Elementary recursive quantifier elimination based on Thom encoding and sign determination

Daniel Perrucci[♭*] Marie-Françoise Roy[♯]

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

February 21, 2017

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.

Keywords: Quantifier Elimination, Real Closed Fields, Thom Encoding, Sign Determination.

AMS subject classifications: 14P10, 03C10.

1 Introduction

The first proofs of quantifier elimination for real closed fields by Tarski, Seidenberg, Cohen or Hörmander ([21, 22, 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 [3, Chapter 11]).

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

*Partially supported by the Argentinian grants PIP 2014-2016 11220130100527CO CONICET and UBACYT 20020120100133.

point method also gives a quantifier elimination algorithm which is doubly exponential in the number of blocks ([13, 14, 15, 20, 2, 3]).

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 o algebraic identities with elementary recursive degree bounds for the Positivstellensatz and Hilbert 17'th 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 [21], as presented in [3, 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

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

Let $\mathbf{D} \subset \mathbf{R}$ be a subring. In this paper, given a finite family of polynomials $\mathcal{F} \subset \mathbf{D}[x_1, \dots, x_k]$, we will construct for $1 \le i \le k-1$ a new explicit family of polynomials $\mathrm{Elim}_i(\mathcal{F}) \subset \mathbf{D}[x_1, \dots, x_i]$ which is suitable for quantifier elimination on first order formulas with atoms defined by polynomials in $\mathcal{F}$.

For organization matters, the definition of the family $\mathrm{Elim}_i(\mathcal{F})$ is posponed to Definition 27 in Section 4, and we include below our main result, which is Theorem 1. This theorem also states *complexity* bounds for the quantifier elimination method we present. Roughly speaking, the complexity is the number of operations in $\mathbf{D}$ that the computation takes; this concept will be further explained in Section 2.

Theorem 1 *Let $\mathcal{F} \subset \mathbf{D}[x_1, \dots, x_k]$ be a finite family of polynomials. Given a first order formula of type*

$$\mathrm{Qu}_{i+1} x_{i+1} \dots \mathrm{Qu}_k x_k \, \Phi(x_1, \dots, x_k)$$

with $1 \le i \le k-1$, $\mathrm{Qu}_h \in \{\forall, \exists\}$ for $i+1 \le h \le k$ and $\Phi(x_1, \dots, x_k)$ a quantifier free formula with atoms defined by polynomials in $\mathcal{F}$, there exists an equivalent quantifier free formula

$$\Psi(x_1, \dots, x_i)$$

with atoms in $\mathrm{Elim}_i(\mathcal{F})$. More precisely, there exists $T_\Phi \subset \mathrm{SIGN}(\mathrm{Elim}_i(\mathcal{F}))$ so that

$$\Psi(x_1, \dots, x_i) \quad = \bigvee_{\tau \in T_\Phi} (\mathrm{sign}(\mathrm{Elim}_i(\mathcal{F})) = \tau)\,.$$

If $\mathcal{F} \subset \mathbf{D}[x_1, \dots, x_k]$ is formed by s polynomials of degree bounded by d, then

$$\#\mathrm{Elim}_i(\mathcal{F}) \le s^{2^{k-i}} \max\{2, d\}^{(16^{k-i}-1)\mathrm{bit}(d)},$$

the degree of the polynomials in $\mathrm{Elim}_i(\mathcal{F})$ is bounded by

$$4^{\frac{4^{k-i}-1}{3}} d^{4^{k-i}},$$

and the complexity of computing the quantifier free formula Ψ is

$$O\Big(s^{2^k} \max\{2, d\}^{\mathrm{bit}(d)(16^k + (k-1)4^{k+1})}\Big)$$

operations in $\mathbf{D}$.

This paper is organized as follows. In Section 2 we state some preliminaries on complexity, Thom encodings, Tarski queries and Sign determination. In Section 3, we develop the main step of our construction, which is the elimination of one variable. Finally, in Section 4, we prove Theorem 1.

2 Preliminaries

2.1 Complexity

The computations we consider in this paper perform arithmetic operations in a subring $\mathbf{D}$ of a real closed field $\mathbf{R}$. The notion of *complexity* of a computation we consider is the number of arithmetic operations in $\mathbf{D}$ done during the described procedure. We consider that sign evaluation in $\mathbf{D}$ is cost free. We also consider that accessing, reading and writing pre-computed objects is cost free. For instance, we can access at any moment for free to any specific coefficient of a multivariate polynomial or any specific entry of a matrix. Also, we do not consider the cost of doing arithmetic operations between auxiliar numerical quantities (such as cardinalities of sets). In short, we focus on the operations in $\mathbf{D}$, which is the natural ambient for our input.

For the complexity of basic algorithms for polynomial operations we refer to [3, Chapter 8]. Also, we use Berkowitz Algorithm [5] as a division free algorithm to compute the determinant of a $p \times p$ matrix with entries in a commutative ring $\mathbf{A}$, within $O(p^4)$ operations in $\mathbf{A}$.

2.2 Thom encodings

We recall now the Thom encoding of real algebraic numbers [11] and explain its main properties. We refer to [3, Section 2.1] for classical proofs and to [18, Section 6.1] for proofs based on algebraic identities coming from Mixed Taylor Formulas.

Definition 2 *Let $P(y) = \sum_{0 \le h \le p} \gamma_h y^h \in \mathbf{R}[y]$ with $p \ge 1$ and $\gamma_p \ne 0$. We denote $\mathrm{Der}(P)$ the list formed by P and the first $p-1$ derivatives of P.*

Given a real root θ of P, the Thom encoding *of θ with respect to P is the list of signs of $\mathrm{Der}(P')$ evaluated at θ.*

Every real root of P is uniquely determined by its Thom encoding with respect to P; in the sense that two different real roots can not have the same Thom encoding.

For convenience we identify sign conditions on $\mathrm{Der}(P')$ (resp. $\mathrm{Der}(P)$), which are by definition elements in $\{1, 0, -1\}^{\mathrm{Der}(P')}$ (resp. $\{1, 0, -1\}^{\mathrm{Der}(P)}$), with elements in $\{-1, 0, 1\}^{\{1,\dots,p-1\}}$ (resp. $\{-1, 0, 1\}^{\{0,\dots,p-1\}}$). By convention, for any sign condition η on $\mathrm{Der}(P')$ or $\mathrm{Der}(P)$ we extend its definition with $\eta(p) = \mathrm{sign}(\gamma_p)$.

It is clear that the multiplicity of a real root of P can be deduced from its Thom encoding. Also, Thom encodings can be used to order real numbers as follows.

Notation 3 *Let $P(y) = \sum_{0 \le h \le p} \gamma_h y^h \in \mathbf{R}[y]$ with $p \ge 1$ and $\gamma_p \ne 0$. For η_1, η_2 sign conditions on $\mathrm{Der}(P)$, we use the notation $\eta_1 \prec_P \eta_2$ to indicate that $\eta_1 \ne \eta_2$ and, if q is the biggest value of k such that $\eta_1(k) \ne \eta_2(k)$, then*

- *$\eta_1(q) < \eta_2(q)$ and $\eta_1(q+1) = 1$ or*

- $\eta_1(q) > \eta_2(q)$ *and* $\eta_1(q+1) = -1$.

We use the notation $\eta_1 \preceq_P \eta_2$ *to indicate that either* $\eta_1 = \eta_2$ *or* $\eta_1 \prec_P \eta_2$.

