Linear fragments of Peano arithmetic

Petr Glivický

petrglivicky@gmail.com

University of Economics, Prague

JAF 36, St. Petersburg
June 7, 2017

Content

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

- $\mathrm{Pr} = \mathrm{LA}_0$,
- $\mathrm{LA} = \mathrm{LA}_1$,
- LA_2,
- LA_3,
- $\vdots$

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

Every model $\mathcal{A} = \langle A, 0, 1, +, a\cdot, \leq \rangle$ of LA can be canonically "definably" extended to a (discretely ordered) module $\mathcal{M}_\mathcal{A} = \langle M, 0, 1, +, -, r, \leq \rangle_{r \in R_a}$, where $M = A \cup -A$, over the ring $R_a = \mathbb{Q}[a] \cap M$.

For example:

- $(2a) \cdot x$ is defined as $a \cdot x + a \cdot x$,
- $(a^2) \cdot x$ is defined as $a \cdot (a \cdot x)$,
- $(a/2) \cdot x$ is defined as the unique y such that $a \cdot x = y + y$ (assuming $a/2 \in R_a$).

More generally, any $\mathcal{A} = \langle A, 0, 1, +, a_\alpha\cdot, \leq \rangle_{\alpha \in \kappa} \models \mathrm{LA}_\kappa$ corresponds to a discretely ordered module $\mathcal{M}_\mathcal{A}$ over the ring $\mathbb{Q}[a_\alpha]_{\alpha \in \kappa} \cap M$.

We often identify $\mathcal{A}$ and $\mathcal{M}_\mathcal{A}$.

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 module over a ring R (associative, with 1). Then 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 $(\exists \overline{z})\psi$, where ψ 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 $(\exists \overline{z}) \bigwedge_{i<n} \chi_i$, 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* $\bigvee_{i<n}(\exists \overline{z})\psi_i$, *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 $\kappa = 1$.

Moreover, we completely characterize definable sets in models of LA_1 in the process.

Section 3

Definable sets in models of LA_1

All the results will be shown in a more general context of certain discretely ordered modules.

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

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

R_τ denotes an R_a with a having the remainders τ.

It is easy to see that $\mathcal{M}$ 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 $R = R_\tau$ be fixed and $\mathcal{M} = \langle M, 0, 1, -, +, \leq, r\rangle_{r\in R}$ be a fixed discretely ordered (with 1 being the least positive element), integrally-divisible R-module.

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

We show that $\mathcal{M}$ has quantifier elimination in the language extended by functions r^{-1} providing integral division by all scalars $0 < r \in R$.

Let $\mathcal{M}'$ denote the expansion of $\mathcal{M}$ by definitions of functions r^{-1}:

$$r^{-1}(x) = y \leftrightarrow (\exists z)(x = ry + z \,\&\, 0 \leq z < r \cdot 1).$$

Theorem

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

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

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.*

Remarks:

1. This is a common generalization of QE theorems of Baur-Monk and Presburger.
2. The congruences $\equiv_n$ of the QE-language of Pr are quantifier-free definable from the functions r^{-1}. Indeed, $x \equiv_n y \leftrightarrow n \cdot n^{-1}(x-y) = x - y$. (But r^{-1} is not quantifier-free definable from $\equiv_r$ for nonstandard r.)

The proof is quite long and technical. Consists of developing a calculus of so called bracket functions $\left[\begin{smallmatrix} q \\ r \end{smallmatrix}\right](x) = r^{-1}(qx)$ with $q, r \in R$, which extends the calculus of continued fractions.

The problem is much harder than that of unordered modules or Pr. A simple illustration:

When trying to eliminate the quantifiers in the formula

$$(\exists x, y \geq 0) z = qx + ry,$$

with $0 < q, r \in R$ fixed, one has to deal with the set

$$S = \{qx + ry; 0 \leq x, y \in M\}.$$

Above $L = \mathrm{lcm}(q, r)$ we have S is equal to $\{px; x \in M\}$ for $p = \gcd(q, r)$ which is definable by the congruence $x \equiv_p 0$ (and thus "eliminable").

But below L, the set S is quite messy.

$$S = \{qx + ry; 0 \leq x, y \in M\}$$

Above L: $S = \{px; x \in M\}$. Below L: S messy.

