An elementary recursive bound for effective Positivstellensatz and Hilbert 17-th problem

Henri Lombardi*
Daniel Perrucci †
Marie-Françoise Roy‡

version: April 10, 2017

Abstract

We prove an elementary recursive bound on the degrees for Hilbert 17-th problem. More precisely we express a nonnegative polynomial as a sum of squares of rational functions, and we obtain as degree estimates for the numerators and denominators the following tower of five exponentials

$$2^{2^{2^{d^{4^k}}}}$$

where d is the degree and k is the number of variables of the input polynomial. Our method is based on the proof of an elementary recursive bound on the degrees for Stengle's Positivstellensatz. More precisely we give an algebraic certificate of the emptyness of the realization of a system of sign conditions and we obtain as degree bounds for this certificate a tower of five exponentials, namely

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

where d is a bound on the degrees, s is the number of polynomials and k is the number of variables of the input polynomials.

Contents

*Laboratoire of Mathématiques (UMR CNRS 6623) UFR des Sciences et Techniques, Université of Franche-Comté 25030 Besançon cedex FRANCE. E-mail: lombardi@math.univ-fcomte.fr

†Departamento de Matemática, FCEN, Universidad de Buenos Aires and IMAS CONICET-UBA, ARGENTINA. Partially supported by the grants UBACYT 20020120100133 and PIP 099/11 CONICET. E-mail: perrucci@dm.uba.ar

‡IRMAR (UMR CNRS 6625), Université de Rennes 1, Campus de Beaulieu 35042 Rennes cedex FRANCE. E-mail: marie-francoise.roy@univ-rennes1.fr

MSC Classification: 12D15, 14P99, 13J30.

Keywords: Hilbert 17-th problem, Positivstellensatz, Real Nullstellensatz, degree bounds, elementary recursive functions.

1 Introduction

Throughout this paper, we denote by $\mathbb{N}$ the set of nonnegative integers, by $\mathbb{N}_*$ the set of positive integers, by $\mathbb{R}$ the field of real numbers, by $\mathbf{K}$ an ordered field, by $\mathbf{K}_+$ the set of positive elements of $\mathbf{K}$ and by $\mathbf{R}$ a real closed extension of $\mathbf{K}$.

1.1 Hilbert 17-th problem

Hilbert 17-th problem asks whether a real multivariate polynomial taking only nonnegative values is a sum of squares of rational functions ([27], [28], [29]). E. Artin gave a positive answer proving the following statement [1].

Theorem 1.1.1 (Hilbert 17-th problem) *Let $P \in \mathbb{R}[x_1, \ldots, x_k]$. If P takes only nonnegative values in $\mathbb{R}^k$, then P is a sum of squares in $\mathbb{R}(x_1, \ldots, x_k)$.*

1.2 Positivstellensatz

In order to give the statement of the Positivstellensatz, we will deal with finite conjunctions of equalities, strict inequalities and nonstrict inequalities on polynomials in $\mathbf{K}[x]$, where $x = (x_1, \ldots, x_k)$ is a set of variables.

Definition 1.2.1 *A* system of sign conditions $\mathcal{F}$ *in* $\mathbf{K}[x]$ *is a list of three finite (possibly empty) subsets* $[\mathcal{F}_{\neq}, \mathcal{F}_{\geq}, \mathcal{F}_{=}]$ *of* $\mathbf{K}[x]$*, representing the conjunction*

$$\begin{cases} P \neq 0 & \text{for } P \in \mathcal{F}_{\neq}, \\ P \geq 0 & \text{for } P \in \mathcal{F}_{\geq}, \\ P = 0 & \text{for } P \in \mathcal{F}_{=}. \end{cases}$$

Since the condition $P \leq 0$ is equivalent to $-P \geq 0$, the condition $P > 0$ is equivalent to $P \neq 0 \wedge P \geq 0$ and the condition $P < 0$ is equivalent to $P \neq 0 \wedge -P \geq 0$, any finite conjunction of equalities, strict inequalities and nonstrict inequalities can be represented by a system of sign conditions as in Definition 1.2.1. Throughout this paper, by a slight abuse of language, we will refer to such more general conjunctions as systems of sign conditions, when we should be strictly speaking referring to the systems of sign conditions associated to such conjunctions.

If $P \in \mathbf{K}[x]$ and $\xi = (\xi_1, \ldots, \xi_k) \in \mathbf{L}^k$ where $\mathbf{L}$ is a field extension of $\mathbf{K}$, we denote by $P(\xi) \in \mathbf{L}$ the result of the substitution of x by ξ.

Definition 1.2.2 *For an ordered extension* $\mathbf{L}$ *of* $\mathbf{K}$*, the* realization in $\mathbf{L}$ of *a system of sign conditions* $\mathcal{F}$ *in* $\mathbf{K}[x]$ *is the set*

$$\mathrm{Real}(\mathcal{F}, \mathbf{L}) = \{\xi \in \mathbf{L}^k \mid \bigwedge_{P \in \mathcal{F}_{\neq}} P(\xi) \neq 0, \bigwedge_{P \in \mathcal{F}_{\geq}} P(\xi) \geq 0, \bigwedge_{P \in \mathcal{F}_{=}} P(\xi) = 0\}.$$

If $\mathrm{Real}(\mathcal{F}, \mathbf{L})$ *is the empty set, we say that* $\mathcal{F}$ *is* unrealizable *in* $\mathbf{L}$.

Stengle's Positivstellensatz, which we will refer from now on simply as the Positivstellensatz, states that if a system $\mathcal{F}$ is unrealizable in $\mathbf{R}$, there is an algebraic identity which certifies this fact. To describe such an identity, we introduce the following notation and definitions.

Notation 1.2.3 *Let $\mathcal{P}$ be a finite subset of $\mathbf{K}[x]$. We denote by*

- $\mathcal{P}^2$ *the set of squares of elements of $\mathcal{P}$,*
- $\mathscr{M}(\mathcal{P})$ *the multiplicative monoid generated by $\mathcal{P}$,*
- $\mathscr{N}(\mathcal{P})_{\mathbf{K}[x]}$ *the nonnegative cone generated by $\mathcal{P}$ in $\mathbf{K}[x]$, which is the set of elements of type $\sum_{1\leq i\leq m}\omega_i V_i^2 \cdot N_i$ with $\omega_i \in \mathbf{K}_+$, $V_i \in \mathbf{K}[x]$ and $N_i \in \mathscr{M}(\mathcal{P})$ for $1 \leq i \leq m$,*
- $\mathscr{Z}(\mathcal{P})_{\mathbf{K}[x]}$ *the ideal generated by $\mathcal{P}$ in $\mathbf{K}[x]$.*

When the ring $\mathbf{K}[x]$ is clear from the context, we simply write $\mathscr{N}(\mathcal{P})$ for $\mathscr{N}(\mathcal{P})_{\mathbf{K}[x]}$ and $\mathscr{Z}(\mathcal{P})$ for $\mathscr{Z}(\mathcal{P})_{\mathbf{K}[x]}$.

Definition 1.2.4 *A system of sign conditions $\mathcal{F}$ in $\mathbf{K}[x]$ is* incompatible *if there is an algebraic identity*

$$S + N + Z = 0 \tag{1}$$

with $S \in \mathscr{M}(\mathcal{F}_{\neq}^2)$, $N \in \mathscr{N}(\mathcal{F}_{\geq})_{\mathbf{K}[x]}$ and $Z \in \mathscr{Z}(\mathcal{F}_{=})_{\mathbf{K}[x]}$. The identity (1) is called an incompatibility *of $\mathcal{F}$. We use the notation*

$$\downarrow \mathcal{F} \downarrow_{\mathbf{K}[x]}$$

to mean that an incompatibility of $\mathcal{F}$ is provided. We denote simply

$$\downarrow \mathcal{F} \downarrow$$

when the ring $\mathbf{K}[x]$ is clear from the context. The polynomials S, N and Z are called the monoid, cone *and* ideal part *of the incompatibility.*

An incompatibility (1) of $\mathcal{F}$ is a certificate that $\mathcal{F}$ is unrealizable in any ordered extension $\mathbf{L}$ of $\mathbf{K}$. Indeed, suppose that there exsists $\xi \in \mathrm{Real}(\mathcal{F}, \mathbf{L})$. Then

$$S(\xi) > 0, \; N(\xi) \geq 0, \text{ and } Z(\xi) = 0,$$

which is impossible since $S + N + Z = 0$.