It is easy to see that $\preceq_P$ defines a partial order on $\{-1,0,1\}^{\mathrm{Der}(P)}$. In addition, $\preceq_P$ defines a total order on $\mathrm{SIGN}(\mathrm{Der}(P))$. Indeed, let $\theta_1, \theta_2 \in \mathbf{R}$, $\eta_1 = \mathrm{sign}(\mathrm{Der}(P)(\theta_1))$ and $\eta_2 = \mathrm{sign}(\mathrm{Der}(P)(\theta_2))$ with $\eta_1 \neq \eta_2$, and let q be as in Notation 3. Note that since $\eta_1(p) = \eta_2(p) = \mathrm{sign}(\gamma_p)$, then $q < p$. It is not possible that there exists k such that $q < k < p$ and $\eta_1(k) = \eta_2(k) = 0$; otherwise θ_1 and θ_2 would be roots of $P^{(k)}$ with the same Thom encoding with respect to this polynomial, and therefore $\theta_1 = \theta_2$, which is impossible since $\eta_1 \neq \eta_2$. In particular, we have then that either $\eta_1(q+1) = 1$ or $\eta_1(q+1) = -1$ and therefore it is possible to order η_1 and η_2 according to $\preceq_P$.

Proposition 4 *Let* $P(y) = \sum_{0 \le h \le p} \gamma_h y^h \in \mathbf{R}[y]$ *with* $p \ge 1$ *and* $\gamma_p \neq 0$ *and* $\theta_1, \theta_2 \in \mathbf{R}$. *If* $\mathrm{sign}(\mathrm{Der}(P)(\theta_1)) \prec_P \mathrm{sign}(\mathrm{Der}(P)(\theta_2))$ *then* $\theta_1 < \theta_2$.

2.3 Tarski queries

Let $P, Q \in \mathbf{R}[y]$ with $P \not\equiv 0$. The Tarski-query of Q for P is

$$\begin{aligned} \mathrm{TaQu}(Q;P) &= \sum_{\theta \in \mathbf{R} \,|\, P(\theta)=0} \mathrm{sign}(Q(\theta)) \\ &= \#\{\theta \in \mathbf{R} \mid P(\theta) = 0,\, Q(\theta) > 0\} - \#\{\theta \in \mathbf{R} \mid P(\theta) = 0,\, Q(\theta) < 0\}. \end{aligned}$$

There are several methods to compute the Tarski-query of Q for P. Here, we describe one which is well adapted to the parametric case.

Definition 5 (Hermite's Matrix) *Let* $P, Q \in \mathbf{R}[y]$ *with* $\deg P = p \ge 1$. *The Hermite's matrix* $\mathrm{Her}(P;Q) \in \mathbf{R}^{p \times p}$ *is the matrix defined for* $1 \le j_1, j_2 \le p$ *by*

$$\mathrm{Her}(P;Q)_{j_1,j_2} = \mathrm{Tra}(Q(y) y^{j_1+j_2-2})$$

where $\mathrm{Tra}(A(y))$ *is the trace of the linear mapping of multiplication by* $A(y) \in \mathbf{R}[y]$ *in the* $\mathbf{R}$*-vector space* $\mathbf{R}[y]/P(y)$.

Remark 6 *Let* $P(y) = \sum_{0 \le h \le p} \gamma_h y^h, Q = \sum_{0 \le h \le q} \gamma'_h y^h \in \mathbf{R}[y]$ *with* $p \ge 1$ *and* $\gamma_p \neq 0$. *For* $j \in \mathbb{N}$ *we denote by* $\mathrm{A}_{p,j} \in \mathbb{Z}[c_0, \dots, c_{p-1}]$ *the unique polynomial such that*

$$\mathrm{A}_{p,j}(s_p(y_1, \dots, y_p), \dots, s_1(y_1, \dots, y_p)) = \sum_{1 \le k \le p} y_k^j \in \mathbb{Z}[y_1, \dots, y_p],$$

where for $1 \le j \le p$, $s_j(y_1, \dots, y_p)$ *is the* j*-th elementary symmetric function evaluated in* $y_1, \dots, y_p$. *Note that* $\deg \mathrm{A}_{p,j} = j$ *(see [12, Proof of Theorem 3, Chapter 7]).*

Then we have that for $1 \le j_1, j_2 \le p$,

$$\mathrm{Her}(P;Q)_{j_1,j_2} = \sum_{0 \le h \le q} \gamma'_h \mathrm{A}_{p,h+j_1+j_2-2}\left((-1)^p \frac{\gamma_0}{\gamma_p}, \ldots, -\frac{\gamma_{p-1}}{\gamma_p}\right)$$

(see [3, Section 4.3]); therefore

$$\gamma_p^{q+2p-2}\mathrm{Her}(P;Q)_{j_1,j_2}$$

is a polynomial in the coefficients of P *and* Q *with degree* $q + 2p - 2$ *with respect to the coefficients of* P *and degree* 1 *with respect to the coefficients of* Q.

Theorem 7 (Hermite's Theory (1)) *Let* $P, Q \in \mathbf{R}[y]$ *with* $\deg P = p \ge 1$. *Then*

$$\mathrm{Si}(\mathrm{Her}(P;Q)) = \mathrm{TaQu}(Q;P)$$

where $\mathrm{Si}(\mathrm{Her}(P;Q))$ *is the signature of the symmetric matrix* $\mathrm{Her}(P;Q)$.

Proof: See [3, Theorem 4.58] or [18, Section 5.1] for a proof based on algebraic identities.
□

A nice property of the Hermite's matrix is that its signature can always be computed from the sign of its principal minors (property which is not extensive to general symmetric matrices, or even Hankel matrices, as shown for instance by the matrices $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, having same principal minors and different signatures).

Notation 8 *Let* $P, Q \in \mathbf{R}[y]$ *with* $\deg P = p \ge 1$. *For* $0 \le j \le p-1$, *we denote by* $\mathrm{hmi}_j(P;Q)$ *the* $(p-j)$*-th principal minor of* $\mathrm{Her}(P;Q)$. *We extend this definition with* $\mathrm{hmi}_p(P;Q) = 1$. *We denote by* $\mathrm{hmi}(P;Q)$ *the list*

$$[\mathrm{hmi}_0(P;Q), \ldots, \mathrm{hmi}_{p-1}(P;Q), 1] \subset \mathbf{R}.$$

We also consider the following notation.

Notation 9
- *For* $k \in \mathbb{N}, \varepsilon_k = (-1)^{k(k-1)/2}$.
- *Let* $h = h_0, \ldots, h_p$ *be a finite list in* $\mathbf{R}$ *such that* $h_p \neq 0$. *We denote by* $(d_0, \ldots, d_s)$ *the strictly decreasing sequence of natural numbers defined by* $\{d_0, \ldots, d_s\} = \{j \mid 0 \le j \le p,\ h_j \neq 0\}$. *We define*

$$\mathrm{PmV}(h) = \sum_{\substack{1 \le i \le s, \\ d_{i-1}-d_i \ odd}} \varepsilon_{d_{i-1}-d_i} \mathrm{sign}(h_{d_{i-1}}) \mathrm{sign}(h_{d_i}).$$

Note that in Notation 9 it is always the case that $d_0 = p$. Also, when all elements of h are non-zero, $\mathrm{PmV}(h)$ is the difference between the number of sign permanencies and the number of sign changes in $h_p, \ldots, h_0$.

Theorem 10 (Hermite's Theory (2)) *Let $P, Q \in \mathbf{R}[y]$ with $\deg P = p \geq 1$, Then*

$$\mathrm{Si}(\mathrm{Her}(P;Q)) = \mathrm{PmV}(\mathrm{hmi}(P;Q)).$$

Proof: See [3, Theorem 4.33, Proposition 4.55 and Lemma 9.26] or [18, Section 5.2] for a proof based on algebraic identities. □

2.4 Sign determination

Consider now $P \in \mathbf{R}[y]$ and $\mathcal{P} = P_1, \ldots, P_s$, a finite list of polynomials in $\mathbf{R}[y]$. Let σ be a sign condition on $\mathcal{P}$. The cardinality of

$$\{\theta \in \mathbf{R} \mid P(\theta) = 0, \, \mathrm{sign}(\mathcal{P}(\theta)) = \sigma\}$$

is denoted by $c(\sigma, \{\theta \in \mathbf{R} \mid P(\theta) = 0\})$ or simply by $c(\sigma)$ if the polynomial P is fixed and clear from the context. Note that if

$$\{\theta \in \mathbf{R} \mid P(\theta) = 0, \, \mathrm{sign}(\mathcal{P}(\theta)) = \sigma\} = \emptyset,$$

then $c(\sigma) = 0$.

