Quantifier elimination for linear arithmetic

Petr Glivický

petrglivicky@gmail.com

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

Manchester
17.9.2013

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

Content

Linear arithmetic

Presburger arithmetic	Linear arithmetic	Peano arithmetic
Pr	LA	P
$\langle 0, 1, +, \leq \rangle$	$L^{lin} = \langle 0, 1, +, \underline{a}, \leq \rangle$	$\langle 0, 1, +, \cdot, \leq \rangle$

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.

Example

Let $\mathcal{M} = \langle M, 0, 1, +, \cdot, \leq \rangle \models \mathrm{P}$ be nonstandard and $a \in M - \mathbb{N}$ then $\langle M, 0, 1, +, a \cdot \_, \leq \rangle \models \mathrm{LA}$.

Ring of scalars

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

Let $\mathcal{A} = \langle A, 0, 1, +, -, \underline{a}, \leq \rangle \models \mathrm{ZLA}$.
For each $q \in \mathbb{Q}[a] \cap A = \mathrm{D}_{\mathcal{A}}$, we may define multiplication by q ("scalar" $\underline{q}$).

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

Doded

An ordered integral domain $\mathrm{D} = \langle \mathrm{D}, 0, 1, +, -, \cdot, \leq \rangle$ 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 $\deg : \mathrm{D} \to \mathbb{N} \cup \{-\infty\}$ such that $\mathrm{rng}(\deg)$ is a lower set in $\mathbb{N} \cup \{-\infty\}$, and $\deg r \leq \deg q \Leftrightarrow |r| \leq n|q|$, for some $n \in \mathbb{N}$.

Example

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

Lineal

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

In $\mathcal{A}$, we may define

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

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

Lineal

A lineal is any structure
$\mathcal{F} = \langle F, 0, 1, +, -, \leq, r, c, q^{-1} \rangle_{r \in \mathrm{D}_\mathcal{F}, c \in \mathrm{C}_\mathcal{F}, 0 < q \in \mathrm{D}_\mathcal{F}}$ where

- $\mathrm{D}_\mathcal{F}$ is an universe of a doded $\mathrm{D}_\mathcal{F}$,
- $\mathcal{F}$ and $\mathcal{C}_\mathcal{F} = \mathcal{F} \restriction \mathrm{C}_\mathcal{F}$ are expansions of discretely ordered $\mathrm{D}_\mathcal{F}$-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 $\mathcal{A}, \mathcal{B} \models \mathrm{ZLA}$, the rings of scalars $\mathrm{D}_{\mathcal{A}}, \mathrm{D}_{\mathcal{B}}$ 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 $\mathrm{D}, \mathrm{C} \subseteq Fm_L$. A (D, C)-linealization of T is any map $\mathcal{A} \mapsto \mathcal{F}_\mathcal{A}$, for $\mathcal{A} \models T$, such that every

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

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

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

Example

ZPr and ZLA are linear theories.
ZPr has a $(\mathbb{Z}, \mathbb{Z})$-linealization, ZLA has a $(\mathbb{Q}[a], \mathbb{Q}[a])$-linealization.

Solvable theories

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

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

Proposition

For a theory T in a language with a constant symbol, it is equivalent:

1) *T is solvable.*
2) *T has quantifier elimination and is axiomatizable by open formulas.*
3) *T is model-complete and is axiomatizable by open formulas.*
4) *For $\mathcal{N} \subseteq \mathcal{M} \models T$, it is $\mathcal{N} \prec \mathcal{M}$.*
5) *For $\mathcal{M} \models T$, $X \subseteq M$, it is $M\langle X \rangle = M_{(X)}$, and it is a dense set (of all atoms) in $\mathrm{Df}^1(X, \mathcal{M})$.*

Almost uniform solvability

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

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

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 $\underline{\varphi}$:

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

Example

All arithmetical theories with full induction ($T = \mathrm{Pr}, \mathrm{LA}, \mathrm{P}$) have solvable extensions by definitions (i.e. T^{Fm_L} is solvable): For every $\varphi(x, \overline{y})$ define a new function $f(\overline{y})$ giving the minimal x such that $\varphi(x, \overline{y})$ holds (or 0 if there is no such x).

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, $\mathcal{A} \mapsto \mathcal{F}_{\mathcal{A}}$ be a (D, C)-linealization, and $E = \mathrm{D} \cup \mathrm{C} \cup \mathrm{D}^{-1}$. 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

$\mathrm{LA}^\bullet$ denotes the extension of LA by conditional definitions of all scalars $\underline{q}$, 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 $\mathbf{a} = \tau_p(k) \mod \mathbf{p^k}$, for all $p \in \mathbb{P}$, $0 < k \in \mathbb{N}$.

Let $\mathbb{Z}[a] \subseteq \mathrm{D}_\tau \subseteq \mathbb{Q}[a]$ 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 $\mathcal{C}_\tau^+ = \langle {}^+\mathrm{D}_\tau, 0, 1, +, -, \leq, \underline{a}\rangle$, where $\underline{a}$ is the unary function of multiplication by the variable a.