Example 1.2.5 *The identity*

$$P^2 - P^2 = 0 \tag{2}$$

is an incompatibility of $\mathcal{F}_1 = [\{P\}, \emptyset, \{P\}]$, since $P^2 \in \mathscr{M}(\{P\}^2)$, $0 \in \mathscr{N}(\emptyset)$ and $-P^2 \in \mathscr{Z}(\{P\})$. For simplicity we write

$$\downarrow P \neq 0, \; P = 0 \downarrow$$

to mean $\downarrow \mathcal{F}_1 \downarrow$.

The identity (2) is also and incompatibility of $\mathcal{F}_2 = [\{P\}, \{P, -P\}, \emptyset]$, since $P^2 \in \mathscr{M}(\{P\}^2)$, $-P^2 \in \mathscr{N}(\{P, -P\})$ and $0 \in \mathscr{Z}(\emptyset)$. For simplicity, and following the procedure explained before so that every system of sign conditions is as in Definition 1.2.1, we write

$$\downarrow P > 0, \; P \leq 0 \downarrow$$

to mean $\downarrow \mathcal{F}_2 \downarrow$.

Similarly, the identity (2) also shows that

$$\downarrow P > 0, \; P = 0 \downarrow, \quad \downarrow P < 0, \; P = 0 \downarrow, \quad \downarrow P < 0, \; P \geq 0 \downarrow \quad \text{and} \quad \downarrow P > 0, \; P < 0 \downarrow.$$

Notation 1.2.6 *Let $\mathcal{F} = [\mathcal{F}_{\neq}, \mathcal{F}_{\geq}, \mathcal{F}_{=}]$ and $\mathcal{F}' = [\mathcal{F}'_{\neq}, \mathcal{F}'_{\geq}, \mathcal{F}'_{=}]$ be systems of sign conditions in $\mathbf{K}[x]$. We denote by $\mathcal{F},\ \mathcal{F}'$ the system $[\mathcal{F}_{\neq} \cup \mathcal{F}'_{\neq}, \mathcal{F}_{\geq} \cup \mathcal{F}'_{\geq}, \mathcal{F}_{=} \cup \mathcal{F}'_{=}]$.*

Note that $\downarrow \mathcal{F} \downarrow$ implies $\Big\downarrow \mathcal{F},\ \mathcal{F}' \Big\downarrow$.

A major concern in this paper are degrees of incompatibilities in the Positivstellensatz. To deal with them, we introduce below the following definitions.

Definition 1.2.7 *Let $\mathcal{P}$ be a finite set in $\mathbf{K}[x]$.*

- *For $N = \sum_{1\leq i\leq m} \omega_i V_i^2 \cdot N_i \in \mathscr{N}(\mathcal{P})$, with $\omega_i \in \mathbf{K}_+$, $V_i \in \mathbf{K}[x]$ and $N_i \in \mathscr{M}(\mathcal{P})$ for $1 \leq i \leq m$, we say that $\omega_i V_i^2 \cdot N_i$ are the* components *of N in $\mathscr{N}(\mathcal{P})$.*
- *For $Z = \sum_{1\leq i\leq m} W_i \cdot P_i \in \mathscr{Z}(\mathcal{P})$ with $W_i \in \mathbf{K}[x]$ and $P_i \in \mathcal{P}$ for $1 \leq i \leq m$, we say that $W_i \cdot P_i$ are the* components *of Z in $\mathscr{Z}(\mathcal{P})$.*

Note that $N \in \mathscr{N}(\mathcal{P})$ and $Z \in \mathscr{Z}(\mathcal{P})$ can be written as a sum of components in many different ways. So, when we talk of the components of N or Z, the ones we refer to should be clear from the context.

Definition 1.2.8 *Let $\mathcal{F}$ by a system of sign conditions in $\mathbf{K}[x]$. The* degree of the incompatibility

$$S + N + Z = 0 \tag{3}$$

with $S \in \mathscr{M}(\mathcal{F}_{\neq}^2)$, $N \in \mathscr{N}(\mathcal{P})$, and $Z \in \mathscr{Z}(\mathcal{F}_{=})$ is the maximum of the total degrees in x of S, the components of N and the components of Z. For a subset of variables $w \subset x$, the degree in w of the incompatibility (3) is the maximum of the total degrees in w of S, the components of N and the components of Z.

Contrary to the common convention, we consider the degree of the zero polynomial as 0. In this way, we have for instance the incompatibility $0 = 0$ of degree 0 which proves $\downarrow 0 \neq 0 \downarrow$.

The Positivstellensatz is the following theorem.

Theorem 1.2.9 (Positivstellensatz) *Let $\mathcal{F}$ be a system of sign conditions in $\mathbf{K}[x]$. The following are equivalent:*

1. *$\mathcal{F}$ is unrealizable in $\mathbf{R}$,*
2. *$\mathcal{F}$ is unrealizable in every ordered extension of $\mathbf{K}$,*
3. *$\mathcal{F}$ is incompatible.*

3. $\implies$ 2. and 2. $\implies$ 1. are clear, the difficult part is to prove 1. $\implies$ 3.

This statement comes from [52] (see also [6, 18, 19, 35, 48]).

An immediate consequence of the Positivstellensatz (Theorem 1.2.9) is the Real Nullstellensatz.

Theorem 1.2.10 (Real Nullstellensatz) *Let $P, P_1, \dots, P_s \in \mathbf{K}[x_1, \dots, x_k]$. If P vanishes on the common zero set of $P_1, \dots, P_s$ in $\mathbf{R}^k$, there is an identity*

$$P^{2e} + N = Z$$

with $N \in \mathscr{N}(\emptyset)_{\mathbf{K}[x_1,\dots,x_k]}$, and $Z \in \mathscr{Z}(P_1, \dots, P_s)_{\mathbf{K}[x_1,\dots,x_k]}$

Proof. Apply Theorem 1.2.9 (Positivstellensatz) to the system of sign conditions $[\{P\}, \emptyset, \{P_1, \dots, P_s\}]$, which corresponds to $P \neq 0, P_1 = 0, \dots, P_s = 0$. □

As another consequence of the Positivstellensatz (Theorem 1.2.9), we have an improved version of Hilbert 17-th problem due to Stengle [52].

Theorem 1.2.11 (Improved Hilbert 17-th problem) *Let $P \in \mathbf{K}[x_1, \dots, x_k]$ be a polynomial of degree d. If P is nonnegative in $\mathbf{R}^k$, then*

$$P = \sum_i \omega_i \frac{P_i^2}{Q^2}$$

with $\omega_i \in \mathbf{K}_+, P_i \in \mathbf{K}[x_1, \dots, x_k], Q \in \mathbf{K}[x_1, \dots, x_k]$, Q vanishing only at points where P vanishes.

Proof. Since P is nonnegative in $\mathbf{R}^k$, by Theorem 1.2.9 (Positivstellensatz) applied to the system $[\{P\}, \{-P\}, \emptyset]$, which corresponds to the sign condition $P < 0$, we have an identity

$$P^{2e} + N_1 - N_2 \cdot P = 0$$

with $e \in \mathbb{N}$ and $N_1, N_2 \in \mathscr{N}(\emptyset)_{\mathbf{K}[x_1,\dots,x_k]}$. Therefore

$$P = \frac{N_2 \cdot P^2}{P^{2e} + N_1} = \frac{N_2 \cdot P^2 \cdot (P^{2e} + N_1)}{(P^{2e} + N_1)^2}. \quad (4)$$

The result follows by expanding the numerator of the last expression in (4). □

1.3 Historical background on constructive proofs and degree bounds

In order to compare different degree bounds, in this section we use the notions of primitive recursive function and elementary recursive function (see [49, Chapter 1]).

With respect to Hilbert 17-th problem, Artin's proof of Theorem 1.1.1 is non-constructive and uses Zorn's lemma. Later, Kreisel and Daykin produced the first constructive proofs [33, 34, 14, 16] of this result, providing primitive recursive degree bounds.

For the Positivstellensatz, the original proofs were also non-constructive and used Zorn's lemma. The first constructive proof was given in [39, 40, 41], and it is based on the translation into algebraic identities of Cohen-Hörmander's quantifier elimination algorithm [9, 30, 6]. Following this construction, primitive recursive degree estimates for the incompatibility of the input system were obtained in [43]. In order to state this result precisely, we introduce the following notation.

Notation 1.3.1 *Let $\mathcal{F} = [\mathcal{F}_{\neq},\ \mathcal{F}_{\geq},\ \mathcal{F}_{=}]$ be a system of sign conditions in $\mathbf{K}[x]$. We denote by $|\mathcal{F}|$ a subset of $\mathcal{F}_{\neq} \cup \mathcal{F}_{\geq} \cup \mathcal{F}_{=}$ such that for every $P \in \mathcal{F}_{\neq} \cup \mathcal{F}_{\geq} \cup \mathcal{F}_{=}$ one and only one element of $\{P, -P\}$ is in $|\mathcal{F}|$.*

The first known degree bound for the Positivstellensatz is the following result (see [43, Théorème 26]), which is, in fact, still the only known degree bound till now.