The (univariate) *Sign Determination problem* is to determine $c(\sigma)$ for every sign condition σ on $\mathcal{P}$. It is a basic algorithmic problem for real numbers which has been studied extensively (see for example [21, 1, 6, 3]).

There is a very close relation between the sign determination problem and Tarski queries.

Proposition 11 *Let $P \in \mathbf{R}[y]$ with $\deg P = p \geq 1$ and $\mathcal{P} = P_1, \ldots, P_s$ a finite list of polynomials in $\mathbf{R}[y]$. The list of all Tarski-queries*

$$\left[\mathrm{TaQu}(Q;P), Q \in \left\{ \prod_{1 \leq h \leq s} P_h^{\alpha_h} \mid (\alpha_1, \ldots, \alpha_s) \in \{0,1,2\}^{\{1,\ldots,s\}}, \, \#\{h \mid \alpha_h \neq 0\} \leq \mathrm{bit}(p) \right\} \right]$$

determines the cardinality $c(\sigma)$ for every sign condition σ on $\mathcal{P}$ at the roots of P.

Proof: The sign determination procedure described in [3, Algorithm 10.11] proceeds in s steps as follows: for $i = 1, \ldots, s$, at step i, the cardinality $c(\sigma)$ for every sign condition σ on $P_1, \ldots, P_i$ is computed. In order to do so, at each step, first several Tarski queries $\mathrm{TaQu}(Q;P)$ are calculated, and then an invertible linear system with entries in $\mathbb{Z}$ is solved. By [3, Proposition 10.74], every polynomial Q such that $\mathrm{TaQu}(Q;P)$ is calculated along the execution of the algorithm, is a product of at most $\mathrm{bit}(p)$ of the polynomials $P_1, \ldots, P_s$

each of them raised to the power 1 or 2. Therefore, once all Tarski-queries $\mathrm{TaQu}(Q;P)$ with

$$Q \in \Big\{ \prod_{1\le h\le s} P_h^{\alpha_h} \mid (\alpha_1,\dots,\alpha_s) \in \{0,1,2\}^{\{1,\dots,s\}},\ \#\{h \mid \alpha_h \neq 0\} \le \mathrm{bit}(p) \Big\}$$

are known, the output of the algorithm, which is the cardinality $c(\sigma)$ for every sign condition σ on $P_1,\dots,P_s$ at the zeroes of P, is determined. □

As it was said before, in this paper we do not consider the cost of doing arithmetic operations between auxiliar numerical quantities (such as cardinalities of sets). Nevertheless, we refer to [4, Section 10.3] for details on specific methods to solve the integer linear systems involved in the sign determination algorithm cited in the proof of Proposition 11, as well as bounds on its bit complexity.

Remark 12 *Given $P, Q \in \mathbf{R}[y]$ with $\deg P = p \ge 1$, solving the sign determination problem for the list $\mathrm{Der}(P')$ (see Definition 2) means to compute the Thom encodings of the real roots of P. Solving the sign determination problem for the list $[\mathrm{Der}(P'), Q]$ (the list $\mathrm{Der}(P')$ extended with the polynomial Q) means to additionally compute the sign of Q at each of the real roots of P, encoded by their Thom encoding.*

In view of Proposition 11 and Remark 12 we consider the following Notation and Definition.

Notation 13 *Let $\mathbf{A}$ be a commutative ring, $P, Q \in \mathbf{A}[y]$ with $\deg P = p \ge 1$ and $j \in \mathbb{N}$. We define*

$$\begin{aligned}
\mathrm{PDer}_j(P) &= \Big\{ \prod_{1\le h\le p-1} (P^{(h)})^{\alpha_h} \mid \alpha \in \{0,1,2\}^{\{1,\dots,p-1\}},\ \#\{h \mid \alpha_h \neq 0\} \le j \Big\} \subset \mathbf{A}[y], \\
\mathrm{PDer}_j(P;Q) &= \{AB \mid A \in \mathrm{PDer}_j(P),\ B \in \{Q, Q^2\}\} \subset \mathbf{A}[y].
\end{aligned}$$

Definition 14 *Let $P, Q \in \mathbf{R}[y]$ with $\deg P = p \ge 1$. We define*

$$\begin{aligned}
\mathrm{thelim}(P) &= \bigcup_{A \in \mathrm{PDer}_{\mathrm{bit}(p)}(P)} \mathrm{hmi}(P;A) \subset \mathbf{R}, \\
\mathrm{thelim}(P;Q) &= \bigcup_{A \in \mathrm{PDer}_{\mathrm{bit}(p)-1}(P;Q)} \mathrm{hmi}(P;A) \subset \mathbf{R}.
\end{aligned}$$

Corollary 15 *Let $P, Q \in \mathbf{R}[y]$ with $\deg P = p \ge 1$. The list of signs of $\mathrm{thelim}(P)$ and $\mathrm{thelim}(P;Q)$ determines the Thom encoding of the real roots of P and the sign of Q at each of these roots.*

Proof: Consider $\mathcal{P} = P_1,\dots,P_p = [\mathrm{Der}(P'), Q]$; we have that

$$\mathrm{PDer}_{\mathrm{bit}(p)}(P) \ \cup\ \mathrm{PDer}_{\mathrm{bit}(p)-1}(P;Q) =$$
$$= \Big\{ \prod_{1\le h\le p} P_h^{\alpha_h} \mid \alpha \in \{0,1,2\}^{\{1,\dots,s\}},\ \#\{h \mid \alpha_h \neq 0\} \le \mathrm{bit}(p) \Big\}.$$

The result follows then from Theorem 7, Theorem 10 and Proposition 11. □

Note that the results we present here are not optimal in the number of Tarski queries to be considered, but they are instead well adapted to the parametric case. For a more refined sign determination process see [3, Chapter 10].

3 Eliminating one variable

In this section, we consider a set of variables $u = (u_1, \dots, u_\ell)$ which we take as parameters, and a single variable y which we take as the main variable. In order to study the elimination of the variable y, we first review sign determination in a parametric context.

Through this section, derivative, degree and leading coefficient are taken with respect to y. For $P \in \mathbf{D}[u, y]$ we denote by $\deg P$ and $\deg_u P$ its degree with respect to y and to u respectively. For a finite family $\mathcal{F} \subset \mathbf{D}[u, y]$, we denote by $\deg \mathcal{F}$ and $\deg_u \mathcal{F}$ the maximum of $\deg P$ and $\deg_u P$ for $P \in \mathcal{F}$ respectively.

3.1 Parametric Thom encoding and sign determination

Given $P, Q \in \mathbf{D}[u, y]$, we want to describe polynomial conditions on the parameters fixing the Thom encoding of the real roots of P and the sign of Q at each of them. The first problem to consider in this parametric context is that some specializations of the parameters may cause a drop in the degree of P, which is particularly important since this degree fixes the size of the Hermite's matrix of P and Q. Note that, on the other hand, specializations of the parameters causing a drop in the degree of Q do not cause any problem.

Definition 16 *Let* $P(u, y) = \sum_{0 \le h \le p} c_h(u) y^h \in \mathbf{D}[u, y]$ *with* $p \ge 0$ *and* $c_p(u) \not\equiv 0$.

