathcal{M}' there are finitely many terms (of \mathcal{M}') $t_i(\bar{y})$, for $i < n$, with $n \in \mathbb{N}$, such that

$$\mathcal{M}' \models (\exists x)\varphi(x, \bar{y}) \leftrightarrow \bigvee_{i < n} \varphi(t_i(\bar{y}), \bar{y}).$$

Corollary

- 1 \mathcal{M}' has quantifier elimination.
- 2 In \mathcal{M} , every formula is equivalent to a disjunction of primitive positive formulas, i.e. to a formula of the form $\bigvee_{i < n} (\exists \bar{z}) \psi_i$, where each ψ_i is a system of linear inequalities.

A more detailed analysis

Further on, by a term or formula, we mean always an \mathcal{M}' -term or an \mathcal{M}' -formula. We will denote by \mathbf{C} the set of all constant terms in \mathcal{M}' .

A term $t(\bar{x})$ is **harmonic** if

$$t(\bar{x}) = \sum_{i=0}^{N-1} q_i r_i^{-1}(x_{f(i)}) + c,$$

for some $q_i, r_i \in D$, $c \in \mathbf{C}$ and $f : N \rightarrow I(\bar{x})$.

A formula or a “piecewise-term” are harmonic if all its maximal subterms are.

A “piecewise-term” τ is called an **almost-term** if it is of the form

$$\tau(\bar{x}) = \begin{cases} s(\bar{x}) + c_i & \text{if } \psi_i(\bar{x}), i < n, \end{cases}$$

where $s(\bar{x})$ is a term, and $c_i \in \mathbf{C}$, for $i < n$.

Harmonic form theorem

Theorem (Harmonic form theorem)

- 1) For every term $t(\bar{x})$, there is an open harmonic almost-term $\tau(\bar{x})$ such that $\mathcal{M}' \models t(\bar{x}) = \tau(\bar{x})$.
- 2) For every formula $\varphi(\bar{x})$, there is an open harmonic formula $\psi(\bar{x})$ such that $\mathcal{M}' \models \varphi(\bar{x}) \leftrightarrow \psi(\bar{x})$.

Representation of definable sets

For $\bar{a} \in M$ we denote by $K(\bar{a})$ the l -dimensional box with orthogonal edges of lengths $a_i + 1$, $i < l$, i.e. $K(\bar{a}) = \prod_{i < l} [0, a_i]$.

Theorem

Every set $A \subseteq M^n$ X -definable in \mathcal{M}' (for $X \subseteq M$) can be written as

$$A = \bigcup_{i < k} g[P_i],$$

where $g : (K(\bar{a}) \times M)^n \rightarrow M^n$ is a “linear coordination” of M^n , $\bar{a} = (a_0, \dots, a_l) \in M^l$, $l \in \mathbb{N}$, and P_i , for $i < k$, are finitely many polyhedra in $(K(\bar{a}) \times M)^n$ over parameters from X .

“Every definable set is a finite union of linear images of polyhedra.”

Section 3

Properties of LA

Theorem (Properties of LA)

1) LA is model-complete.

Moreover: Every formula is in LA equivalent to a disjunction of primitive positive formulas, i.e. to a formula of the form $\bigvee_{i < n} (\exists \bar{z}) \psi_i$, where each ψ_i is a system of linear inequalities.

2) For $\mathcal{A}, \mathcal{B} \models LA$, it is $\mathcal{A} \equiv \mathcal{B} \Leftrightarrow a^{\mathcal{A}} \equiv a^{\mathcal{B}} \pmod{n}$, for all $0 < n \in \mathbb{N}$.

$LA_\tau = LA + \{a \equiv \tau(p, k) \pmod{p^k}; p \in \mathbb{N} \text{ prime}, k \in \mathbb{N}\}$, for $\tau \in \prod_{p \in \mathbb{P}} \mathbb{J}_p$, are all simple complete extensions of LA.