Theorem 1.3.2 (Positivstellensatz with primitive recursive degree estimates) *Let $\mathcal{F}$ be a system of sign conditions in $\mathbf{K}[x_1, \ldots, x_k]$, such that $\#|\mathcal{F}| = s$ and the degree of every polynomial in $\mathcal{F}$ is bounded by d. If $\mathrm{Real}(\mathcal{F}, \mathbf{R})$ is empty, one can compute an incompatibility $\downarrow \mathcal{F} \downarrow$ with degree bounded by*

$$2^{2^{\cdot^{\cdot^{\cdot^{d\log(d)+\log\log(s)+c}}}}}$$

where c is a universal constant and the height of the exponential tower is $k + 4$.

A different constructive proof of the Real Nullstellensatz and Hilbert 17-th problem was given in [50], providing also primitive recursive degree bounds for the incompatibility it produces.

On the other hand, lower bounds on the degrees for the Positivstellensatz are given in [24], where for $k \geq 2$, an example is provided of an incompatible system $\mathcal{F}$ in $\mathbf{K}[x_1, \ldots, x_k]$ with $|\mathcal{F}| = k$ and the degree of every polynomial in $\mathcal{F}$ bounded by 2, such that every incompatibility of the system has degree at least 2^{k-2}. Concerning Hilbert 17-th problem, an example of a nonnegative polynomial of degree 4 in k variables, such that in any decomposition as a sum of squares of rational functions, the degree of some denominator is bounded from below by a linear function in k, appears in [5].

The huge gap between the best known lower bound on the degrees for the Positivstellensatz, which is singly exponential, and the best upper bound on the degrees known up to now, which is primitive recursive, is in strong contrast with the state of the art for the Hilbert Nullstellensatz. For this result, elementary recursive upper degree bounds are already known since [25]. Indeed, it is easy using resultants to obtain a doubly exponential bound on the degree of a Nullstellensatz identity [54, 4]. More recent and sophisticated results give singly exponential degree estimates [7, 8, 32, 31], which are known to be optimal.

1.4 Our results

The aim of this paper is to provide for the first time elementary recursive estimates on the degrees of the polynomials involved in the Positivstellensatz, Real Nullstellensatz and Hibert 17th problem. The existence of such bounds is a long-standing open question.

Notation 1.4.1 *We denote by $\mathrm{bit}(d)$ the number of bits of the natural number d, defined by*

$$\mathrm{bit}(d) = \begin{cases} 1 & \text{if } d = 0, \\ k & \text{if } d \neq 0 \text{ and } 2^{k-1} \leq d < 2^k. \end{cases}$$

We can state now the main results of this paper.

Theorem 1.4.2 (Positivstellensatz with elementary recursive degree estimates) *Let $\mathcal{F}$ be a system of sign conditions in $\mathbf{K}[x_1,\dots,x_k]$, such that $\#|\mathcal{F}| = s$ and the degree of every polynomial in $\mathcal{F}$ is bounded by d. If $\mathrm{Real}(\mathcal{F},\mathbf{R})$ is empty, one can compute an incompatibility $\downarrow \mathcal{F} \downarrow$ with degree bounded by*

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

As an immediate consequence of Theorem 1.4.2 we also get the following result.

Theorem 1.4.3 (Real Nullstellensatz with elementary recursive degree estimates) *Let $P, P_1,\dots,P_s \in \mathbf{K}[x_1,\dots,x_k]$ with degree bounded by d. If P vanishes on the common zero set of $P_1,\dots,P_s$ in $\mathbf{R}^k$, there is an identity*

$$P^{2e} + N = Z$$

with $N \in \mathscr{N}(\emptyset)_{\mathbf{K}[x_1,\dots,x_k]}$, and $Z \in \mathscr{Z}(P_1,\dots,P_s)_{\mathbf{K}[x_1,\dots,x_k]}$ of degree bounded by

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

The final main theorem of this paper is the following result.

Theorem 1.4.4 (Hilbert 17-th problem with elementary recursive degree estimates) *Let $P \in \mathbf{K}[x_1,\dots,x_k]$ be a polynomial of degree d. If P is nonnegative in $\mathbf{R}^k$, then*

$$P = \sum_i \omega_i \frac{P_i^2}{Q^2}$$

with $\omega_i \in \mathbf{K}_+, P_i \in \mathbf{K}[x_1,\dots,x_k], Q \in \mathbf{K}[x_1,\dots,x_k]$, Q vanishing only at points where P vanishes and $\deg P_i^2$ for every i and $\deg Q^2$ bounded by

$$2^{2^{2^{d^{4^k}}}}.$$

We sketch now a very brief description of the strategy we follow in our proof of Theorem 1.4.2 and Theorem 1.4.4. If a system of sign conditions $\mathcal{F}$ in $\mathbf{K}[x]$ is unrealizable in $\mathbf{R}$, we want to construct an incompatibility of $\mathcal{F}$. The idea is to transform a proof of the fact that $\mathcal{F}$ is unrealizable into a construction of an incompatibility. This was already the strategy used by [40, 43]; the proof that $\mathcal{F}$ is unrealizable was using Cohen-Hörmander quantifier elimination method [9, 30, 6] and was giving primitive recursive bounds for the final incompatibility.

In the current paper, the proof that $\mathcal{F}$ is unrealizable has to be based on more powerful tools than Cohen-Hörmander quantifier elimination method to obtain elementary recursive degree bounds, but it also has to remain *on the algebraic side*, so that we are able to turn it into a construction of an incompatibility.

The methods to prove the unrealizability in $\mathbf{R}$ of a system $\mathcal{F}$ are composed of many steps. Therefore, we need to know how to turn each of this steps into the construction of a new incompatibility. This is in general a very hard task and requires transforming standard and rather abstract proofs into very concrete proofs, in a way such that the outcome is so transparent that it becomes possible to read these new proofs as algebraic certificates or as constructions of algebraic certificates from other ones. More explicitly, in order to construct incompatibilities, we first need to associate to a well-chosen existing proof of the preceeding results, some specific algebraic identities. Then, using the key notions of weak inference and weak existence coming from [43], we have to show how to translate these modified proofs into constructions of incompatibilities. This translation is far from straightforward, relies heavily on the selected proof and the associated algebraic identities, and, as said before, should be done at each step for the corresponding specific result, most of the times in a different way. Indeed, the methods we develop here to consctruct incompatibilities associated to some well known results in mathematics may actually be of interest independent of our main results.

Since a single step of a proof that a system $\mathcal{F}$ is unrealizable in $\mathbf{R}$ which cannot be transformed into the construction of an incompatibility is enough to ruin the whole construction, it is clear that the choice of the method we use to prove that $\mathcal{F}$ is unrealizable, taking into account which steps compose this method, is of major importance.

Proving that that a system of sign conditions $\mathcal{F}$ is unrealizable in $\mathbf{R}$ is an instance of the Existential Theory of the Reals, which is a special case of Quantifier Elimination of the theory of real closed fields. Most of the proofs of Quantifier Elimination are based on the elimination of variables one after the other. More recent methods eliminate in one step a block of variables [22, 23, 47, 2, 15, 4].

The first proofs of Quantifier Elimination for the reals by Tarski, Seidenberg, Cohen or Hormander [53, 51, 9, 30] were all providing primitive recursive algorithms. The situation changed with the Cylindrical Algebraic Decomposition method [10, 38] and elementary recursive algorithms where obtained [44]. Cylindrical Algebraic Decomposition, is in fact doubly exponential (see for example [4]).

Singly exponential degree bounds, have been obtained for the Existential Theory of the Reals [22, 23, 47, 2, 15, 4] by eliminating in one step the block of existential variables. But these singly exponential results are based on the critical point method which seems *too geometric* to be translated into algebraic identities, and this is why we choose to use the technique of elimination of one variable after the other. In order to obtain our main results we need a method such that for each of its steps we are able to produce an incompatibility, and therefore we are led to design a suitable new elimination method with this property. This new elimination method produces a new purely algebraic proof of Quantifier Elimination which is elementary recursive [46].

Our proof translates into constructions of incompatibilities several main ingredients. Some of them are classical mathematical facts, but many of them come from much more recent results in computer algebra. These main ingredients are:

- the Intermediate Value Theorem for polynomials,
- Laplace's proof of the Fundamental Theorem of Algebra,
- Hermite's quadratic form, for real root counting with polynomial constraints,
- subresultants whose signs are determining the signature of Hermite's quadratic form,
- Sylvester's inertia law,

- Thom's lemma characterizing real algebraic numbers by sign conditions, and sign determination,
- a new elimination method reducing one by one the number of variables to consider.