For $-1 \le j \le p$*, the* truncation of P at j *is*

$$\mathrm{Tru}_j(P) = c_j(u) y^j + \dots + c_0(u) \in \mathbf{D}[u, y].$$

The set of truncations of P *is the finite subset of* $\mathbf{D}[u, y]$ *defined inductively on the degree of* P *by* $\mathrm{Tru}(0) = \emptyset$ *and*

$$\mathrm{Tru}(P) = \begin{cases} \{P\} & \textit{if } \mathrm{lc}(P) \in \mathbf{D} \\ \{P\} \cup \mathrm{Tru}(\mathrm{Tru}_{p-1}(P)) & \textit{otherwise.} \end{cases}$$

The set of relevant coefficients of P *is the finite subset of* $\mathbf{D}[u]$ *defined inductively on the degree of* P *by* $\mathrm{RC}(0) = \emptyset$ *and*

$$\mathrm{RC}(P) = \begin{cases} \emptyset & \textit{if } \mathrm{lc}(P) \in \mathbf{D}, \\ \{\mathrm{lc}(P)\} \cup \mathrm{RC}(\mathrm{Tru}_{p-1}(P)) & \textit{otherwise.} \end{cases}$$

The idea behind Definition 16 is that the degree of P is fixed once the sign of the relevant coefficients of P is known.

Another problem arising in the parametric context is that we want to eliminate the variable y keeping conditions on the parameters u defined by polynomials rather than rational functions. Therefore, we consider the following definition.

Notation 17 *Let* $P(u, y) = \sum_{0\le h\le p} c_h(u)y^h, Q = \sum_{0\le h\le q} c'_h(u)y^h \in \mathbf{D}[u, y]$ *with* $p \ge 1$ *and* $c_p(u) \not\equiv 0$*. As in Definition 5 we consider the matrix* $\mathrm{Her}(P; Q) \in \mathbf{D}(u)^{p\times p}$*. Taking into account Remark 6 and following Notation 8, for* $0 \le j \le p - 1$*, we denote by*

$$\mathrm{HMi}_j(P; Q) = c_p(u)^{(p-j)(q+2p-2)}\mathrm{hmi}_j(P; Q) \in \mathbf{D}[u].$$

We denote by $\mathrm{HMi}(P; Q)$ *the list*

$$[\mathrm{HMi}_0(P; Q), \ldots, \mathrm{HMi}_{p-1}(P; Q)] \subset \mathbf{D}[u].$$

Lemma 18

$$\deg_u \mathrm{HMi}(P; Q) \le p\Big((q + 2p - 2) \deg_u P + \deg_u Q\Big).$$

Moreover, given the matrix $c_p(u)^{q+2p-2}\mathrm{Her}(P; Q)$*, the computation of* $\mathrm{HMi}(P; Q)$ *can be done in* $O(p^4)$ *operations in* $\mathbf{D}[u]$*, each of them between polynomials of degree bounded by* $p((q + 2p - 2) \deg_u P + \deg_u Q)$*.*

Proof: The degree bound for $\mathrm{HMi}(P; Q)$ follows from the fact that $\mathrm{HMi}(P; Q)$ is the list of principal minors of the matrix $c_p(u)^{q+2p-2}\mathrm{Her}(P; Q) \in \mathbf{D}[u]^{p\times p}$ and the degree bound from Remark 6.

For the bound on the number of operations in $\mathbf{D}[u]$ and the degree bound in intermediate computations, we simply use Berkowitz Algorithm (see [5]), taking into account that along the execution of this division free algorithm for the computation of the determinant of a given matrix, all its principal minors are recursively computed. □

Now we consider the following definitions.

Definition 19 *Let* $P, Q \in \mathbf{D}[u, y]$ *with* $\deg P = p$*. If* $p \ge 1$*, following Notation 13, we define*

$$\begin{aligned}\mathrm{ThElim}(P) &= \bigcup_{A\in\mathrm{PDer}_{\mathrm{bit}(p)}(P)} \mathrm{HMi}(P; A) \subset \mathbf{D}[u],\\ \mathrm{ThElim}(P; Q) &= \bigcup_{A\in\mathrm{PDer}_{\mathrm{bit}(p)-1}(P;Q)} \mathrm{HMi}(P; A) \subset \mathbf{D}[u].\end{aligned}$$

If $p = 0$ *(i.e.,* $P \in \mathbf{D}[u]$*), we define* $\mathrm{ThElim}(P)$ *and* $\mathrm{ThElim}(P; Q)$ *as the empty lists.*

Finally, we define

$$\mathrm{Elim}(P; Q) = \mathrm{RC}(P) \cup \bigcup_{T\in\mathrm{Tru}(P)} \Big(\mathrm{ThElim}(T) \cup \mathrm{ThElim}(T; Q)\Big).$$

We can prove now the following result.

Proposition 20 *Let $P, Q \in \mathbf{D}[u, y]$ with $P \not\equiv 0$. For every $\upsilon \in \mathbf{R}^\ell$, the realizable sign condition on the family*

$$\mathrm{Elim}(P; Q) \subset \mathbf{D}[u]$$

satisfied by υ determines the fact that $P(\upsilon, y) \equiv 0$ or $P(\upsilon, y) \not\equiv 0$, and, if $P(\upsilon, y) \not\equiv 0$, it also determines the Thom encoding of the real roots of $P(\upsilon, y)$ and the sign of $Q(\upsilon, y)$ at each of these roots.

Proof: Let $p = \deg P$. It is clear that the fact that $P(\upsilon, y) \equiv 0$ or $P(\upsilon, y) \not\equiv 0$ is determined by the sign condition on $\mathrm{RC}(P)$ satisfied by υ. From now we suppose that $P(\upsilon, y) \not\equiv 0$. Again, it is also clear that the degree of $P(\upsilon, y) \leq p$ is also determined by the sign condition on $\mathrm{RC}(P)$ satisfied by υ; we call p' this degree. If $p' = 0$ then $P(\upsilon, y)$ has no real root; so from now we suppose $p' \geq 1$ and we only keep the information given by the sign condition satisfied by υ on

$$\mathrm{ThElim}(T) \cup \mathrm{ThElim}(T; Q)$$

for

$$T = \mathrm{Tru}_{p'}(P) \in \mathrm{Tru}(P).$$

Now, for $0 \leq j \leq p' - 1$ and $A \in \mathrm{PDer}_{\mathrm{bit}(p')}(T)$ or $A \in \mathrm{PDer}_{\mathrm{bit}(p')-1}(T; Q)$ we have that

$$\mathrm{HMi}_j(T; A) = c_{p'}(u)^{(p'-j)(q+2p'-2)} \mathrm{hmi}_j(T; A).$$

It is the case that either $c_{p'}(u) \in \mathbf{D}$ or $c_{p'}(u) \in \mathrm{RC}(P)$, but in any situation the sign of $c_{p'}(\upsilon)$ is known, and then the sign of every element in $\mathrm{hmi}_j(T(\upsilon, y); A(\upsilon, y))$ is also known.

Finally, by Corollary 15 this is enough to determine the Thom encoding of the real roots of $T(\upsilon, y)$ and the sign of $Q(\upsilon, y)$ at each of these roots. □

Remark 21 *The proof of correctness of Proposition 20 is based on the determination of Thom encoding of real roots and the sign of another polynomial at these roots; thus, this proof is entirely based on algebra. For instance, there is no need of sample points meeting every connected component of the realization of sign conditions.*

Remark 22 *Let $P, Q \in \mathbf{D}[u, y]$ with $\deg P = p \geq 1$ and $\deg Q = q$. Following Notation 13, there are*

$$\sum_{0 \leq h \leq j} \binom{p-1}{h} 2^h \leq 2p^j$$

elements in $\mathrm{PDer}_j(P)$. Therefore, there are at most $2p^{\mathrm{bit}(p)+1}$ elements in $\mathrm{ThElim}(P)$ and by Lemma 18 their degree in $u = (u_1, \dots, u_\ell)$ are bounded by

$$p\Big((2(p-1)\mathrm{bit}(p) + 2p - 2) \deg_u P + 2\mathrm{bit}(p) \deg_u P\Big) \leq 2p^2(\mathrm{bit}(p) + 1) \deg_u P.$$

Similarly, there are at most $4p^{\mathrm{bit}(p)}$ elements in $\mathrm{ThElim}(P; Q)$ and their degree in $u = (u_1, \dots, u_\ell)$ are bounded by

$$\begin{aligned} & p\Big((2(p-1)(\mathrm{bit}(p) - 1) + 2q + 2p - 2) \deg_u P + 2(\mathrm{bit}(p) - 1) \deg_u P + 2 \deg_u Q\Big) = \\ = \quad & p\Big((2p\mathrm{bit}(p) + 2q - 2) \deg_u P + 2 \deg_u Q\Big). \end{aligned}$$

3.2 Fixing the realizable sign conditions on a family

In order to fix the realizable sign conditions on a parametric family of univariate polynomials, we consider the following definition.

