Annals of Pure and Applied Logic ••• (••••) •••–•••

Contents lists available at ScienceDirect

Annals of Pure and Applied Logic

www.elsevier.com/locate/apal

Elementary recursive quantifier elimination based on Thom encoding and sign determination

Daniel Perrucci [a,*,1], Marie-Françoise Roy [b]

[a] Departamento de Matemática, FCEN, Universidad de Buenos Aires and IMAS UBA-CONICET, Ciudad Universitaria, 1428 Buenos Aires, Argentina
[b] IRMAR (UMR CNRS 6625), Université de Rennes 1, Campus de Beaulieu, 35042 Rennes cedex, France

ARTICLE INFO

Article history:
Received 9 September 2016
Received in revised form 21 February 2017
Accepted 25 February 2017
Available online xxxx

MSC:
14P10
03C10
14Q20
12D15

Keywords:
Quantifier elimination
Real closed fields
Thom encoding
Sign determination

ABSTRACT

We describe a new quantifier elimination algorithm for real closed fields based on Thom encoding and sign determination. The complexity of this algorithm is elementary recursive and its proof of correctness is completely algebraic. In particular, the notion of connected components of semialgebraic sets is not used.

1. Introduction

The first proofs of quantifier elimination for real closed fields by Tarski, Seidenberg, Cohen or Hörmander [22,21,8,16] were all providing primitive recursive algorithms.

The situation changed with the Cylindrical Algebraic Decomposition method [10] and elementary recursive algorithms where obtained (see also [17,19]). This method produces a set of sampling points meeting every connected component defined by a sign condition on a family of polynomials. Cylindrical Algebraic Decomposition, being based on repeated projections, is in fact doubly exponential in the number of variables (see for example [2, Chapter 11]).

[*] Corresponding author.
E-mail address: perrucci@dm.uba.ar (D. Perrucci).

[1] Partially supported by the Argentinian grants PIP 2014–2016 11220130100527CO CONICET and UBACYT 20020120100133.

http://dx.doi.org/10.1016/j.apal.2017.03.001
0168-0072/© 2017 Elsevier B.V. All rights reserved.

Single exponential degree bounds, using the critical point method to project in one step a block of variables, have been obtained for the existential theory over the reals. The critical point method also gives a quantifier elimination algorithm which is doubly exponential in the number of blocks [13–15,20,1,2].

For all these elementary recursive methods, the proofs of correctness of the algorithms are based on geometric properties of semialgebraic sets, such as the fact that they have a finite number of connected components. They are also valid for general real closed fields, where the notion of semialgebraic connectedness has to be used.

Our aim in this paper is to provide an elementary recursive algorithm for quantifier elimination over real closed fields (Theorem 1) with the particularity that its proof of correctness is entirely based on algebra and does not involve the notion of connected components of semialgebraic sets (see details in Remark 21, Remark 25 and Remark 28).

The development of such algebraic proofs is very important in the field of constructive algebra. For instance, the elimination of one variable step of the algorithm we present here is, in the special case of monic polynomials, a key step in the construction of algebraic identities with elementary recursive degree bounds for the Positivstellensatz and Hilbert 17th problem in [18].

Another motivation for the present work is to provide an elementary recursive algorithm for quantifier elimination over real closed fields, suitable for being formally checked by a proof assistant such as `Coq` [7] using the algebraic nature of its correctness proof. Indeed, because of the algebraic nature of its correctness proof, the original proof of Tarski's quantifier elimination [22], as presented in [2, Chapter 2] has already been checked using `Coq` in [9].

We start with some notation.

Let $\mathbf{R}$ be a real closed field. For $\alpha \in \mathbf{R}$, its *sign* is as usual defined as follows:

$$\operatorname{sign}(\alpha) = \begin{cases} -1 & \text{if } \alpha < 0, \\ 0 & \text{if } \alpha = 0, \\ 1 & \text{if } \alpha > 0. \end{cases}$$

Given a family of polynomials $\mathcal{F} \subset \mathbf{R}[x_1, \ldots, x_k]$, a *sign condition* on $\mathcal{F}$ is an element τ of $\{-1, 0, 1\}^{\mathcal{F}}$. We use the notation

$$\operatorname{sign}(\mathcal{F}) = \tau$$

to mean

$$\bigwedge_{Q \in \mathcal{F}} (\operatorname{sign}(Q) = \tau(Q)) .$$

The *realization* of a sign condition τ on $\mathcal{F}$ is defined as

$$\operatorname{Real}(\tau, \mathbf{R}) = \{v \in \mathbf{R}^k \mid \operatorname{sign}(\mathcal{F}(v)) = \tau\}.$$

If $\operatorname{Real}(\tau, \mathbf{R}) \neq \emptyset$, we say that τ is *realizable*. Finally, we note by $\operatorname{SIGN}(\mathcal{F})$ the set of realizable sign conditions on $\mathcal{F}$.

For $p \in \mathbb{Z}$, $p \geq 0$, we denote by $\operatorname{bit}(p)$ the number of binary digits needed to represent p. This is to say

$$\operatorname{bit}(p) = \begin{cases} 1 & \text{if} \quad p = 0, \\ k & \text{if} \quad p \geq 1 \text{ and } 2^{k-1} \leq p < 2^k \text{ with } k \in \mathbb{Z}. \end{cases}$$

Please cite this article in press as: D. Perrucci, M.-F. Roy, Elementary recursive quantifier elimination based on Thom encoding and sign determination, Ann. Pure Appl. Logic (2017), http://dx.doi.org/10.1016/j.apal.2017.03.001