

Doctoral thesis:
Study of Arithmetical Structures and Theories
with Regard to Representative and Descriptive
Analysis

Petr Glivický

petrglivicky@gmail.com

Dept. of Theoretical Computer Science and Mathematical Logic
Faculty of Mathematics and Physics
Charles University in Prague

Doctoral thesis defense
23.9.2013
Prague

Slides available at <http://www.glivicky.cz>

Content

- 1 Analysis of Linear theories
 - Linear theories
 - QE for liner theories
 - Properties of linear arithmetic
 - A more detailed analysis
- 2 Dependency of Peano products
 - Dependency problem
 - Meeting pairs of Peano products
- 3 Quasi-Euclidean rings

Section 1

Analysis of Linear theories

Linear arithmetic

Presburger
arithmetic

Pr

$\langle 0, 1, +, \leq \rangle$

Linear
arithmetic

LA

$L^{lin} = \langle 0, 1, +, \underline{a}, \leq \rangle$

Peano
arithmetic

P

$\langle 0, 1, +, \cdot, \leq \rangle$

Linear arithmetic (LA) is the extension of Pr by

$$\underline{a}(x + 1) = \underline{a}x + \underline{a}1,$$

$$\underline{a}1 \neq n \text{ for all } n \in \mathbb{N},$$

induction for all L^{lin} -formulas.

ZLA is a \mathbb{Z} -like variant of LA.

Ring of scalars

Let $\mathcal{A} = \langle A, 0, 1, +, -, \underline{a}, \leq \rangle \models \text{ZLA}$.

For $q \in \mathbb{Q}[a] \cap A = D_{\mathcal{A}}$, we may define multiplication by q (“scalar” \underline{q}).

$D_{\mathcal{A}}$ is a discretely ordered integral domain and \mathcal{A} may be seen as a discretely ordered $D_{\mathcal{A}}$ -module.

Doded

An ordered integral domain $D = \langle D, 0, 1, +, -, \cdot, \leq \rangle$ is called a **doded** if it

- is discretely ordered by \leq , with 1 being the least positive element,
- is regularly quasi-Euclidean, i.e. the Euclidean algorithm in D is correctly defined and always stops in finitely many steps,
- has degrees, i.e. there is a function $\text{deg} : D \rightarrow \mathbb{N} \cup \{-\infty\}$ such that $\text{rng}(\text{deg})$ is a lower set in $\mathbb{N} \cup \{-\infty\}$, and $\text{deg } r \leq \text{deg } q \Leftrightarrow |r| \leq n|q|$, for some $n \in \mathbb{N}$.

Example

The ordered ring \mathbb{Z} and the rings $D_{\mathcal{A}}$ for $\mathcal{A} \models \text{ZLA}$ are dodeds.

Lineal

Let $\mathcal{A} = \langle A, 0, 1, +, -, \underline{a}, \leq \rangle \models \text{ZLA}$:

In \mathcal{A} , we may define

- scalar multiplication \underline{q} , for $q \in D_{\mathcal{A}}$,
- constants $\mathbf{q} = \underline{q}(1)$, for $q \in D_{\mathcal{A}}$,
- integral inverses \underline{q}^{-1} , for $0 < q \in D_{\mathcal{A}}$ ($0 \leq x - \underline{q}(\underline{q}^{-1}(x)) < \mathbf{q}$).

The set $\mathbf{C}_{\mathcal{A}} = \{\mathbf{q}; q \in D_{\mathcal{A}}\}$ is a universe of a substructure of $\mathcal{F}_{\mathcal{A}} = \langle A, 0, 1, +, -, \leq, \underline{q}, \mathbf{q}, \underline{r}^{-1} \rangle_{q \in D_{\mathcal{A}}, 0 < r \in D_{\mathcal{A}}}$.

Linear

A **lineal** is any structure

$\mathcal{F} = \langle F, 0, 1, +, -, \leq, r, c, q^{-1} \rangle_{r \in D_{\mathcal{F}}, c \in C_{\mathcal{F}}, 0 < q \in D_{\mathcal{F}}}$ where

- $D_{\mathcal{F}}$ is an universe of a doded $D_{\mathcal{F}}$,
- \mathcal{F} and $C_{\mathcal{F}} = \mathcal{F} \upharpoonright C_{\mathcal{F}}$ are expansions of discretely ordered $D_{\mathcal{F}}$ -modules (with the least positive element 1) by constants c and integral inverses q^{-1} .