Definition 23 *Let $\mathcal{F}$ be a finite family of polynomials in $\mathbf{D}[u,y]$. We denote by*

$$\mathrm{Der}(\mathcal{F}) = \bigcup_{P \in \mathcal{F} \setminus \mathbf{D}[u]} \mathrm{Der}(P) \subset \mathbf{D}[u,y].$$

We define

$$\mathrm{Elim}(\mathcal{F}) = \bigcup_{P \in \mathcal{F} \setminus \{0\}} \left(\mathrm{RC}(P) \cup \bigcup_{T \in \mathrm{Tru}(P)} \left(\mathrm{ThElim}(T) \cup \bigcup_{Q \in \mathrm{Der}(\mathcal{F} \setminus \{P\})} \mathrm{ThElim}(T;Q) \right) \right) \subset \mathbf{D}[u].$$

We prove now the following result.

Proposition 24 *Let $\mathcal{F}$ be a finite family of polynomials in $\mathbf{D}[u,y]$. For every $\upsilon \in \mathbf{R}^{\ell}$, the realizable sign condition on the family*

$$\mathrm{Elim}(\mathcal{F}) \subset \mathbf{D}[u]$$

satisfied by υ determines the list $\mathrm{SIGN}(\mathcal{F}(\upsilon,y))$.

Proof: By Proposition 20, the sign condition on $\mathrm{Elim}(\mathcal{F})$ satisfied by υ determines for every $P \in \mathcal{F} \setminus \{0\}$ the fact that $P(\upsilon,y) \equiv 0$ or $P(\upsilon,y) \not\equiv 0$, and, if $P(\upsilon,y) \not\equiv 0$, it also determines the Thom encoding of the real roots of $P(\upsilon,y)$ and, for every $Q \in \mathrm{Der}(\mathcal{F}\setminus\{P\})$, the sign of $Q(\upsilon,y)$ at each of these real roots.

Now, for each $P \in \mathcal{F}$ with $P(\upsilon,y) \not\equiv 0$, since the Thom encoding of the real roots of $P(\upsilon,y)$ is known and the sign of the leading coefficient of $P(\upsilon,y)$ is also known, we can deduce the multiplicity of each real root and, by Proposition 4, also the order between them. All this information is enough to determine the sign of $P(\upsilon,y)$ on every (bounded or unbounded) interval of the real line defined by the real roots of $P(\upsilon,y)$.

Finally, in order to determine the list $\mathrm{SIGN}(\mathcal{F}(\upsilon,y))$ we only need to know how to order the real roots coming from different polynomials $P_1(\upsilon,y)$ and $P_2(\upsilon,y)$ in $\mathcal{F}(\upsilon,y)$. Once again by Proposition 20, the signs of $\mathrm{Der}(P_1(\upsilon,y))$ at all the real roots of $P_1(\upsilon,y)$ and $P_2(\upsilon,y)$ is known. The only detail to take into account is that if it happens that $\deg P_1(u,y) = \deg P_1(\upsilon,y) = p_1$ we also need to know the sign of $P_1(\upsilon,y)^{(p_1)}$ at all the real roots of $P_1(\upsilon,y)$ and $P_2(\upsilon,y)$ to be able to order them (and by definition, $P_1(u,y)^{(p_1)} \notin \mathrm{Der}(P_1(u,y))$). Nevertheless, this is indeed the case since the leading coefficient $c_{p_1}(u)$ of $P_1(u,y)$ is either in $\mathbf{D}$ or in $\mathrm{RC}(P_1)$ and in any situation the sign of $c_{p_1}(\upsilon)$ is known. Finally we can order the real roots of $P_1(\upsilon,y)$ and $P_2(\upsilon,y)$ using once again Proposition 4. □

Remark 25 *As in Proposition 20 (see Remark 21), the proof of correctness of Proposition 24 is entirely based on algebra. No geometric concept is needed.*

Lemma 26 *Let $\mathcal{F}$ be a family of s polynomials in $\mathbf{D}[u,y]$ with $\deg \mathcal{F} = p$. If $p=0$ (i.e., $\mathcal{F} \subset \mathbf{D}[u]$) then $\mathrm{Elim}(\mathcal{F}) = \mathcal{F} \setminus \mathbf{D}$. If $p \geq 1$, there are at most*

$$4s^2 p^{\mathrm{bit}(p)+2}$$

elements in $\mathrm{Elim}(\mathcal{F})$, their degree in $u = (u_1, \ldots, u_\ell)$ are bounded by

$$4p^3 \deg_u \mathcal{F}$$

and the complexity of computing $\mathrm{Elim}(\mathcal{F})$ is

$$O(s^2 p^{\mathrm{bit}(p)+5})$$

operations in $\mathbf{D}[u]$, each of them between polynomials of degree at most $4p^3 \deg_u \mathcal{F}$.

Proof: If $p = 0$ there is nothing to prove, so we suppose $p \geq 1$. By Remark 22, there are at most

$$s\left(p+1+p\left(2p^{\mathrm{bit}(p)+1} + (s-1)4p^{\mathrm{bit}(p)+1}\right)\right) \leq 4s^2 p^{\mathrm{bit}(p)+2}$$

elements in $\mathrm{Elim}(\mathcal{F})$ and their degree in $u = (u_1, \ldots, u_\ell)$ are bounded by

$$2p^2(\mathrm{bit}(p)+1)\deg_u \mathcal{F} \leq 4p^3 \deg_u \mathcal{F}.$$

The computation of $\mathrm{RC}(P)$ for every $P \in \mathcal{F} \setminus \{0\}$ is cost free. There are at most sp polynomials $T \in \mathrm{Tru}(P)$ for some $P \in \mathcal{F}\setminus\{0\}$ to consider, and for each of these polynomials T we have to compute

$$\mathrm{ThElim}(T) \cup \bigcup_{Q \in \mathrm{Der}(\mathcal{F}\setminus\{P\})} \mathrm{ThElim}(T;Q)$$

(this is so since if $\deg T = 0$ then $\mathrm{ThElim}(T)$ and $\mathrm{ThElim}(T;Q)$ are the empty lists).

From now, we consider a fixed $T(u,y) = \sum_{0 \leq h \leq p'} c_h(u) y^h \in \mathbf{D}[u,y]$, with $1 \leq p' \leq p$ and $c_{p'}(u) \not\equiv 0$. We consider also the basis $\mathcal{B} = \{1, y, \ldots, y^{p'-1}\}$ of the $\mathbf{R}(u)$-vector space $V = \mathbf{R}(u)[y]/T(u,y)$. For $h \in \mathbb{N}$, we define $M_h \in \mathbf{D}[u]^{p' \times p'}$ as the matrix in basis $\mathcal{B}$ of the linear mapping of multiplication by $(c_{p'}(u)y)^h$ in V. It is clear that

$$M_1 = \begin{pmatrix} 0 & \cdots & \cdots & 0 & -c_0(u) \\ c_{p'}(u) & \ddots & & \vdots & -c_1(u) \\ 0 & c_{p'}(u) & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & c_{p'}(u) & -c_{p'-1}(u) \end{pmatrix}$$

and also that $\deg_u M_h \leq h \deg_u P$.