Now:

- **For Pr:** L and thus also $S \cap [0, L]$ are finite $\Rightarrow$ eliminable,
- **For unordered modules** (Baur-Monk): No inequalities, so we have $S = \{qx + ry; x, y \in M\}$ equal to $\{px; x \in M\}$ everywhere $\Rightarrow$ eliminable,
- **For LA_1:** $S \cap [0, L]$ messy and can be infinite if q, r are nonstandard $\Rightarrow$ a problem...

... and this is just the simplest case. The general problem is multidimensional, needs to deal also with inverses r^{-1}, ...

Definable functions and sets

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

We are going to characterize all definable functions and definable sets in $\mathcal{M}$.

By the QE Theorem, every definable function is a "piecewise term", i.e. an expression of the form

$$\tau(\overline{x}) = \begin{cases} t_i(\overline{x}) \text{ if } \psi_i(\overline{x}), \ i < n, \end{cases}$$

where t_i are terms, ψ_i are formulas that define a disjoint covering of $M^{l(\overline{x})}$.

The terms of $\mathcal{M}'$ can be quite complex as functions r^{-1} are not distributive w.r.t. addition and do not commute with multiplication; e.g. $r^{-1}(qx + px)$ cannot be easily simplified.

A term $t(\overline{x})$ is called harmonic if it is a linear combination of basic "harmonic" terms r^{-1}:

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

for some $q_i, r_i \in \mathrm{D}$, $c \in \mathrm{C}$ and $f : N \to l(\overline{x})$.

A formula or a piecewise term are harmonic if all its maximal subterms (including those in the side-formulas ψ_i) are. They are quantifier-free if all maximal subformulas are quantifier free.

Harmonic form theorem

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

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

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

Theorem (Harmonic form theorem)

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

Representation of definable sets

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

More precisely: For $\bar{a} \in M$ we denote by $K(\bar{a})$ the $l(\bar{a})$-dimensional box $K(\bar{a}) = \prod_{i<l(\bar{a})}[0, a_i]$.

A polyhedron over $X \subseteq M$ is any subset of M^m, for any m, definable by a system of linear inequalities with parameters from X.

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 $g : (K(\bar{a}) \times M)^n \to M^n$ is a "linear coordination" of M^n, $\bar{a} \in M^l$, $l \in \mathbb{N}$, and P_i, for $i < k$, are finitely many polyhedra in $(K(\bar{a}) \times M)^n$ over parameters from X.

Section 4

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* $\mathcal{A}, \mathcal{B} \models \mathrm{LA}$, *it is* $\mathcal{A} \equiv \mathcal{B} \Leftrightarrow a^{\mathcal{A}} \equiv a^{\mathcal{B}} \mod n$, *for all* $0 < n \in \mathbb{N}$.
$\mathrm{LA}_\tau = \mathrm{LA} + \{a \equiv \tau(p,k) \mod p^k; p \in \mathbb{N}$ *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 (over certain basic* LA^-*)*
$(\exists y, z)(x = qy + z \,\&\, z < q)$, *for all* $0 < q \in \mathbb{Z}[a]$.

Remark: All these properties are similar to those well-known for Pr. But we have already seen that the proof is much harder.

Corollary

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

$$\mathbb{N}_{\mathcal{U}} = (\prod_{n\in\mathbb{N}} \langle \mathbb{N}, 0, 1, +, n\cdot, \leq \rangle)/\mathcal{U},$$

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

Thus models of LA can be seen as "pseudofinite" $\mathbb{Z}$-modules.

A theory T is NIP (not independence property) if the following does not exist in any $\mathcal{M} \models T$:

$$\text{an } L(T)\text{-formula } \varphi(\overline{x}, \overline{y}), \text{ sequences } (\overline{a_i})_{i\in\mathbb{N}}, (\overline{b_J})_{J\subseteq\mathbb{N}},$$

such that $\mathcal{M} \models \varphi(\overline{a_i}, \overline{b_J}) \Leftrightarrow i \in J$.

I.e. T is NIP if no model of T encodes the powerset $\mathcal{P}(\mathbb{N})$ of $\mathbb{N}$.