Finally, for any unrealizable system of sign conditions we are able to construct an explicit incompatibility and prove that the degree bound of this incompatibility is elementary recursive. More precisely the five levels of exponentials in Theorem 1.4.2 and Theorem 1.4.4 come from the following facts

- eliminating all variables one after another produces univariate polynomials of doubly exponential degree,
- Laplace's proof of the Fundamental Theorem of Algebra introduces a polynomial of exponential degree,
- the construction of incompatibilities for the Intermediate Value Theorem produces algebraic identities of doubly exponential degrees.

Applying Laplace's proof of the Fundamental Theorem of Algebra to a univariate polynomial of doubly exponential degree, coming from the elimination process produces a polynomial of triple exponential degree. Since the Intermediate Value Theorem adds two more exponents to the degree of the final incompatibility, we obtain by our method a tower of five exponents.

We are lucky enough that the other ingredients of our construction do not increase the height of the tower above five exponentials. Full details will be provided in the paper.

1.5 Organization of the paper

Since the paper is very long, a significant effort is made to keep the organization simple.

In Section 2 we describe the concepts of weak inference and weak existence and we include many lemmas showing examples of them, with degree estimates, which correspond each to a very simple mathematical fact. These lemmas are used a large number of times in the rest of the paper and can be considered as the basis steps we use to obtain our results.

From Section 3 to 6 we develop weak inference versions of different theorems. In Section 3 we give a weak inference version of the Intermediate Value Theorem for polynomials. In Section 4 we give a weak inference version of the classical Laplace's proof of the Fundamental Theorem of Algebra and finally get a weak inference version of the factorization of a real polynomial into factors of degrees one and two. In Section 5, which is independent from Section 3 and Section 4, we obtain incompatibilities expressing the impossibility for a polynomial to have a number of real roots in conflict with the rank and signature of its Hermite's quadratic form, through an incompatibility version of Sylvester's Inertia Law. In Section 6 we show how to eliminate a variable in a family of polynomials under weak inference form. As said before, all these results may be of interest independent of our main results. Finally, in Section 7 we prove Theorem 1.4.2 and Theorem 1.4.4.

Each of Sections 3 to 6 contains a final theorem which is the only result from the section which is used outside the section, and it is used only in one of the remaining sections, as illustrated in the following diagram.

$$\begin{array}{ccccc} \text{Section 3} & \rightarrow & \text{Section 4} & & \\ & & & \searrow & \\ & & & & \text{Section 6} \rightarrow \text{Section 7} \\ & & & \nearrow & \\ & & \text{Section 5} & & \end{array}$$

A final annex provides the details of the proofs of several technical lemmas comparing the values of numerical functions which we use in our degree estimates.

Acknowledgements We would like to thank the anonymous referee for his/her relevant remarks. Special thanks to Saugata Basu for his linguistic advice.

2 Weak inference and weak existence

In this section we describe the concepts of weak inference (Definition 2.1.1) and weak existence (Definition 2.2.1) introduced in [43], improving and making more precise results from [42] (see also [11]). These are mechanisms to construct new incompatibilities from other ones already available. Most of the work we do in the paper is to develop weak inference and weak existence versions of known mathematical and algorithmical results, and obtain the corresponding degree estimates; therefore, these notions are central to our work. Several examples of the use of these notions, which play a role in the other sections of the paper, are provided, the most important being the case by case reasoning (see Subsection 2.1.3).

2.1 Weak inference

The idea behind the concept of weak inference is the following: let $\mathcal{F}$, $\mathcal{F}_1, \ldots, \mathcal{F}_m$, be systems of sign conditions in $\mathbf{K}[u] = \mathbf{K}[u_1, \ldots, u_n]$. Suppose that we know that for every $\vartheta = (\vartheta_1, \ldots, \vartheta_n) \in \mathbf{R}^n$ if the system $\mathcal{F}$ is satisfied at ϑ, then at least one of the systems $\mathcal{F}_1, \ldots, \mathcal{F}_m$ is also satisfied at ϑ. If we are given initial incompatibilities $\downarrow \mathcal{F}_1,\ \mathcal{H} \downarrow_{\mathbf{K}[v]}, \ldots, \downarrow \mathcal{F}_m,\ \mathcal{H} \downarrow_{\mathbf{K}[v]}, v \supset u$, this means that all the systems $[\mathcal{F}_1,\ \mathcal{H}], \ldots, [\mathcal{F}_m,\ \mathcal{H}]$ are unrealizable. Then we can conclude that the system $[\mathcal{F},\ \mathcal{H}]$ is also unrealizable in $\mathbf{R}$ and we would like an incompatibility $\downarrow \mathcal{F},\ \mathcal{H} \downarrow_{\mathbf{K}[v]}$ to certify this fact. A weak inference is an explicit way to construct this final incompatibility from the given initial ones.

Definition 2.1.1 (Weak Inference) *Let $\mathcal{F}, \mathcal{F}_1, \ldots, \mathcal{F}_m$ be systems of sign conditions in $\mathbf{K}[u]$. A* weak inference

$$\mathcal{F} \quad \vdash \quad \bigvee_{1 \le j \le m} \mathcal{F}_j$$

is a construction that, for any system of sign conditions $\mathcal{H}$ in $\mathbf{K}[v]$ with $v \supset u$, and any incompatibilities

$$\downarrow \mathcal{F}_1,\ \mathcal{H} \downarrow_{\mathbf{K}[v]}, \ldots, \downarrow \mathcal{F}_m,\ \mathcal{H} \downarrow_{\mathbf{K}[v]}$$

called the initial *incompatibilities, produces an incompatibility*

$$\downarrow \mathcal{F},\ \mathcal{H} \downarrow_{\mathbf{K}[v]}$$

called the final *incompatibility.*

Whenever we prove a weak inference, we also provide a description of the monoid part and a bound for the degree in the final incompatibility. This information is necessary to obtain the degree bound in our main results.

2.1.1 Basic rules

In the following lemmas we give some simple examples of weak inferences, most of them involving a one-term disjunction to the right (that is with $m = 1$ in Definition 2.1.1).

Lemma 2.1.2 *Let $P_1, P_2, \ldots, P_m \in \mathbf{K}[u]$. Then*

$$\begin{aligned} P_1 > 0 &\ \vdash\ P_1 \geq 0, & (1)\\ P_1 > 0 &\ \vdash\ P_1 \neq 0, & (2)\\ &\ \vdash\ P_1^2 \geq 0, & (3)\\ P_1 \neq 0 &\ \vdash\ P_1^2 > 0, & (4)\\ P_1 = 0 &\ \vdash\ P_1 \cdot P_2 = 0, & (5)\\ \bigwedge_{1\leq j\leq m} P_j \neq 0 &\ \vdash\ \prod_{1\leq j\leq m} P_j \neq 0, & (6)\\ \bigwedge_{1\leq j\leq m} P_j \geq 0 &\ \vdash\ \prod_{1\leq j\leq m} P_j \geq 0, & (7)\\ \bigwedge_{1\leq j\leq m} P_j > 0 &\ \vdash\ \prod_{1\leq j\leq m} P_j > 0. & (8) \end{aligned}$$

Moreover, in all cases, the initial incompatibility serves as the final incompatibility.

Proof. Since the proof of all the items is very similar, we only prove (8) which is the least obvious one. Consider the initial incompatibility

$$S \cdot \Big(\prod_{1\leq j\leq m} P_i \Big)^{2e} + N_0 + N_1 \cdot \prod_{1\leq j\leq m} P_i + Z = 0$$

with $S \in \mathscr{M}(\mathcal{H}_{\neq}^2)$, $N_0, N_1 \in \mathscr{N}(\mathcal{H}_{\geq})$ and $Z \in \mathscr{Z}(\mathcal{H}_{=})$, where $\mathcal{H} = [\mathcal{H}_{\neq}, \mathcal{H}_{\geq}, \mathcal{H}_{=}]$ is a system of sign conditions in $\mathbf{K}[v]$ with $v \supset u$. This proves the claim since

$$S \cdot \Big(\prod_{1\leq j\leq m} P_i \Big)^{2e} = S \cdot \prod_{1\leq j\leq m} P_i^{2e} \in \mathscr{M}((\mathcal{H}_{\neq} \cup \{P_1, \ldots, P_m\})^2),$$

$N_0 + N_1 \cdot \prod_{1\leq i\leq m} P_i \in \mathscr{N}(\mathcal{H}_{\geq} \cup \{P_1, \ldots, P_m\})$ and $Z \in \mathscr{Z}(\mathcal{H}_{=})$. □

Lemma 2.1.3 *Let $\alpha \in \mathbf{K}, P \in \mathbf{K}[u]$.*
If $\alpha > 0$,

$$\begin{aligned} P \geq 0 &\ \vdash\ \alpha P \geq 0, & (9)\\ P > 0 &\ \vdash\ \alpha P > 0. & (10) \end{aligned}$$

If $\alpha < 0$,

$$\begin{aligned} P \geq 0 &\ \vdash\ \alpha P \leq 0, & (11)\\ P > 0 &\ \vdash\ \alpha P < 0. & (12) \end{aligned}$$

For any α,

$$P = 0 \ \vdash\ \alpha P = 0. \qquad (13)$$

Moreover, in all cases, up to a division by an element of $\mathbf{K}_+$, the initial incompatibility serves as the final incompatibility.