We need to compute $\mathrm{HMi}(T;A)$ for a number of polynomials $A \in \mathbf{D}[u,y]$ with $\deg A \leq 2p\mathrm{bit}(p)$. If $A = \sum_{0 \leq h \leq a} c'_h(u) y^h$, then for $0 \leq j \leq p'-1$, $\mathrm{HMi}_j(T;A)$ is the $(p'-j)$-th principal minor of the matrix

$$c_{p'}(u)^{a+2p'-2}\mathrm{Her}(T;A),$$

and for $1 \leq j_1, j_2 \leq p'$ we have that

$$c_{p'}(u)^{a+2p'-2}\mathrm{Her}(T;A)_{j_1,j_2} = \sum_{0\leq h\leq a} c'_h(u)c_{p'}(u)^{a+2p'-h-j_1-j_2}\mathrm{Tra}(M_{h+j_1+j_2-2}). \quad (1)$$

We describe first the part of the computation which depends on T but not on A, then we describe the computation of all the polynomials A we need to consider, and finally we describe the part of the computation which depends on both T and A.

First Step: Our aim is to compute $\mathrm{Tra}(M_h)$ for $0 \leq h \leq 2p\mathrm{bit}(p) + 2p - 2$.

The matrices M_0 and M_1 are already known and computing their traces is cost free. We compute then $\mathrm{Tra}(M_h)$ for $2 \leq h \leq p' - 1$ and then we proceed using a recursive formula to compute all the remaining required traces.

Successively computing

$$M_2 = M_1 \cdot M_1,\ \ldots\ , M_{h+1} = M_1 \cdot M_h,\ \ldots\ M_{p'-1} = M_1 \cdot M_{p'-2},$$

and taking into account that M_1 has at most 2 non-zero entries per row, we can compute M_h for $2 \leq h \leq p'-1$ within $O(p^3)$ operations in $\mathbf{D}[u]$, and the traces of all these matrices within $O(p^2)$ operations in $\mathbf{D}[u]$.

For $h \geq p'$ we have that

$$\mathrm{Tra}(M_h) = -\sum_{1\leq i\leq p'} c_{p'-i}(u)c_{p'}(u)^{i-1}\mathrm{Tra}(M_{h-i}).$$

We compute $c_{p'}(u)^{i-1}$ for $1 \leq i \leq p'$ within $O(p)$ operations in $\mathbf{D}[u]$, then we successively compute $\mathrm{Tra}(M_h)$ for $p' \leq h \leq 2p\mathrm{bit}(p) + 2p - 2$ within $O(p^2\mathrm{bit}(p))$ operations in $\mathbf{D}[u]$.

Finally, the whole step can be done within $O(p^3)$ operations in $\mathbf{D}[u]$. Since for $h \in \mathbb{N}$ we have that $\deg_u M_h \leq h \deg_u P$, these operations are between polynomials of degree at most $(2p\mathrm{bit}(p) + 2p - 2) \deg_u \mathcal{F} \leq 4p^3 \deg_u \mathcal{F}$.

Second Step: Now we proceed to the computation of all the polynomials A.

Following Remark 22 there are at most $2p^{\mathrm{bit}(p)}$ polynomials $A \in \mathrm{PDer}_{\mathrm{bit}(p')}(T)$. We compute all of them starting from the constant polynomial 1 and then multiplying each time a derivative of T, of degree at most p, and a previously computed polynomial in $\mathrm{PDer}_{\mathrm{bit}(p')}(T)$, of degree at most $(2\mathrm{bit}(p)-1)p$. In this way, we compute all the polynomials in $\mathrm{PDer}_{\mathrm{bit}(p')}(T)$ within $O(p^{\mathrm{bit}(p)+3})$ operations in $\mathbf{D}[u]$.

Similarly, for each polynomial $Q \in \mathrm{Der}(\mathcal{F} \setminus \{P\})$ there are at most $4p^{\mathrm{bit}(p)-1}$ polynomials $A \in \mathrm{PDer}_{\mathrm{bit}(p')-1}(T;Q)$ and we compute all of them multiplying each time Q by a previously computed polynomial in $\mathrm{PDer}_{\mathrm{bit}(p')-1}(T) \cup \mathrm{PDer}_{\mathrm{bit}(p')-1}(T,Q)$, of degree at most $(2\mathrm{bit}(p) - 1)p$. In this way, we compute all the polynomials in $\mathrm{PDer}_{\mathrm{bit}(p')-1}(T;Q)$ within $O(p^{\mathrm{bit}(p)+2})$ operations in $\mathbf{D}[u]$.

Finally, since there are at most $(s - 1)p$ polynomials $Q \in \mathrm{Der}(\mathcal{F} \setminus \{P\})$, the whole step can be done within $O(sp^{\mathrm{bit}(p)+3})$ operations in $\mathbf{D}[u]$. It is clear that all these operations are between polynomials of degree at most $2p\mathrm{bit}(p) \deg_u \mathcal{F} \leq 4p^3 \deg_u \mathcal{F}$.

Third Step: We have to compute $\mathrm{HMi}(T;A)$ for every $A \in \mathrm{PDer}_{\mathrm{bit}(p')}(T)$ and also, for every $Q \in \mathrm{Der}(\mathcal{F} \setminus \{P\})$ and every $A \in \mathrm{PDer}_{\mathrm{bit}(p')-1}(T;Q)$. By Remark 22, there are then $O(sp^{\mathrm{bit}(p)})$ polynomials A to consider.

For a fixed $A = \sum_{0 \le h \le a} c'_h(u) y^h$ with $a \le 2p\mathrm{bit}(p)$, in order to compute he matrix $c_{p'}(u)^{a+2p'-2}\mathrm{Her}(T;A)$, we first compute $c_{p'}(u)^i$ for $1 \le i \le a+2p'-2$ within $O(p\mathrm{bit}(p))$ operations in $\mathbf{D}[u]$. Then, using equation (1), we can compute each entry of this matrix within $O(p)$ operations since all the required traces have already been computed. Note that since $c_{p'}(u)^{a+2p'-2}\mathrm{Her}(T;A)$ is a Hankel matrix, we only need to compute $2p'-1$ entries. Therefore, the computation of $c_{p'}(u)^{a+2p'-2}\mathrm{Her}(T;A)$ can be done within $O(p^2)$ operations in $\mathbf{D}[u]$, each of them between polynomials of degree at most $(2p\mathrm{bit}(p)+2p-1)\deg_u \mathcal{F}$.

The last part of the step is to compute the principal minors of $c_{p'}(u)^{a+2p'-2}\mathrm{Her}(T;A)$. By Lemma 18 this can be done within $O(p^4)$ operations in $\mathbf{D}[u]$, each of them between polynomials of degree at most $p(2p\mathrm{bit}(p)+2p-1)\deg_u \mathcal{F}$.

Finally, the whole step can be done within $O(sp^{\mathrm{bit}(p)+4})$ operations in $\mathbf{D}[u]$, each of them between polynomials of degree at most $p(2p\mathrm{bit}(p)+2p-1)\deg_u \mathcal{F} \le 4p^3 \deg_u \mathcal{F}$. □

4 Main result

Let $\mathcal{F}$ be a finite family in $\mathbf{D}[x_1, \dots, x_k]$. In this section we define the families $\mathrm{Elim}_i(\mathcal{F})$ for $0 \le i \le k-1$ and we prove Theorem 1.

The main idea is to repeatedly use the construction of Elim as in Definition 23, where for each $i = k-1, \dots, 0$ (taken in this order), the vector $u = (x_1, \dots, x_i)$ will play the role of the set of parameters and $y = x_{i+1}$ will play the role of the main variable.