A theory T is dp-minimal if the following does not exist in any $\mathcal{M} \models T$:

$$L(T)\text{-formulas } \varphi(x, \overline{y}), \psi(x, \overline{y}) \text{ sequences } (\overline{a_i})_{i\in\mathbb{N}}, (\overline{b_j})_{j\in\mathbb{N}},$$

such that for all $i, j \in \mathbb{N}$ the following has a solution $x \in M$:
$\varphi(x, \overline{a_i}) \,\&\, \psi(x, \overline{b_j}) \,\&\, \bigwedge_{k\neq i} \neg\varphi(x, \overline{a_k}) \,\&\, \bigwedge_{l\neq j} \neg\psi(x, \overline{b_l})$.

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 $x \mapsto (x \operatorname{div} a, x \bmod a)$ is a definable function which is a bijection between infinite sets $[0, a^2)$ and $[0, a)^2$.

Application: (In)dependence of Peano multiplications

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

Over a fixed saturated model of Pr, the value of a saturated "Peano multiplication" in the point (c, d) is uniquely determined by its values on the line $\{(a, x); x \in M\} \subseteq M^2$ if and only if c or d is a polynomial in a over $\mathbb{Q}$.

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) *$c \cdot d = c \circ d$ for every Peano multiplication $\circ$ on $\mathcal{M}$ with $a \cdot x = a \circ x$ for all $x \in M$.*
2) *$c \in \mathbb{Q}[a]$ or $d \in \mathbb{Q}[a]$.*

Section 5

Properties of LA_2 and above

Wild models of LA_2

Unlike models of Pr and LA, models of LA_2 can be model-theoretically wild. There is a model of LA_2 where a nonstandard initial segment of a Peano multiplication is definable:

Proposition (with P. Pudlák)

There is a model $\mathcal{M} = \langle M, 0, 1, +, a\cdot, b\cdot, \leq \rangle \models \mathrm{LA}_2$ and a nonstandard $I \in M$ such that $\cdot \restriction [0, I]^2$ is definable in $\mathcal{M}$ for some Peano multiplication $\cdot$ on $\mathcal{M}$ (i.e. such that $\langle M, 0, 1, +, \cdot, \leq \rangle \models \mathrm{PA}$).

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

Unlike Pr and LA:

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:

Multiplication on $[0, I]^2$ can be defined from the squaring function on $[0, 2I]$ by $x \cdot y = ((x + y)^2 - x^2 - y^2)/2$.

In a saturated model of Peano arithmetic, for any $\mathbb{N} < I \in M$, we find elements a, b such that the sequence $(1, 1^2, 2, 2^2, \ldots, 2I, (2I)^2)$ 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 (though unstable) is NIP.

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

We answer **NO**:

Corollary (with P. Pudlák)

The wild model $\mathcal{M}$ of LA_2 from the previous proposition, considered as an ordered module over $\mathbb{Z}[a,b]/_{=_M}$, is not NIP.

We know that no pp-elimination is possible for the arithmetics LA_κ with $\kappa \geq 2$. However, the arithmetics LA_κ satisfy bounded QE for all κ:

Recall that an ordered R-module $\mathcal{M} = \langle M, 0, 1, +, -, \leq, r\rangle_{r\in R}$ with a unit $1 > 0$ is called integrally divisible if
$\mathcal{M} \models (\forall x)(\exists y, z)(x = ry + z \,\&\, 0 \leq z < r \cdot 1)$ for every $0 < r \in R$.

Theorem

Let $\mathcal{M}$ be an integrally divisible ordered module with unit. Then every formula is in $\mathcal{M}$ equivalent to a bounded formula.

Corollary

For any κ, every $\mathcal{M} \models \mathrm{LA}_\kappa$ 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 $\psi(\overline{x})$ is protoperiodic.

$\psi(\overline{x})$ is protoperiodic if there exists a disjoint covering $\mathcal{A}$ of $M^{l(\overline{x})}$ by finitely many convex polyhedra, such that for any $A \in \mathcal{A}$ and a direction $s = \overline{\alpha} \in R^{l(\overline{x})}$ 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. $(\forall \overline{u}, \overline{v} \in A)((\exists m \in M)\overline{u} = Psm + \overline{v} \to (\psi(\overline{u}) \leftrightarrow \psi(\overline{v})))$).

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 $\mathcal{M}_R$ 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, forthcomming]*
- *[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, forthcomming]*