Proof. Immediate. □

Lemma 2.1.4 *Let $P \in \mathbf{K}[u]$. Then*

$$P \geq 0,\ P \leq 0 \quad \vdash \quad P = 0.$$

If we have an initial incompatibility in $\mathbf{K}[v]$ where $v \supset u$ with monoid part S and degree in $w \subset v$ bounded by δ_w, the final incompatibility has the same monoid part and degree in w bounded by $\delta_w + \max\{\delta_w - \deg_w P, 0\}$.

Proof. Consider the initial incompatibility

$$S + N + Z + W \cdot P = 0$$

with $S \in \mathscr{M}(\mathcal{H}_{\neq}^2)$, $N \in \mathscr{N}(\mathcal{H}_{\geq})$, $Z \in \mathscr{Z}(\mathcal{H}_{=})$ and $W \in \mathbf{K}[v]$, where $\mathcal{H} = [\mathcal{H}_{\neq}, \mathcal{H}_{\geq}, \mathcal{H}_{=}]$ is a system of sign conditions in $\mathbf{K}[v]$. If W is the zero polynomial there is nothing to do; otherwise we rewrite the initial incompatibility as

$$S + N + \tfrac{1}{4}(1+W)^2 \cdot P + \tfrac{1}{4}(1-W)^2 \cdot (-P) + Z = 0.$$

This proves the claim since $S \in \mathscr{M}(\mathcal{H}_{\neq}^2)$, $N + \frac{1}{4}(1+W)^2 \cdot P + \frac{1}{4}(1-W)^2 \cdot (-P) \in \mathscr{N}(\mathcal{H}_{\geq} \cup \{P, -P\})$ and $Z \in \mathscr{Z}(\mathcal{H}_{=})$. The degree bound follows easily. □

Lemma 2.1.5 *Let $P_1, \dots, P_m \in \mathbf{K}[u]$. Then*

$$\bigwedge_{1 \leq j \leq m} P_j = 0 \ \vdash \ \sum_{1 \leq j \leq m} P_j = 0, \tag{14}$$

$$\bigwedge_{1 \leq j \leq m'} P_j \geq 0, \quad \bigwedge_{m'+1 \leq j \leq m} P_j = 0 \ \vdash \ \sum_{1 \leq j \leq m} P_j \geq 0. \tag{15}$$

In both cases, if we have an initial incompatibility in $\mathbf{K}[v]$ where $v \supset u$ with monoid part S and degree in $w \subset v$ bounded by δ_w, the final incompatibility has the same monoid part and degree in w bounded by $\delta_w + \max\{\deg_w P_j \mid 1 \leq j \leq m\} - \deg_w \sum_{1 \leq j \leq m} P_j$.

Proof. We first prove item 14. Consider the initial incompatibility

$$S + N + Z + W \cdot \sum_{1 \leq j \leq m} P_j = 0$$

with $S \in \mathscr{M}(\mathcal{H}_{\neq}^2), N \in \mathscr{N}(\mathcal{H}_{\geq})$, $Z \in \mathscr{Z}(\mathcal{H}_{=})$ and $W \in \mathbf{K}[v]$, where $\mathcal{H} = [\mathcal{H}_{\neq}, \mathcal{H}_{\geq}, \mathcal{H}_{=}]$ is a system of sign conditions in $\mathbf{K}[v]$. We rewrite this equation as

$$S + N + Z + \sum_{1 \leq j \leq m} W \cdot P_j = 0.$$

This proves the claim since $S \in \mathscr{M}(\mathcal{H}_{\neq}^2)$, $N \in \mathscr{N}(\mathcal{H}_{\geq})$ and $Z + \sum_{1 \leq j \leq m} W \cdot P_j \in \mathscr{Z}(\mathcal{H}_{=} \cup \{P_1, \dots, P_m\})$. The degree bound follows easily.

Now we prove item 15. Consider the initial incompatibility

$$S + N_0 + N_1 \cdot \sum_{1\le j\le m} P_j + Z = 0$$

with $S \in \mathscr{M}(\mathcal{H}_{\neq}^2), N_0, N_1 \in \mathscr{N}(\mathcal{H}_{\geq})$ and $Z \in \mathscr{Z}(\mathcal{H}_{=})$, where $\mathcal{H} = [\mathcal{H}_{\neq}, \mathcal{H}_{\geq}, \mathcal{H}_{=}]$ is a system of sign conditions in $\mathbf{K}[v]$. We rewrite this equation as

$$S + N_0 + \sum_{1\le j\le m'} N_1 \cdot P_j + Z + \sum_{m'+1\le j\le m} N_1 \cdot P_j = 0.$$

This proves the claim since $S \in \mathscr{M}(\mathcal{H}_{\neq}^2)$, $N_0 + \sum_{1\le j\le m'} N_1 \cdot P_j \in \mathscr{N}(\mathcal{H}_{\geq} \cup \{P_1, \ldots, P_{m'}\})$ and $Z + \sum_{m'+1\le j\le m} N_1 \cdot P_j \in \mathscr{Z}(\mathcal{H}_{=} \cup \{P_{m'+1}, \ldots, P_m\})$. The degree bound follows easily. □

Lemma 2.1.6 *Let $P_1, \ldots, P_m \in \mathbf{K}[u]$. Then*

$$P_1 \neq 0, \bigwedge_{2\le j\le m} P_j = 0 \quad \vdash \quad \sum_{1\le j\le m} P_j \neq 0.$$

If we have an initial incompatibility in $\mathbf{K}[v]$ where $v \supset u$ with monoid part $S(\sum_{1\le j\le m} P_j)^{2e}$ and degree in $w \subset v$ bounded by δ_w, the final incompatibility has monoid part $S \cdot P_1^{2e}$ and degree in w bounded by $\delta_w + 2e\Big(\max\{\deg_w P_j \mid 1 \le j \le m\} - \deg_w \sum_{1\le j\le m} P_j\Big)$.

Proof. Consider the initial incompatibility

$$S \cdot \Big(\sum_{1\le j\le m} P_j\Big)^{2e} + N + Z = 0$$

with $S \in \mathscr{M}(\mathcal{H}_{\neq}^2), N \in \mathscr{N}(\mathcal{H}_{\geq})$ and $Z \in \mathscr{Z}(\mathcal{H}_{=})$, where $\mathcal{H} = [\mathcal{H}_{\neq}, \mathcal{H}_{\geq}, \mathcal{H}_{=}]$ is a system of sign conditions in $\mathbf{K}[v]$. We rewrite this equation as

$$S \cdot P_1^{2e} + N + Z + Z_2 = 0$$

where $Z_2 \in \mathscr{Z}(\{P_2, \ldots, P_m\})$ is the sum of all the terms in the expansion of $S \cdot (\sum_{1\le j\le m} P_j)^{2e}$ which involve at least one of $P_2, \ldots, P_m$. This proves the claim since $S \cdot P_1^{2e} \in \mathscr{M}((\mathcal{H}_{\neq} \cup \{P_1\})^2)$, $N \in \mathscr{N}(\mathcal{H}_{\geq})$ and $Z + Z_2 \in \mathscr{Z}(\mathcal{H}_{=} \cup \{P_2, \ldots, P_m\})$. The degree bound follows easily. □

Lemma 2.1.7 *Let $P_1, \ldots, P_m \in \mathbf{K}[u]$. Then*

$$P_1 > 0, \bigwedge_{2\le j\le m'} P_j \ge 0, \bigwedge_{m'+1\le j\le m} P_j = 0 \quad \vdash \quad \sum_{1\le j\le m} P_j > 0.$$

If we have an initial incompatibility in $\mathbf{K}[v]$ where $v \supset u$ with monoid part $S \cdot \big(\sum_{1\le j\le m} P_j\big)^{2e}$ and degree in $w \subset v$ bounded by δ_w, the final incompatibility has monoid part $S \cdot P_1^{2e}$ and degree in w bounded by $\delta_w + \max\{1, 2e\}\Big(\max\{\deg_w P_j \mid 1 \le j \le m\} - \deg_w \sum_{1\le j\le m} P_j\Big)$.