3) $R_\tau = \{r(a)/n; 0 \leq r(a) \in \mathbb{Z}[a], 0 \neq n \in \mathbb{N}, p^k | r(\tau(p, k)) \forall p^k | n\}$ is the unique prime model of LA_τ , for $\tau \in \prod_{p \in \mathbb{P}} \mathbb{J}_p$.

4) LA is decidable.

LA_τ is decidable if and only if τ is recursive.

5) The induction scheme in LA may be equivalently replaced by the scheme of integral divisibility

$(\exists y, z)(x = qy + z \ \& \ z < q)$, for all $0 < q \in \mathbb{Z}[a]$.

Corollary

Up to elementary equivalence, models of LA are exactly all ultraproducts

$$\mathcal{Z}_{\mathcal{U}} = \left(\prod_{n \in \mathbb{N}} \langle \mathbb{Z}, 0, 1, +, -, \underline{n}, \leq \rangle \right) / \mathcal{U},$$

where \mathcal{U} is a non-principal ultrafilter on \mathbb{N} , i.e. $\mathcal{U} \in \beta\mathbb{N} - \mathbb{N}$.

Note: Properties of LA and Pr are similar, but the proof for LA is incomparably harder (due to [in]decomposability of sets $\{qx + ry; 0 \leq x, y \in A\}$ in $\mathcal{A} \models \text{Pr}[LA]$).

The following corollary is on the structure of models of Peano arithmetic:

Corollary

Let $\mathcal{M} = \langle M, 0, 1, -, +, \cdot, \leq \rangle$ be a saturated model of Peano arithmetic, $0 \leq a \in M - \mathbb{N}$, $c, d \in M$. Then the following are equivalent:

- 1) For every “Peano multiplication” \circ on \mathcal{M} with $a \cdot x = a \circ x$ for all x , it is $c \cdot d = c \circ d$.
- 2) $c \in \mathbb{Q}[a]$ or $d \in \mathbb{Q}[a]$.

Recall that Presburger arithmetic is dp-minimal and thus also NIP. For LA , this is different:

Theorem

LA is NIP but not dp-minimal.

Proof sketch: For the NIP property use the description of definable sets (in all dimensions) as linear images of finite unions of polyhedra, i.e. solutions of systems of linear inequalities. But linear inequalities have VC-dimension 1 hence are NIP.

But LA cannot be dp-minimal because $x \mapsto (x \operatorname{div} a, x \operatorname{mod} a)$ is a definable function which is a bijection between infinite sets $[0, a^2)$ and $[0, a)^2$.

Section 4

Properties of LA_2 and above

Wild models of LA_2

The pp-elimination, though true for $\text{Pr} = LA_0$ and $LA = LA_1$, does not hold for LA_κ with $\kappa \geq 2$.

This is an easy consequence of the following:

Proposition (with P. Pudlák)

There is a model $\mathcal{M} = \langle M, 0, 1, -, +, a \cdot, b \cdot, \leq \rangle \models LA_2$ and a non-standard $l \in M$ such that $\cdot \upharpoonright [0, l]^2$ is definable in \mathcal{M} for some Peano multiplication \cdot on \mathcal{M} (i.e. such that $\langle M, 0, 1, +, \cdot, \leq \rangle \models PA$).

Note that no such model can exist for LA_1 (easy consequence of model-completeness).

Corollary

For $\kappa \geq 2$, the theory LA_κ does not have pp-elimination. It is not even model complete (i.e. does not have elimination to \exists -formulas).

Proof idea:

In a saturated model of Peano arithmetic, for any $\mathbb{N} < I \in M$, we find elements a, b such that the sequence $(1, 1^2, 2, 2^2, \dots, 2I, (2I)^2)$ is encoded by the set of all numerators of convergents of the continued fraction of a/b . The crucial observation is that this set is definable in the language of LA_2 with a, b as the two scalars.

(Note that for LA_1 every continued fraction of scalars is finite, thus the construction above does not allow to define an infinite part of a Peano multiplication.)

The following is well known:

Proposition

*(Unordered) modules are stable and thus NIP.
Presburger arithmetic (although unstable) is NIP.*

Question (Chernikov and Hils): Is every ordered module NIP?

