Quantifier elimination for certain discretely ordered modules

Petr Glivický

petrglivicky@gmail.com

Institute of Mathematics
Academy of Sciences of the Czech Republic

(research performed at the Faculty of Mathematics and Physics,
Charles University in Prague)

ASTA 2014, Spineto
17.6.2014

Content

1. Background

2. Dodeds and doded-modules
   - Two-sorted QE for doded-modules
   - Primitive positive elimination for ordered modules over dodeds
   - A more detailed analysis

3. Application to arithmetics

Section 1

Background

Baur-Monk Theorem

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 $(\exists \overline{z})\psi_i$, 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 $(\exists \overline{z}) \bigwedge_{i<n} \chi_i$, where χ_i are atomic formulas.

Ordered version

Question: What can be said about ordered modules?

Ordered $\mathbb{Z}$-modules $=$ $\mathbb{Z}$-groups $=$ models of Presburger arithmetic (Pr)

$$(\mathrm{Pr} = \mathit{Th}(\langle \mathbb{Z}, 0, 1, -, +, \leq \rangle))$$

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.*

So the following structures have the elimination to (boolean combinations of) pp-formulas:

$\langle M, 0, -, +, r\rangle_{r\in R}$ and $\langle M, 0, 1, -, +, \leq\rangle = \langle M, 0, 1, -, +, \leq, z\rangle_{z\in\mathbb{Z}}$

(unordered) modules — discretely ordered $\mathbb{Z}$-modules

What about ordered modules $\langle M, 0, 1, -, +, \leq, r\rangle_{r\in\mathbb{R}}$ with $R \neq \mathbb{Z}$?

Section 2

Dodeds and doded-modules

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 an initial segment of $\mathbb{N} \cup \{-\infty\}$, and $\deg r \leq \deg q \Leftrightarrow |r| \leq n|q|$, for some $n \in \mathbb{N}$.

Doded

Example

1. The ordered ring $\mathbb{Z}$ is doded. The degree function is given by $\deg(z) = 0$ for $z \neq 0$ and $\deg(0) = -\infty$.
2. Let $\tau \in \prod_{p \in \mathbb{P}} \mathbb{J}_p$ where $\mathbb{J}_p$ is the ring of p-adic integers. We represent τ as a function $\tau : \mathbb{P} \times \mathbb{N} \to \mathbb{N}$ and think of the value $\tau(p, k)$ as the residue $x \mod p^k$ of some fixed element x. The ring R_τ then consists of all $p(x) \in \mathbb{Q}[x]$ which have integer value with respect to τ.

   It is $\mathbb{Z}[x] \subseteq R_\tau \subseteq \mathbb{Q}[x]$, and it can be proven that R_τ is doded for any $\tau \in \prod_{p \in \mathbb{P}} \mathbb{J}_p$.

Remark: Rings R_τ are quasi-Euclidean but not k-stage Euclidean for any $k \in \mathbb{N}$.

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.

Let further D be a fixed doded 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. Denote $\mathcal{M}'$ the expansion of $\mathcal{M}$ by definitions of functions r^{-1} providing integral division by all scalars $0 < r \in D$.

Corollary

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

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

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

Hence $\mathcal{M}'$ has quantifier elimination.

A more detailed analysis

Further, 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 realizations of constants terms in $\mathcal{M}'$.

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

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

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

A formula 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)

1) *For every term $t(\overline{x})$, there is an open 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 an open harmonic formula $\psi(\overline{x})$ such that $\mathcal{M}' \models \varphi(\overline{x}) \leftrightarrow \psi(\overline{x})$.*

Representation of definable sets

Corollary

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, $\bar{a} = (a_0, \ldots, a_l) \in M^l$, $l \in \mathbb{N}$, 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

Application to 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.

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

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

Note that $R_a \cong R_\tau$ for some $\tau \in \prod_{p \in \mathbb{P}} \mathbb{J}_p$ and hence is a doded.

Then the elimination results for doded-modules apply:

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) 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* $\mathcal{A} \equiv \mathcal{B} \Leftrightarrow a^{\mathcal{A}} \equiv a^{\mathcal{B}} \mod n$, *for all* $0 < n \in \mathbb{N}$.

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

Corollary

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

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

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

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 $\mathcal{A} \models \mathrm{Pr}[\mathrm{LA}]$).

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 product"* $\circ$ *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* $d \in \mathbb{Q}[a]$.

Thank you

Thank you for your attention.