Properties of LA

Theorem (Properties of LA)

1) $\mathrm{LA}^\bullet$ *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 $\mathcal{A}, \mathcal{B} \models \mathrm{LA}$*, it is* $\mathcal{A} \equiv \mathcal{B} \Leftrightarrow \mathbf{a}^{\mathcal{A}} \equiv \mathbf{a}^{\mathcal{B}} \mod n$*, for all* $0 < n \in \mathbb{N}$*.*

3) $\mathcal{C}_\tau^+$ *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*
$$(\exists y, z)(x = \underline{q}y + z \,\&\, z < \underline{q}),\ \text{for all } 0 < q \in \mathbb{Z}[a].$$

Properties of LA

Corollary

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

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

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

Open question

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 lineal, in particular $\mathcal{F}$ can be a lineal extension of a model of ZLA.
We write D and C instead of $\mathrm{D}_{\mathcal{F}}$ and $\mathrm{C}_{\mathcal{F}}$.

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

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

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

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

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

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

Harmonic form theorem

Theorem (Harmonic form theorem)

Let $\mathcal{F}$ be a lineal.

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

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

"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 $\frac{-1}{\mathcal{R}} : \mathcal{R}^2 \to \mathcal{R}$, $\frac{-1}{\mathcal{M}} : \mathcal{R} \times \mathcal{M} \to \mathcal{M}$ 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, $\varphi(\overline{r}, \overline{y}, x)$ be an $\mathbb{L}'$-formula without scalar quantifiers, and $\overline{\rho} \in R^{l(\overline{r})}$ be scalars. Then there are finitely many $\mathbb{L}'$-terms $t_i(\overline{r}, \overline{y})$, for $i < n$, with $n \in \mathbb{N}$, such that

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

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.

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

$$\mathrm{icl}^O(E) = \{\overline{d} \in B^n; (\forall o, o' \in O)(o \restriction E = o' \restriction E \Rightarrow o(\overline{d}) = o'(\overline{d}))\},$$

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

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

Dependency closure for Peano products

Let $\mathcal{B}$ be a fixed saturated model of Pr, O a set of binary operations on B (products).

A point $\overline{d} \in B^2$ *O-depends* on $E \subseteq B^2$ *[for $\cdot \in O$]* if, for all $\circ, \circ' \in O$ [such that $\circ' = \cdot$] and $\circ \restriction E = \circ' \restriction E$, it is $d_0 \circ d_1 = d_0 \circ' d_1$.

The set $\mathrm{icl}^O_{[\cdot]}(E) = \{\overline{d} \in B^2; \overline{d} \sim$-depends on E [for $\cdot$]$\}$ is called the O-dependency closure of E [for $\cdot$].

Dependency closure for Peano products

Determining $\mathrm{icl}^{O}(E)$ for $|E| < |\mathcal{B}|$ is relatively easy.

In particular:

Theorem

It is $\mathrm{icl}^{\mathsf{P}(\mathcal{B})}(\mathbb{N}) = \mathrm{icl}^{\mathsf{PP}(\mathcal{B})}(\mathbb{N}) = \mathrm{icl}^{\mathsf{sPP}(\mathcal{B})}(\mathbb{N}) = \mathrm{icl}^{\cong_a}(\mathbb{N}) = \mathrm{icl}^{\cong_a}_{\cdot}(\mathbb{N})$ *and all are equal to* $(\mathbb{N} \times B) \cup (B \times \mathbb{N})$.

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

Dependency closure for Peano products

We determine $\mathrm{icl}^O(E_a)$ 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 $\mathrm{icl}^{\mathsf{P}(\mathcal{B})}(E_a) = \mathrm{icl}^{\mathsf{PP}(\mathcal{B})}(E_a) = \mathrm{icl}^{\mathsf{sPP}(\mathcal{B})}(E_a) = \mathrm{icl}^{\cong_a}(E_a) = \mathrm{icl}^{\cong_a}_{\cdot}(E_a)$ *and all are equal to* $(D_a \times B) \cup (B \times D_a)$.

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

Meeting pairs of Peano products

Let $a \in B - \mathbb{N}$. A pair $(\cdot, \circ)$ of Peano products on $\mathcal{B}$ is called an *a*-meeting pair if it is $\cdot \restriction E_a = \circ \restriction E_a$, 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 $\cdot \in \mathrm{sPP}(\mathcal{B})$ be a saturated Peano product on $\mathcal{B}$. Then there is $\circ \in \mathrm{sPP}(\mathcal{B})$ such that $(\cdot, \circ)$ is an a-meeting pair of Peano products on $\mathcal{B}$. Moreover, $\circ$ can be chosen in such a way that $\cdot \cong_a \circ$.

Thank you

Thank you for your attention.