Proof. Consider the initial incompatibility

$$S \cdot \Big(\sum_{1 \le j \le m} P_j \Big)^{2e} + N_0 + N_1 \cdot \sum_{1 \le j \le m} P_j + Z = 0$$

with $S \in \mathscr{M}(\mathcal{H}_{\neq}^2), N_0, N_1 \in \mathscr{N}(\mathcal{H}_{\geq})$ and $Z \in \mathscr{Z}(\mathcal{H}_{=})$, where $\mathcal{H} = [\mathcal{H}_{\neq},\, \mathcal{H}_{\geq},\, \mathcal{H}_{=}]$ is a system of sign conditions in $\mathbf{K}[v]$. We rewrite this equation as

$$S \cdot P_1^{2e} + N_0 + N_2 + \sum_{1 \le j \le m'} N_1 \cdot P_j + Z + Z_2 + \sum_{m'+1 \le j \le m} N_1 \cdot P_j = 0,$$

where $N_2 \in \mathscr{N}(\{P_1, \ldots, P_{m'}\})$ is the sum of all the terms in the expansion of $S \cdot (\sum_{1 \le j \le m} P_j)^{2e}$ which do not involve any of $P_{m'+1}, \ldots, P_m$ with the exception of the term $S \cdot P_1^{2e}$ and $Z_2 \in \mathscr{Z}(\{P_{m'+1}, \ldots, P_m\})$ is the sum of all the terms in the expansion of $S \cdot (\sum_{1 \le j \le m} P_j)^{2e}$ which involve at least one of $P_{m'+1}, \ldots, P_m$. This proves the claim since $S \cdot P_1^{2e} \in \mathscr{M}((\mathcal{H}_{\neq} \cup \{P_1\})^2)$, $N_0 + N_2 + \sum_{1 \le j \le m'} N_1 \cdot P_j \in \mathscr{N}(\mathcal{H}_{\geq} \cup \{P_1, \ldots, P_{m'}\})$ and $Z + Z_2 + \sum_{m'+1 \le j \le m} N_1 \cdot P_j \in \mathscr{Z}(\mathcal{H}_{=} \cup \{P_{m'+1}, \ldots, P_m\})$. The degree bound follows easily. □

Lemma 2.1.8 *Let $m_1, \ldots, m_n \in \mathbb{N}_*$ and $P_{j,k}, Q_{j,k} \in \mathbf{K}[u]$ for $1 \le j \le m_k, 1 \le k \le n$. Then*

$$\bigwedge_{\substack{1 \le k \le n, \\ 1 \le j \le m_k}} P_{j,k} = 0 \quad \vdash \quad \bigwedge_{1 \le k \le n} \sum_{1 \le j \le m_k} P_{j,k} \cdot Q_{j,k} = 0.$$

If we have an initial incompatibility in $\mathbf{K}[v]$ where $v \supset u$ with monoid part S and degree in $w \subset v$ bounded by δ_w, the final incompatibility has the same monoid part and degree in w bounded by

$$\delta_w + \max\Big\{ \max\{\deg_w P_{j,k} \cdot Q_{j,k} \mid 1 \le j \le m_k\} - \deg_w \sum_{1 \le j \le m_k} P_{j,k} \cdot Q_{j,k} \mid 1 \le k \le n \Big\}.$$

Proof. Follows from Lemmas 2.1.2 (item 5) and an easy adaptation of the proof of Lemma 2.1.5 (item 14). □

Lemma 2.1.9 *Let $P_1, P_2 \in \mathbf{K}[u]$. Then*

$$P_1 \cdot P_2 \ge 0,\ P_2 > 0 \quad \vdash \quad P_1 \ge 0.$$

If we have an initial incompatibility in $\mathbf{K}[v]$ where $v \supset u$ with monoid part S and degree in $w \subset v$ bounded by δ_w, the final incompatibility has monoid part $S \cdot P_2^2$ and degree in w bounded by $\delta_w + 2\deg_w P_2$.

Proof. Consider the initial incompatibility

$$S + N_0 + N_1 \cdot P_1 + Z = 0$$

with $S \in \mathscr{M}(\mathcal{H}_{\neq}^2)$, $N_0, N_1 \in \mathscr{N}(\mathcal{H}_{\geq})$ and $Z \in \mathscr{Z}(\mathcal{H}_{=})$, where $\mathcal{H} = [\mathcal{H}_{\neq},\, \mathcal{H}_{\geq},\, \mathcal{H}_{=}]$ is a system of sign conditions in $\mathbf{K}[v]$. We multiply this equation by P_2^2 and we obtain

$$S \cdot P_2^2 + N_0 \cdot P_2^2 + N_1 \cdot P_1 \cdot P_2^2 + Z \cdot P_2^2 = 0.$$

This proves the claim since $S \cdot P_2^2 \in \mathscr{M}((\mathcal{H}_{\neq} \cup \{P_2\})^2)$, $N_0 \cdot P_2^2 + N_1 \cdot P_1 \cdot P_2^2 \in \mathscr{N}(\mathcal{H}_{\geq} \cup \{P_1 \cdot P_2, P_2\})$ and $Z \cdot P_2^2 \in \mathscr{Z}(\mathcal{H}_{=})$. The degree bound follows easily. □

Lemma 2.1.10 *Let $P_1, P_2 \in \mathbf{K}[u]$. Then*

$$P_1 \cdot P_2 > 0,\ P_2 > 0 \quad \vdash \quad P_1 > 0.$$

If we have an initial incompatibility in $\mathbf{K}[v]$ where $v \supset u$ with monoid part $S \cdot P_1^{2e}$ and degree in $w \subset v$ bounded by δ_w, the final incompatibility has monoid part $S \cdot P_2^2$ if $e = 0$ and $S \cdot (P_1 \cdot P_2)^{2e}$ if $e \geq 1$ and degree in w bounded by $\delta_w + 2\max\{1, e\} \deg_w P_2$ in both cases.

Proof. Consider the initial incompatibility

$$S \cdot P_1^{2e} + N_0 + N_1 \cdot P_1 + Z = 0$$

with $S \in \mathscr{M}(\mathcal{H}_{\neq}^2)$, $N_0, N_1 \in \mathscr{N}(\mathcal{H}_{\geq})$ and $Z \in \mathscr{Z}(\mathcal{H}_{=})$, where $\mathcal{H} = [\mathcal{H}_{\neq}, \mathcal{H}_{\geq}, \mathcal{H}_{=}]$ is a system of sign conditions in $\mathbf{K}[v]$. If $e = 0$, we proceed as in the proof of Lemma 2.1.9. If $e \geq 1$, we multiply this equation by P_2^{2e} and we obtain

$$S \cdot (P_1 \cdot P_2)^{2e} + N_0 \cdot P_2^{2e} + N_1 \cdot P_1 \cdot P_2^{2e} + Z \cdot P_2^{2e} = 0.$$

This proves the claim since $S \cdot (P_1 \cdot P_2)^{2e} \in \mathscr{M}((\mathcal{H}_{\neq} \cup \{P_1 \cdot P_2, P_2\})^2)$, $N_0 \cdot P_2^{2e} + N_1 \cdot P_1 \cdot P_2^{2e} \in \mathscr{N}(\mathcal{H}_{\geq} \cup \{P_1 \cdot P_2, P_2\})$ and $Z \cdot P_2^{2e} \in \mathscr{Z}(\mathcal{H}_{=})$. The degree bound follows easily. □

Lemma 2.1.11 *Let $P_1, P_2 \in \mathbf{K}[u]$. Then*

$$P_1 + P_2 > 0,\ P_1 \cdot P_2 \geq 0 \quad \vdash \quad P_1 \geq 0,\ P_2 \geq 0.$$

If we have an initial incompatibility in $\mathbf{K}[v]$ where $v \supset u$ with monoid part S and degree in $w \subset v$ bounded by δ_w, the final incompatibility has monoid part $S \cdot (P_1 + P_2)^2$ and degree in w bounded by $\delta_w + 2\max\{\deg_w P_1, \deg_w P_2\}$.