Definition 27 *We define* $\mathrm{Elim}_k(\mathcal{F})$ *as* $\mathcal{F}$*. Then, for* $i = k-1, \dots, 0$*, we define inductively*

$$\mathrm{Elim}_i(\mathcal{F}) = \mathrm{Elim}(\mathrm{Elim}_{i+1}(\mathcal{F})) \subset \mathbf{D}[x_1, \dots, x_i].$$

Proof of Theorem 1: The proof is based on a cylindrical structure on the realizable sign conditions described by the families $\mathrm{Elim}_i(\mathcal{F})$ for $1 \le i \le k$.

First, we prove the existence of the quantifier free formula Ψ in a constructive way. To do so, we proceed in three steps.

The first step is to successively compute $\mathrm{Elim}_{k-1}(\mathcal{F}), \dots, \mathrm{Elim}_0(\mathcal{F})$.

The second step is to successively compute $\mathrm{SIGN}(\mathrm{Elim}_1(\mathcal{F})), \dots, \mathrm{SIGN}(\mathrm{Elim}_k(\mathcal{F}))$ together with some additional information that will be needed in the third step. More precisely, starting from $\mathrm{Elim}_0(\mathcal{F}) \subset \mathbf{D}$, for $i = 0, \dots, k-1$, we consider every $\tau \in \mathrm{SIGN}(\mathrm{Elim}_i(\mathcal{F}))$. Following the procedure described in the proof of Proposition 24, for each such τ we compute

$$\mathrm{SIGN}(\mathrm{Elim}_{i+1}(\mathcal{F})(v, x_{i+1}))$$

for any $v \in \mathbf{R}^i$ such that

$$\mathrm{sign}(\mathrm{Elim}_i(\mathcal{F})(v)) = \tau,$$

and we keep the record that $\text{SIGN}(\text{Elim}_{i+1}(\mathcal{F})(\upsilon, x_{i+1})) \subset \text{SIGN}(\text{Elim}_{i+1}(\mathcal{F}))$ is exactly the set of realizable sign conditions on the family $\text{Elim}_{i+1}(\mathcal{F})$ given the extra condition that $\text{sign}(\text{Elim}_i(\mathcal{F})) = \tau$.

Note that these first two steps only depend on $\mathcal{F}$ rather than depending on the given first order formula

$$\text{Qu}_{i+1}x_{i+1} \dots \text{Qu}_k x_k \, \Phi(x_1, \dots, x_k).$$

The last step is to compute Ψ, or what is equivalent, T_Φ. To do so, we proceed by reverse induction on $i = k-1, \dots, 1$.

For $i = k-1$, we are given a first order formula of type

$$\text{Qu}_k x_k \, \Phi(x_1, \dots, x_k).$$

By Proposition 24, for every $\upsilon = (\upsilon_1, \dots, \upsilon_{k-1}) \in \mathbf{R}^{k-1}$, the list $\text{SIGN}(\mathcal{F}(\upsilon, x_k))$ is determined by the realizable sign condition on the family

$$\text{Elim}_{k-1}(\mathcal{F}) \subset \mathbf{D}[x_1, \dots, x_{k-1}]$$

satisfied by υ. Since $\Phi(x_1, \dots, x_k)$ is a quantifier free formula with atoms defined by polynomials in $\mathcal{F}$, from $\text{SIGN}(\mathcal{F}(\upsilon, x_k))$ it is possible to decide the truth value of the formula

$$\text{Qu}_k x_k \, \Phi(\upsilon, x_k).$$

So, we define

$$T_\Phi = \{\tau \in \text{SIGN}(\text{Elim}_{k-1}(\mathcal{F})) \mid \forall \upsilon \in \text{Real}(\tau, \mathbf{R}), \text{Qu}_k x_k \Phi(\upsilon, x_k) \text{ is true}\}$$

and

$$\Psi(x_1, \dots, x_{k-1}) \quad = \quad \bigvee_{\tau \in T_\Phi} (\text{sign}(\text{Elim}_{k-1}(\mathcal{F})) = \tau)$$

and we are done.

Now, we take $1 \leq i \leq k-2$ and we are given a first order formula of type

$$\text{Qu}_{i+1}x_{i+1} \, \text{Qu}_{i+2}x_{i+2} \dots \text{Qu}_k x_k \, \Phi(x_1, \dots, x_k).$$

By the inductive hypothesis, there exists a quantifier free formula

$$\Psi'(x_1, \dots, x_{i+1})$$

with atoms in $\text{Elim}_{i+1}(\mathcal{F})$ which is equivalent to

$$\text{Qu}_{i+2}x_{i+2} \dots \text{Qu}_k x_k \, \Phi(x_1, \dots, x_k).$$

By Proposition 24, for every $\upsilon = (\upsilon_1, \dots, \upsilon_i) \in \mathbf{R}^i$, the list $\text{SIGN}(\text{Elim}_{i+1}(\mathcal{F})(\upsilon, x_{i+1}))$ is determined by the sign condition on the family

$$\text{Elim}_i(\mathcal{F}) \subset \mathbf{D}[x_1, \dots, x_i]$$

satisfied by υ. Since $\Psi'(x_1,\dots,x_{i+1})$ is a quantifier free formula with atoms defined by polynomials in $\mathrm{Elim}_{i+1}(\mathcal{F})$, from $\mathrm{SIGN}(\mathrm{Elim}_{i+1}(\mathcal{F})(\upsilon, x_{i+1}))$ it is possible to decide the truth value of the formula

$$\mathrm{Qu}_{i+1} x_{i+1}\, \Psi'(\upsilon, x_{i+1}).$$

Finally, we define

$$T_\Phi = \{\tau \in \mathrm{SIGN}(\mathrm{Elim}_i(\mathcal{F})) \mid \forall \upsilon \in \mathrm{Real}(\tau, \mathbf{R}), \mathrm{Qu}_{i+1} x_{i+1} \Psi'(\upsilon, x_{i+1}) \text{ is true}\}$$

and

$$\Psi(x_1,\dots,x_i) \quad = \quad \bigvee_{\tau \in T_\Phi} (\mathrm{sign}(\mathrm{Elim}_i(\mathcal{F})) = \tau)$$

and we are done.

We now consider the quantitative part of the theorem. First, using Lemma 26, it can be easily proved by reverse induction that for $i = k,\dots,1$, for every $P \in \mathrm{Elim}_i(\mathcal{F})$,

$$\deg P \le 4^{\frac{4^{k-i}-1}{3}} d^{4^{k-i}}.$$

We prove then, again using Lemma 26 and by reverse induction, that for $i = k,\dots,1$,

$$\#\mathrm{Elim}_i(\mathcal{F}) \le s^{2^{k-i}} \max\{2,d\}^{(16^{k-i}-1)\mathrm{bit}(d)}.$$

Indeed, $\#\mathrm{Elim}_k(\mathcal{F}) = s$ and for $i = k-1,\dots,1$,

$$\begin{aligned}
\#\mathrm{Elim}_i(\mathcal{F}) \quad &\le \quad 4 s^{2^{k-i}} \max\{2,d\}^{2(16^{k-i-1}-1)\mathrm{bit}(d)} (4^{\frac{4^{k-i-1}-1}{3}} d^{4^{k-i-1}})^{(\mathrm{bit}(4^{\frac{4^{k-i-1}-1}{3}} d^{4^{k-i-1}})+2)} \le \\
&\le \quad s^{2^{k-i}} \max\{2,d\}^{2+2(16^{k-i-1}-1)\mathrm{bit}(d)+(2\frac{4^{k-i-1}-1}{3}+4^{k-i-1})(2\frac{4^{k-i-1}-1}{3}+4^{k-i-1}\mathrm{bit}(d)+2)} \le \\
&\le \quad s^{2^{k-i}} \max\{2,d\}^{(16^{k-i}-1)\mathrm{bit}(d)}.
\end{aligned}$$

Finally, we analyze the complexity of computing the quantifier free formula Ψ following the procedure we explained before.