Example

The expansion $\mathcal{F}_{\mathcal{A}}$ of any model \mathcal{A} of ZPr or ZLA is a lineal.

Linealization

For different models $\mathcal{A}, \mathcal{B} \models \text{ZLA}$, the rings of scalars $D_{\mathcal{A}}, D_{\mathcal{B}}$ may be different subrings of $\mathbb{Q}[a]$.

That is, the lineals $\mathcal{F}_{\mathcal{A}}, \mathcal{F}_{\mathcal{B}}$ are expansions of \mathcal{A}, \mathcal{B} , respectively, by different sets of definitions.

Linear theory

Let L be a language extending $L^Z = \langle 0, 1, +, -, \leq \rangle$ (where $-$ is unary), T be an L -theory, and let $D, C \subseteq Fm_L$. A **(D, C)-linearization** of T is any map $\mathcal{A} \mapsto \mathcal{F}_{\mathcal{A}}$, for $\mathcal{A} \models T$, such that every

$$\mathcal{F}_{\mathcal{A}} = \langle A, 0, 1, +, -, \leq, r, c, q^{-1} \rangle_{r \in D_{\mathcal{F}_{\mathcal{A}}}, c \in C_{\mathcal{F}_{\mathcal{A}}}, q \in {}^+D_{\mathcal{F}_{\mathcal{A}}}}$$

is a lineal equidefinable with \mathcal{A} and satisfying $D_{\mathcal{F}_{\mathcal{A}}} \subseteq D$ and $C_{\mathcal{F}_{\mathcal{A}}} \subseteq C$.

An L -theory T is a **linear theory** if it has an (Fm_L, Fm_L) -linearization.

Example

ZPr and ZLA are linear theories.

ZPr has a (\mathbb{Z}, \mathbb{Z}) -linearization, ZLA has a $(\mathbb{Q}[a], \mathbb{Q}[a])$ -linearization.

Solvable theories

A theory T is **[n]-solvable** [for $n \in \mathbb{N}$] if, for every model $\mathcal{M} \models T$, every L -formula $\varphi(x, \bar{y})$ [with $l(\bar{y}) \leq n$] and an $l(\bar{y})$ -tuple \bar{a} from M , it holds

$$\mathcal{M} \models (\exists x)\varphi(x, \bar{a}) \Rightarrow \mathcal{M} \models \varphi(t(\bar{a}), \bar{a}), \text{ for some } L_T\text{-term } t.$$

T is **almost uniformly solvable** if, for each quantifier-free formula $\psi(x, \bar{y})$, there are finitely many terms t_i , $i < n$, such that

$$T \vdash (\exists x)\psi(x, \bar{y}) \rightarrow \bigvee_{i < n} \psi(t_i(\bar{y}), \bar{y}).$$

Solvable extensions by definitions

For a theory T and $F \subseteq Fm_L$, we write

$$T^F = T \cup \{\delta(\varphi); \varphi \in F\}$$

for the extension of T by functions definable by formulas from F , where $\delta(\varphi)$ is the conditional definition of a new function symbol $\underline{\varphi}$:

$$(cor(\varphi) \ \& \ \varphi(\bar{x}, \underline{\varphi}(\bar{x}))) \vee (\neg cor(\varphi) \ \& \ \underline{\varphi}(\bar{x}) = 0).$$

Remark

Any set F such that T^F is solvable corresponds to an elimination set of T .

Main theorem on linear theories

Theorem (Main theorem on linear theories)

Let T be a linear theory in a language L , having a (D, C) -linearization; denote $E = D \cup C \cup D^{-1}$. Then

- 1) T^E is almost uniformly solvable.
- 2) T^C is 0-solvable.

Corollaries

Corollary

- 1) T^E admits quantifier elimination and is axiomatizable by open formulas.
- 2) For $\mathcal{A} \models T$, the structure $\mathcal{C}_{\mathcal{A}}$ is the unique prime model of $Th(\mathcal{A})$.
- 3) For $\mathcal{A} \models T$, the theory $Th(\mathcal{A})$ is equivalent to $T \cup OTh_L(\mathcal{A}^C)$ (or equivalently to $T \cup OTh_L(\mathcal{C}_{\mathcal{A}}^C)$),

where $OTh_L(\mathcal{N})$ is the canonical L -translation of the set of all open sentences true in \mathcal{N} .