Proof. Consider the initial incompatibility

$$S + N_0 + N_1 \cdot P_1 + N_2 \cdot P_2 + N_3 \cdot P_1 \cdot P_2 + Z = 0$$

with $S \in \mathscr{M}(\mathcal{H}_{\neq}^2)$, $N_0, N_1, N_2, N_3 \in \mathscr{N}(\mathcal{H}_{\geq})$ and $Z \in \mathscr{Z}(\mathcal{H}_{=})$, where $\mathcal{H} = [\mathcal{H}_{\neq}, \mathcal{H}_{\geq}, \mathcal{H}_{=}]$ is a system of sign conditions in $\mathbf{K}[v]$. We multiply this equation by $(P_1 + P_2)^2$ and we rewrite it as

$$S \cdot (P_1 + P_2)^2 + N_0 \cdot (P_1 + P_2)^2 + N_1 \cdot P_1^2 \cdot (P_1 + P_2) + N_2 \cdot P_2^2 \cdot (P_1 + P_2) +$$

$$+ (N_1 + N_2) \cdot (P_1 + P_2) \cdot P_1 \cdot P_2 + N_3 \cdot (P_1 + P_2)^2 \cdot P_1 \cdot P_2 + Z \cdot (P_1 + P_2)^2 = 0.$$

This proves the claim since $S \cdot (P_1 + P_2)^2 \in \mathscr{M}((\mathcal{H}_{\neq} \cup \{P_1 + P_2\})^2)$, $N_0 \cdot (P_1 + P_2)^2 + N_1 \cdot P_1^2 \cdot (P_1 + P_2) + N_2 \cdot P_2^2 \cdot (P_1 + P_2) + (N_1 + N_2) \cdot (P_1 + P_2) \cdot P_1 \cdot P_2 + N_3 \cdot (P_1 + P_2)^2 \cdot P_1 \cdot P_2 \in \mathscr{N}(\mathcal{H}_{\geq} \cup \{P_1 + P_2, P_1 \cdot P_2\})$ and $Z \cdot (P_1 + P_2)^2 \in \mathscr{Z}(\mathcal{H}_{=})$. The degree bound follows easily. □

Lemma 2.1.12 *Let $P_1, \dots, P_m \in \mathbf{K}[u]$. Then*

$$\prod_{1 \leq j \leq m} P_j = 0 \quad \vdash \quad \bigvee_{1 \leq j \leq m} P_j = 0.$$

If we have initial incompatibilities in $\mathbf{K}[v]$ where $v \supset u$ with monoid part S_j and degree in $w \subset v$ bounded by $\delta_{w,j}$, the final incompatibility has monoid part $\prod_{1 \leq j \leq m} S_j$ and degree in w bounded by $\sum_{1 \leq j \leq m} \delta_{w,j}$.

Proof. Consider for $1 \le j \le m$ the initial incompatibility

$$S_j + N_j + Z_j + W_j \cdot P_j = 0$$

with $S_j \in \mathscr{M}(\mathcal{H}_{\neq}^2)$, $N_j \in \mathscr{N}(\mathcal{H}_{\geq})$, $Z_j \in \mathscr{Z}(\mathcal{H}_{=})$ and $W_j \in \mathbf{K}[v]$, where $\mathcal{H} = [\mathcal{H}_{\neq}, \mathcal{H}_{\geq}, \mathcal{H}_{=}]$ is a system of sign conditions in $\mathbf{K}[v]$. We pass $W_j \cdot P_j$ to the right hand side in the initial incompatibility, we multiply all the results and we pass $(-1)^m \prod_{1\le j\le m} W_j \cdot P_j$ to the left hand side. We obtain

$$\prod_{1\le j\le m} S_j + N + Z + (-1)^{m+1} \prod_{1\le j\le m} W_j \cdot P_j = 0$$

where $N \in \mathscr{N}(\mathcal{H}_{\geq})$ is the sum of all the terms in the expansion of $\prod_{1\le j\le m}(S_j + N_j)$ with the exception of the term $\prod_{1\le j\le m} S_j$ and $Z \in \mathscr{Z}(\mathcal{H}_{=})$ is the sum of all the terms in the expansion of $\prod_{1\le j\le m}(S_j + N_j + Z_j)$ which involve at least one of $Z_1, \dots, Z_m$. This proves the claim since $\prod_{1\le j\le m} S_j \in \mathscr{M}(\mathcal{H}_{\neq}^2)$, $N \in \mathscr{N}(\mathcal{H}_{\geq})$ and $Z + (-1)^{m+1}\prod_{1\le j\le m} W_j P_j \in \mathscr{Z}(\mathcal{H}_{=} \cup \{\prod_{1\le j\le m} P_j\})$. The degree bound follows easily. □

2.1.2 Sums of squares

The following remark states a very useful algebraic identity.

Remark 2.1.13 *Let $\mathbf{A}$ be a commutative ring and $A_1, \dots, A_m, B_1, \dots, B_m \in \mathbf{A}$. Consider the sum of squares*

$$\mathrm{N}(A_1, \dots, A_m, B_1, \dots, B_m) = \sum_{\substack{\sigma\in\{-1,1\}^m,\\ \sigma\neq(1,\dots,1)}} \Big(\sum_{1\le j\le m} \sigma(j) A_j B_j\Big)^2 + 2^m \sum_{1\le j,j'\le m,\, j\neq j'} (A_j B_{j'})^2.$$

Then

$$\Big(\sum_{1\le j\le m} A_j B_j\Big)^2 + \mathrm{N}(A_1, \dots, A_m, B_1, \dots, B_m) = 2^m \sum_{1\le j\le m} A_j^2 \cdot \sum_{1\le j\le m} B_j^2. \qquad (16)$$

We can now prove some more weak inferences.

Lemma 2.1.14 *Let $P_1, \dots, P_m \in \mathbf{K}[u]$. Then*

$$\sum_{1\le j\le m} P_j^2 = 0 \quad \vdash \quad \bigwedge_{1\le j\le m} P_j = 0.$$

If we have an initial incompatibility in $\mathbf{K}[v]$ where $v \supset u$ with monoid part S and degree in $w \subset v$ bounded by δ_w, the final incompatibility has monoid part S^2 and degree in w bounded by

$$2\Big(\delta_w + \max\{\deg_w P_j \mid 1 \le j \le m\} - \min\{\deg_w P_j \mid 1 \le j \le m\}\Big).$$

Proof. Consider the initial incompatibility

$$S + N + Z + \sum_{1\le j\le m} W_j \cdot P_j = 0$$

with $S \in \mathscr{M}(\mathcal{H}_{\neq}^2)$, $N \in \mathscr{N}(\mathcal{H}_{\geq})$, $Z \in \mathscr{Z}(\mathcal{H}_{=})$ and $W_j \in \mathbf{K}[v]$ for $1 \leq j \leq m$, where $\mathcal{H} = [\mathcal{H}_{\neq},\, \mathcal{H}_{\geq},\, \mathcal{H}_{=}]$ is a system of sign conditions in $\mathbf{K}[v]$. First, we pass $\sum W_j \cdot P_j$ to the right hand side, we raise to the square, we add $\mathrm{N}(W_1, \dots, W_m, P_1, \dots, P_m)$ defined as in Remark 2.1.13 and we substitute using (16). Then we pass $2^m \sum W_j^2 \cdot \sum P_j^2$ to the left hand side and we obtain

$$S^2 + N_1 + \mathrm{N}(W_1, \dots, W_m, P_1, \dots, P_m) + Z_1 - 2^m \sum_{1 \leq j \leq m} W_j^2 \cdot \sum_{1 \leq j \leq m} P_j^2 = 0$$

where $N_1 = 2N \cdot S + N^2$ and $Z_1 = 2Z \cdot S + 2Z \cdot N + Z^2$. This proves the claim since $S^2 \in \mathscr{M}(\mathcal{H}_{\neq}^2)$, $N_1 + \mathrm{N}(W_1, \dots, W_m, P_1, \dots, P_m) \in \mathscr{N}(\mathcal{H}_{\geq})$ and $Z_1 - 2^m \sum W_j^2 \cdot \sum P_j^2 \in \mathscr{Z}(\mathcal{H}_{=} \cup \{\sum P_j^2\})$. The degree bound follows easily taking into account that $\deg_w \sum P_j^2 = 2 \max\{\deg_w P_j\}$. □

Lemma 2.1.15 *Let $P_1, \dots, P_m, Q_1, \dots, Q_m \in \mathbf{K}[u]$. Then*

$$\sum_{1 \leq j \leq m} P_j \cdot Q_j \neq 0 \quad \vdash \quad \sum_{1 \leq j \leq m} P_j^2 \neq 0.$$

If we have an initial incompatibility in $\mathbf{K}[v]$ where $v \supset u$ with monoid part $S \cdot (\sum_{1 \leq j \leq m} P_j^2)^{2e}$ and degree in $w \subset v$ bounded by δ_w, the final incompatibility has monoid part $S \cdot (\sum_{1 \leq j \leq m} P_j \cdot Q_j)^{4e}$ and degree in w bounded by $\delta_w + 4e \max\{\deg_w Q_j \mid 1 \leq j \leq m\}$.