Corollary (with P. Pudlák)

The model \mathcal{M} from the previous proposition, considered as an ordered module over $\mathbb{Z}[a, b] / =_{\mathcal{M}}$, is not NIP.

Despite not having the pp-elimination, the hierarchy for higher order linear arithmetics still collapses. This is a consequence of the following more general result:

Let $\mathcal{M} = \langle M, 0, 1, +, -, \leq, r \rangle_{r \in R}$ be an ordered R -module with a unit $1 > 0$. We say that \mathcal{M} is **i-divisible** if for every $0 < r \in R$ it is $\mathcal{M} \models (\forall x)(\exists y, z)(x = ry + z \ \& \ 0 \leq z < r1)$.

Theorem

Let \mathcal{M} be an i-divisible ordered module. Then every formula is in \mathcal{M} equivalent to a bounded formula.

Corollary

For any κ , every $\mathcal{M} \models LA_\kappa$ has bounded quantifier elimination. Hence, in no model of LA_κ a Peano multiplication is definable on the whole universe.

Proof idea:

The crucial part is to prove that in \mathcal{M} , every formula $\psi(\bar{x})$ is **protoproperiodic**, i.e. there exists a disjunct covering \mathcal{A} of $M^{l(\bar{x})}$ by finitely many convex polyhedra, such that for any $A \in \mathcal{A}$ and a direction $s = \bar{\alpha} \in R^{l(\bar{x})}$ either A is bounded in the direction s ($\exists 0 \leq m \in M$ s.t. $A + sm \not\subseteq A$) or there is a period $0 < P \in R$ for ψ on A in the direction s (i.e. $(\forall \bar{u}, \bar{v} \in A)((\exists m \in M)\bar{u} = Psm + \bar{v} \rightarrow (\psi(\bar{u}) \leftrightarrow \psi(\bar{v})))$).

This is done by induction on complexity of ψ .

Tame and wild linear fragments of PA

Let $\mathcal{M} \models PA$ and let R be a subring of $\mathcal{M} \cup -\mathcal{M}$. Denote M_R the R -(semi)module fragment of \mathcal{M} . We know the following:

Proposition

If R is some R_τ then M_R has pp-elimination (hence is model complete).

But we can also prove the following:

Proposition

If R contains elements a, b such that a/b has an infinite continued fraction (in \mathcal{M}) then M_R is not model complete (hence does not have pp-elimination).

Proof sketch: The set C of all pairs (u, v) such that u/v is a convergent of a/b (in the lowest terms) is infinite and definable in M_R . It is easy to show that C is a (graph of a) concave sequence. But then it cannot be defined by an \exists -formula, as each infinite \exists -definable set in M_R contains three points lying on a line.

Open questions and Thank you

Open questions:

Is it possible to decide pp-elimination/model completeness of M_R also in the remaining cases (when R is not R_τ but does not contain a, b with an infinite continued fraction)? Do such cases exist at all?

Is there a model M_R which is not model complete but is still NIP?

What about full-induction modules which are not fragments of models of PA?

In particular, is there a non-trivial (i.e. with $R = \mathbb{Z}[a, b] \cap M$ not any R_τ) model of LA_2 which has pp-elimination/is model complete/is NIP?

Can the bounded quantifier elimination for models of LA_κ with $\kappa \geq 2$ be strengthened? If yes, how does it depend on κ ?

Thank you for your attention.

References

- [Yu. Penzin, *Solvability of the theory of integers with addition, order and multiplication by an arbitrary number*, *Matematicheskie Zametki* 13 (1971), no. 5, 667–675]
- [P. Glivický, *Definability in linear arithmetics*, *forthcoming*]
- [P. Glivický and P. Pudlák, *A wild model of linear arithmetic and discretely ordered modules*, to appear in *Mathematical Logic Quarterly*, *arXiv: 1602.03083*]
- [P. Glivický, *Bounded quantifier elimination for ordered modules with integer division and linear arithmetics*, *forthcoming*]