Properties of LA

LA^\bullet denotes the extension of LA by conditional definitions of all scalars q , constants $\mathbf{q} = \underline{q}1$ and integral divisors \underline{q}^{-1} for $0 < q \in \mathbb{Q}[a]$.

LA° denotes the extension of LA by conditional definitions of all constants \mathbf{q} for $0 < q \in \mathbb{Q}[a]$.

\mathbb{J}_p denotes the set of all p -adic integers, for $p \in \mathbb{P}$.

LA_τ , for $\tau \in \prod_{p \in \mathbb{P}} \mathbb{J}_p$, is the extension of LA by axioms (α_τ) expressing $\mathbf{a} = \tau_p(k) \bmod \mathbf{p}^k$, for all $p \in \mathbb{P}$, $0 < k \in \mathbb{N}$.

Let $\mathbb{Z}[a] \subseteq \mathbf{D}_\tau \subseteq \mathbb{Q}[a]$ be the set of all $\frac{r}{n} \in \mathbb{Q}[a]$, $0 < n \in \mathbb{N}$, $r \in \mathbb{Z}[a]$, such that “ $n|r(a)$ whenever a satisfies the congruences (α_τ) ”.

We set $\mathbf{C}_\tau^+ = \langle {}^+\mathbf{D}_\tau, 0, 1, +, -, \leq, \underline{a} \rangle$, where \underline{a} is the unary function of multiplication by the variable a .

Properties of LA

Theorem (Properties of LA)

1) LA^\bullet is solvable, LA° is 0-solvable.

Hence: 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) LA_τ , for $\tau \in \prod_{p \in \mathbb{P}} \mathbb{J}_p$, are all simple complete extensions of LA .

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

3) C_τ^+ 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

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

Properties of LA

Corollary

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

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

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 [un]decomposability of sets $\{qx + ry; x, y \in A\}$ in $\mathcal{A} \models \text{Pr}[\text{LA}]$).

Open question

There is a hierarchy of linear arithmetics:

LA_{κ} = “extension of Pr by κ independent scalars”

$LA_0 = Pr$

$LA_1 = LA$

$LA_2 \dots ?$

Open question

- a) Are model-theoretical properties of LA_{κ} , with $\kappa \geq 2$, still similar to those of Pr? In particular, are theories LA_{κ} , with $\kappa \geq 2$, model-complete and decidable?
- b) Could be some model of P definable in a model of LA_{κ} ?

A more detailed analysis

Let \mathcal{F} be a fixed linear, in particular \mathcal{F} can be a linear extension of a model of ZLA.

We write D and C instead of $D_{\mathcal{F}}$ and $C_{\mathcal{F}}$.

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

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

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

A formula is 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 $c_i \in C$, for $i < n$.

Harmonic form theorem

Theorem (Harmonic form theorem)

Let \mathcal{F} be a lineal.

- 1) For every term $t(\bar{x})$, there is an open harmonic almost-term $\tau(\bar{x})$ such that $\mathcal{F} \models t(\bar{x}) = \tau(\bar{x})$.
- 2) For every formula $\varphi(\bar{x})$, there is an open harmonic formula $\psi(\bar{x})$ such that $\mathcal{F} \models \varphi(\bar{x}) \leftrightarrow \psi(\bar{x})$.

Representation of definable sets

Theorem

Every set $D \subseteq F^n$ X -definable in a lineal \mathcal{F} can be written as

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

where $g : (K(\bar{a}) \times F)^n \rightarrow F^n$ is a $(\bar{\delta}, \bar{a}, p)$ -coordination of F^n , with $a_0 = m \in \mathbb{N}$, $\bar{a} = (a_0, \dots, a_N)$ and p a scalar, and $P_i \subseteq P_g$, for $i < k$, are finitely many polyhedra in $(K(\bar{a}) \times F)^n$ over parameters from $X \cup \bar{\delta}$.

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

Two-sorted QE for doded-modules

Let \mathbb{L} denotes the two-sorted language of “ordered rings-ordered modules”.

A **doded-module** is a (two-sorted) \mathbb{L} -structure $\mathcal{A} = \langle \mathcal{R}, \mathcal{M}, \cdot \rangle$ such that

- 1) \mathcal{R} is a doded,
- 2) $\langle \mathcal{M}, r \cdot _ \rangle_{r \in R}$ is a discretely ordered (with 1 being the least positive element), integrally-divisible (i.e. $(\forall x)(\exists y)(\exists 0 \leq z < r \cdot 1)(x = r \cdot y + z)$ holds) \mathcal{R} -module.