Since the second and third step take only sign evaluation in $\mathbf{D}$ and operations in $\mathbb{Q}$, we only need to bound the complexity of the first step.

One more time using Lemma 26, for $1 \le i \le k-1$, the computation of $\mathrm{Elim}_i(\mathcal{F})$ from $\mathrm{Elim}_{i+1}(\mathcal{F})$ can be done within

$$O\left(s^{2^{k-i}} \max\{2,d\}^{2(16^{k-i-1}-1)\mathrm{bit}(d)} (4^{\frac{4^{k-i-1}-1}{3}} d^{4^{k-i-1}})^{(\mathrm{bit}(4^{\frac{4^{k-i-1}-1}{3}} d^{4^{k-i-1}})+5)} \right)$$

operations in $\mathbf{D}[x_1,\dots,x_i]$ between polynomials of degree at most

$$4^{\frac{4^{k-i}-1}{3}} d^{4^{k-i}}.$$

Taking into account that each of these operations can be done within

$$O\left(4^{i 2 \frac{4^{k-i}-1}{3}} d^{i 2 \cdot 4^{k-i}} \right)$$

operations in $\mathbf{D}$ and

$$\begin{aligned}
& s^{2^{k-i}} \max\{2,d\}^{2(16^{k-i-1}-1)\mathrm{bit}(d)} (4^{\frac{4^{k-i-1}-1}{3}} d^{4^{k-i-1}})^{(\mathrm{bit}(4^{\frac{4^{k-i-1}-1}{3}} d^{4^{k-i-1}})+5)} 4^{i2^{\frac{4^{k-i}-1}{3}}} d^{i2\cdot 4^{k-i}} \leq \\
\leq\ & s^{2^{k-i}} \max\{2,d\}^{2(16^{k-i-1}-1)\mathrm{bit}(d)+(2^{\frac{4^{k-i-1}-1}{3}}+4^{k-i-1})(2^{\frac{4^{k-i-1}-1}{3}}+4^{k-i-1}\mathrm{bit}(d)+5)+i4^{\frac{4^{k-i}-1}{3}}+i2\cdot 4^{k-i}} \leq \\
\leq\ & s^{2^{k-i}} \max\{2,d\}^{\mathrm{bit}(d)(16^{k-i}+i4^{k-i+1})},
\end{aligned}$$

the computation of $\mathrm{Elim}_i(\mathcal{F})$ from $\mathrm{Elim}_{i+1}(\mathcal{F})$ can be done within

$$O\left(s^{2^{k-i}} \max\{2,d\}^{\mathrm{bit}(d)(16^{k-i}+i4^{k-i+1})}\right)$$

operations in $\mathbf{D}$.

On the other hand, similarly, the computation of $\mathrm{Elim}_0(\mathcal{F})$ from $\mathrm{Elim}_1(\mathcal{F})$ can be done within

$$O\left(s^{2^k} \max\{2,d\}^{2(16^{k-1}-1)\mathrm{bit}(d)} (4^{\frac{4^{k-1}-1}{3}} d^{4^{k-1}})^{(\mathrm{bit}(4^{\frac{4^{k-1}-1}{3}} d^{4^{k-1}})+5)}\right) \leq O\left(s^{2^k} \max\{2,d\}^{16^k}\right)$$

operations in $\mathbf{D}$.

Finally, since

$$\sum_{i=1}^{k-1} s^{2^{k-i}} \max\{2,d\}^{\mathrm{bit}(d)(16^{k-i}+i4^{k-i+1})} \leq 2s^{2^k} \max\{2,d\}^{\mathrm{bit}(d)(16^k+(k-1)4^{k+1})},$$

the complexity of the first step is

$$O\left(s^{2^k} \max\{2,d\}^{\mathrm{bit}(d)(16^k+(k-1)4^{k+1})}\right)$$

operations in $\mathbf{D}$. □

Remark 28 *Note that the proof of correctness of the quantifier elimination method described in Theorem is entirely based on Proposition 24 and is thus completely algebraic.*

Note also that when the number of variables k is fixed the complexity of our method is polynomial in the number s of the polynomials, but is not polynomial in the degree d of the polynomials. On the other hand, the complexity of the Cylindrical Algebraic Decomposition [10] is polynomial in s and d when k is fixed (see [3, Chapter 11]) .

Acknowledgments: We are very grateful to the referee for his/her relevant and useful suggestions and remarks.

References

[1] Ben-Or M., Kozen D. and Reif J. *The complexity of elementary algebra and geometry.* J. of Computer and Systems Sciences 18, 251–264 (1986)

[2] Basu S., Pollack R. and Roy M.-F. *On the Combinatorial and Algebraic Complexity of Quantifier Elimination.* Journal of the A. C. M. 43, 1002–1045, (1996).

[3] Basu S., Pollack R. and Roy M.-F. *Algorithms in real algebraic geometry*, volume 10 of Algorithms and Computation in Mathematics, Second edition. Springer-Verlag, Berlin, 2006.

[4] Basu S., Pollack R. and Roy M.-F. *Algorithms in real algebraic geometry*, volume 10 of Algorithms and Computation in Mathematics, New online version avialable at `https://perso.univ-rennes1.fr/marie-francoise.roy/bpr-ed2-posted3.html`

[5] Berkowitz S. *On computing the determinant in small parallel time using a small number of processors.* Inf. Process. Lett. 18, 147–150 (1984).

[6] Canny J., *Improved Algorithms for Sign Determination and Existential Quantifier Elimination*, Comput. J. 36 (5), 409–418, 1993

[7] `https://coq.inria.fr/`

[8] Cohen P. J. *Decision procedures for real and p-adic fields.* Comm. in Pure and Applied Math. 22, 131–151 (1969).

[9] Cohen C. and Mahboubi A. *Formal proofs in real algebraic geometry: from ordered fields to quantifier elimination.* Log. Methods Comput. Sci. 8 no. 1, 1:02 (2012).

[10] Collins G. *Quantifier Elimination for real closed fields by cylindric algebraic decomposition.* Second GI Conference on Automata Theory and Formal Languages. LNCS vol 33, 134–183, Springer-Verlag, Berlin (1975).

[11] Coste M. and Roy M.-F. *Thom's lemma, the coding of real algebraic numbers and the computation of the topology of semi-algebraic sets.* J. Symbolic Computation, 121–129 (1988).

[12] Cox D., Little, J. and O'Shea, D. *Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra*, Undergraduate Texts in Mathematics, third edition. Springer, New York, 2007.

[13] Davenport J. H. and Heintz J. *Real quantifier elimination is doubly exponential.* Journal of Symbolic Computation 5, 29–35 (1988).

[14] Grigoriev D. *Complexity of deciding Tarski algebra.* J. Symbolic Comput. 5, 65–108 (1988).

[15] Grigoriev D. and Vorobjov N. *Solving systems of polynomial inequalities in subexponential time.* J. Symbolic Comput. 5, 37–64 (1988).

[16] Hörmander L. *The analysis of linear partial differential operators*, Berlin, Heidelberg, 364–367, Springer, New-York, 1983.

[17] Lojasiewicz S. *Ensembles semi-analytiques.* Institut des Hautes Etudes Scientifiques, 1965.

[18] Lombardi H., Perrucci D. and Roy M.-F. *An elementary recursive bound for effective Positivstellensatz and Hilbert 17-th problem.* Manuscript, 2014.

[19] Monk L. G. *Elementary-recursive decision procedures.* PhD thesis, UC Berkeley, 1975.

[20] Renegar J. *On the computational complexity and geometry of the first-order theory of the reals. I-III.* J. Symbolic Comput. 13, 255–352 (1992).

[21] Tarski A. *A decision method for elementary algebra and geometry*, Second Edition. University of California Press, Berkeley and Los Angeles, California, 1951.

[22] Seidenberg A. *A new decision method for elementary algebra.* Annals of Mathematics 60, 365–374 (1954).