Two-sorted QE for doded-modules

Let \mathbb{L}' denotes the extension of \mathbb{L} by symbols $\bar{\cdot}^{-1} : \mathcal{R}^2 \rightarrow \mathcal{R}$,
 $\bar{\cdot}^{-1} : \mathcal{R} \times \mathcal{M} \rightarrow \mathcal{M}$ for integral division.

For a doded-module \mathcal{A} , let \mathcal{A}' denotes the natural definable \mathbb{L}' -expansion of \mathcal{A} .

Theorem

Let $\mathcal{A} = \langle \mathcal{R}, \mathcal{M}, \cdot \rangle$ be a doded-module, $\varphi(\bar{r}, \bar{y}, x)$ be an \mathbb{L}' -formula without scalar quantifiers, and $\bar{\rho} \in R^{l(\bar{r})}$ be scalars. Then there are finitely many \mathbb{L}' -terms $t_i(\bar{r}, \bar{y})$, for $i < n$, with $n \in \mathbb{N}$, such that

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

Two-sorted QE for doded-modules

Corollary

Let \mathcal{A} be a doded-module. Every scalar-quantifier-free \mathbb{L}' -formula is in \mathcal{A}' equivalent to a quantifier-free \mathbb{L}' -formula.

This generalizes results of van den Dries-Holly and Weispfenning on two-sorted q.e. for unordered ring-modules resp. ordered \mathbb{Z} -modules.

Section 2

Dependency of Peano products

Dependency problem

Given a “background model” \mathcal{B} and a set O of all n -ary operations on B satisfying certain global property (e.g. being a Peano product), we want to describe the dependency closure

$$\text{icl}^O(E) = \{\bar{d} \in B^n; (\forall o, o' \in O)(o \upharpoonright E = o' \upharpoonright E \Rightarrow o(\bar{d}) = o'(\bar{d}))\},$$

for $E \subseteq B^n$. We call this task the (\mathcal{B}, O, E) -dependency problem.

In particular, what if $\mathcal{B} \models \text{Pr}$ and O is the set of all Peano products on \mathcal{B} ?

DD-theorem

Proposition (DD-theorem)

Let o be an n -ary operation on B , $\bar{d} \in B^n$, and $E = E_s \cup E_f \subseteq B^n$, where $|E_s| < |B|$, and suppose that there is a saturated (G, E_f) -fixator \mathcal{A} for o , with $G \subseteq \text{Aut}(B)$. Then the following statements are equivalent:

- 1) $\bar{d} \in \text{icl}_o^{\sim G}(E)$,
- 2) o is a.u.-definable at \bar{d} over E_s in \mathcal{A} .

An operation o is in \mathcal{A} **almost-uniformly definable (a.u.-definable)** at a point $\bar{d} \in A^n$ over a set $E \subseteq A^n$ if, for all $\langle \bar{e}', \bar{d}' \rangle_{\bar{e} \in E}$ such that $\varepsilon = \text{concat} \langle \bar{e}, o(\bar{e}), \bar{d} \rangle_{\bar{e} \in E}$ and $\varepsilon' = \text{concat} \langle \bar{e}', o(\bar{e}'), \bar{d}' \rangle_{\bar{e} \in E}$ are indistinguishable in \mathcal{A} , the pair $(o(\bar{d}), o(\bar{d}'))$ is equidefinable from $(\varepsilon, \varepsilon')$ in \mathcal{A} .

DD-theorem

Proposition (DD-theorem)

Let o be an n -ary operation on B , $\bar{d} \in B^n$, and $E = E_s \cup E_f \subseteq B^n$, where $|E_s| < |B|$, and suppose that there is a saturated (G, E_f) -fixator \mathcal{A} for o , with $G \subseteq \text{Aut}(B)$. Then the following statements are equivalent:

- 1) $\bar{d} \in \text{icl}_o^G(E)$,
- 2) o is a.u.-definable at \bar{d} over E_s in \mathcal{A} .

Let $G \subseteq \text{Aut}(B)$ be a subgroup, o an n -ary operation on B , and $E \subseteq B^n$. We say that a saturated expansion \mathcal{A} of B is a (G, E) -fixator for o if

$$g \in \text{Aut}(\mathcal{A}) \Leftrightarrow g \in G, \text{ and } og(\bar{x}) = go(\bar{x}) \text{ for all } \bar{x} \in E.$$

For $o, o' \in O$, we write $o \sim^G o'$ if $o \cong o'$ via some $g \in G$.

Dependency closure for Peano products

Let \mathcal{B} be a fixed saturated model of Pr. We determine $\text{icl}^O(E_a)$ for $E_a = B \times \{a\}$ where $a \in B$ is non-standard.

$$D_a = \left\{ \frac{p}{n}; 0 \leq p \in \mathbb{Z}[a], 0 < n \in \mathbb{N} \text{ and } \mathcal{B} \models n|p \right\} = \mathbb{Q}[a] \cap B$$

Theorem

It is $\text{icl}^{P(\mathcal{B})}(E_a) = \text{icl}^{\text{PP}(\mathcal{B})}(E_a) = \text{icl}^{\text{sPP}(\mathcal{B})}(E_a) = \text{icl}^{\cong_a}(E_a) = \text{icl}^{\cong_a}(E_a)$ and all are equal to $(D_a \times B) \cup (B \times D_a)$.

Here $P(\mathcal{B})$ denotes the set of all commutative, associative and distributive Robinson products on \mathcal{B} and $\text{PP}(\mathcal{B})$ [$\text{sPP}(\mathcal{B})$] the set of all [saturated] Peano products on \mathcal{B} .

The proof uses the DD-theorem and quantifier elimination for LA: **The fixator for E_a is a model of LA.**

Meeting pairs of Peano products

Let $a \in B - \mathbb{N}$. A pair (\cdot, \circ) of Peano products on B is called an **a -meeting pair** if it is $\cdot \upharpoonright E_a = \circ \upharpoonright E_a$, and $d_0 \cdot d_1 \neq d_0 \circ d_1$, $d'_0 \cdot d'_1 \neq d'_0 \circ d'_1$, for some $d_0, d_1 < a < d'_0, d'_1$.

Corollary (Existence of meeting pairs)

Let $a \in B - \mathbb{N}$, and $\cdot \in \text{sPP}(B)$ be a saturated Peano product on B . Then there is $\circ \in \text{sPP}(B)$ such that (\cdot, \circ) is an a -meeting pair of Peano products on B . Moreover, \circ can be chosen in such a way that $\cdot \cong_a \circ$.

Construction of a new product

We denote LB_x [LcB_x] the set of formulas $\varphi(x, \bar{y})$ in the language of arithmetic $L^{ar} = \langle 0, S, +, \cdot, \leq \rangle$ such that every occurrence of multiplication in φ has the form $x \cdot z$ or $z \cdot x$, where z is a variable which is bound by a quantifier $Qz \leq x$ [$Qz \geq x$].

The L^{ar} -theory ILB [$ILcB$] is the extension of Robinson arithmetic Q by the scheme of induction $I(LB_x)$ [$I(LcB_x)$] for all formulas φ from LB_x [LcB_x] (here, x is the “induction variable”).

Proposition

Let $a \in B - \mathbb{N}$, and (\cdot, \circ) be an a -meeting pair of Peano products on B .

- 1) For $\times = \cdot \upharpoonright [0, a]^2 \cup \circ \upharpoonright (B^2 - [0, a]^2)$, it is $\langle B, \times \rangle \models ILB$.
- 2) For $\times' = \cdot \upharpoonright [a, \infty)^2 \cup \circ \upharpoonright (B^2 - [a, \infty)^2)$, it is $\langle B, \times' \rangle \models ILcB$.

Construction of a new product

Open question

Is it possible, by using similar methods, to construct Robinson products \times which satisfy $I(\Gamma)$ for other sets $\Gamma \subseteq Fm_{L^{ar}}$? In particular, is it possible to construct Peano products this way?

Section 3

Quasi-Euclidean rings

Quasi-Euclidean rings

Theorem

Let $\tau \in \prod_{p \in \mathbb{P}} \mathbb{J}_p$ be arbitrary. Then the ring D_τ is ω -stage Euclidean (quasi-Euclidean) but not k -stage Euclidean for any positive integer k .

I.e. there are 2^ω rings R with $\mathbb{Z}[x] \subseteq R \subseteq \mathbb{Q}[x]$ which are ω -stage Euclidean but not k -stage Euclidean for any positive integer k .

This answers a question of G. E. Cooke from 1976.

Thank you

Thank you for your attention.