Proof. Consider the initial incompatibility

$$S \cdot \Big(\sum_{1 \leq j \leq m} P_j^2 \Big)^{2e} + N + Z = 0$$

with $S \in \mathscr{M}(\mathcal{H}_{\neq}^2)$, $N \in \mathscr{N}(\mathcal{H}_{\geq})$ and $Z \in \mathscr{Z}(\mathcal{H}_{=})$, where $\mathcal{H} = [\mathcal{H}_{\neq},\, \mathcal{H}_{\geq},\, \mathcal{H}_{=}]$ is a system of sign conditions in $\mathbf{K}[v]$. We multiply this equation by $2^{2me}(\sum Q_j^2)^{2e}$, we substitute using (16) and we obtain

$$S \cdot \Big(\sum_{1 \leq j \leq m} P_j \cdot Q_j \Big)^{4e} + N_1 + 2^{2me} N \cdot \Big(\sum_{1 \leq j \leq m} Q_j^2 \Big)^{2e} + 2^{2me} Z \cdot \Big(\sum_{1 \leq j \leq m} Q_j^2 \Big)^{2e} = 0$$

where N_1 is the sum of all the terms in the expansion of $S \cdot ((\sum_{1 \leq j \leq m} P_j \cdot Q_j)^2 + \mathrm{N}(P_1, \dots, P_m, Q_1, \dots, Q_m))^{2e}$ with the exception of the term $S \cdot (\sum_{1 \leq j \leq m} P_j \cdot Q_j)^{4e}$. This proves the claim since $S \cdot (\sum_{1 \leq j \leq m} P_j \cdot Q_j)^{4e} \in \mathscr{M}((\mathcal{H}_{\neq} \cup \{\sum_{1 \leq j \leq m} P_j \cdot Q_j\})^2)$, $N_1 + 2^{2me} N \cdot (\sum_{1 \leq j \leq m} Q_j^2)^{2e} \in \mathscr{N}(\mathcal{H}_{\geq})$ and $2^{2me} Z \cdot (\sum Q_j^2)^{2e} \in \mathscr{Z}(\mathcal{H}_{=})$. The degree bound follows easily. □

2.1.3 Case by case reasoning

We will refer to the weak inferences in the following lemmas as "case by case reasoning", which enable us to consider separately the different possible sign conditions in each case.

Lemma 2.1.16 *Let $P \in \mathbf{K}[u]$. Then*

$$\vdash \quad P \neq 0 \;\vee\; P = 0.$$

If we have initial incompatibilities in $\mathbf{K}[v]$ where $v \supset u$ with monoid part $S_1 \cdot P^{2e}$ and S_2 and degree in $w \subset v$ bounded by $\delta_{w,1}$ and $\delta_{w,2}$, the final incompatibility has monoid part $S_1 \cdot S_2^{2e}$ and degree in w bounded by $\delta_{w,1} + 2e(\delta_{w,2} - \deg_w P)$.

Proof. Consider the initial incompatibilities

$$S_1 \cdot P^{2e} + N_1 + Z_1 = 0 \tag{17}$$

and

$$S_2 + N_2 + Z_2 + W \cdot P = 0 \tag{18}$$

with $S_1, S_2 \in \mathscr{M}(\mathcal{H}_{\neq}^2)$, $N_1, N_2 \in \mathscr{N}(\mathcal{H}_{\geq})$, $Z_1, Z_2 \in \mathscr{Z}(\mathcal{H}_{=})$ and $W \in \mathbf{K}[v]$, where $\mathcal{H} = [\mathcal{H}_{\neq}, \mathcal{H}_{\geq}, \mathcal{H}_{=}]$ is a system of sign conditions in $\mathbf{K}[v]$. If $e = 0$ we take (17) as the final incompatibility. If $e \neq 0$ we proceed as follows. We pass $W \cdot P$ to the right hand side in (18), we raise both sides to the $(2e)$-th power and we multiply the result by S_1. We obtain

$$S_1 \cdot S_2^{2e} + N_3 + Z_3 = S_1 \cdot W^{2e} \cdot P^{2e} \tag{19}$$

where $N_3 \in \mathscr{N}(\mathcal{H}_{\geq})$ is the sum of all the terms in the expansion of $S_1 \cdot (S_2 + N_2 + Z_2)^{2e}$ which do not involve Z_2 with the exception of the term $S_1 \cdot S_2^{2e}$ and $Z_3 \in \mathscr{Z}(\mathcal{H}_{=})$ is the sum of all the terms in the expansion of $S_1 \cdot (S_2 + N_2 + Z_2)^{2e}$ which involve Z_2. If W is the zero polynomial, we take (19) as the final incompatibility. Otherwise, we multiply (17) by W^{2e}, we substitute $S_1 \cdot W^{2e} \cdot P^{2e}$ using (19) and we obtain

$$S_1 \cdot S_2^{2e} + N_1 \cdot W^{2e} + N_3 + Z_1 \cdot W^{2e} + Z_3 = 0.$$

This proves the claim since $S_1 \cdot S_2^{2e} \in \mathscr{M}(\mathcal{H}_{\neq}^2)$, $N_1 \cdot W^{2e} + N_3 \in \mathscr{N}(\mathcal{H}_{\geq})$ and $Z_1 \cdot W^{2e} + Z_3 \in \mathscr{Z}(\mathcal{H}_{=})$. The degree bound follows easily. □

Lemma 2.1.17 *Let $P \in \mathbf{K}[u]$. Then*

$$P \neq 0 \quad \vdash \quad P > 0 \ \vee \ P < 0.$$

If we have initial incompatibilities in $\mathbf{K}[v]$ where $v \supset u$ with monoid part $S_1 \cdot P^{2e_1}$ and $S_2 \cdot P^{2e_2}$ and degree in $w \subset v$ bounded by $\delta_{w,1}$ and $\delta_{w,2}$, the final incompatibility has monoid part $S_1 \cdot S_2 \cdot P^{2(e_1+e_2)}$ and degree in w bounded by $\delta_{w,1} + \delta_{w,2}$.

Proof. Consider the initial incompatibilities

$$S_1 \cdot P^{2e_1} + N_1 + N_1' \cdot P + Z_1 = 0 \tag{20}$$

and

$$S_2 \cdot P^{2e_2} + N_2 - N_2' \cdot P + Z_2 = 0 \tag{21}$$

with $S_1, S_2 \in \mathscr{M}(\mathcal{H}_{\neq}^2)$, $N_1, N_1', N_2, N_2' \in \mathscr{N}(\mathcal{H}_{\geq})$ and $Z_1, Z_2 \in \mathscr{Z}(\mathcal{H}_{=})$, where $\mathcal{H} = [\mathcal{H}_{\neq}, \mathcal{H}_{\geq}, \mathcal{H}_{=}]$ is a system of sign conditions in $\mathbf{K}[v]$. We pass $N_1' \cdot P$ and $-N_2' \cdot P$ to the right hand side in (20) and (21), we multiply the results and we pass $-N_1' \cdot N_2' \cdot P^2$ to the left hand side. We obtain

$$S_1 \cdot S_2 \cdot P^{2(e_1+e_2)} + N_3 + N_1' \cdot N_2' \cdot P^2 + Z_3 = 0$$

where $N_3 = N_1 \cdot S_2 \cdot P^{2e_2} + N_2 \cdot S_1 \cdot P^{2e_1} + N_1 \cdot N_2$ and $Z_3 = Z_1 \cdot S_2 \cdot P^{2e_2} + Z_2 \cdot S_1 \cdot P^{2e_1} + Z_1 \cdot N_2 + Z_2 \cdot N_1 + Z_1 \cdot Z_2$. This proves the claim since $S_1 \cdot S_2 \cdot P^{2(e_1+e_2)} \in \mathscr{M}((\mathcal{H}_{\neq} \cup \{P\})^2)$, $N_3 + N_1' \cdot N_2' \cdot P^2 \in \mathscr{N}(\mathcal{H}_{\geq})$ and $Z_3 \in \mathscr{Z}(\mathcal{H}_{=})$. The degree bound follows easily. □

Lemma 2.1.18 *Let $P \in \mathbf{K}[u]$. Then*

$$\vdash \quad P > 0 \ \vee \ P < 0 \ \vee \ P = 0.$$

If we have initial incompatibilities in $\mathbf{K}[v]$ where $v \supset u$ with monoid part $S_1 \cdot P^{2e_1}, S_2 \cdot P^{2e_2}$ and S_3 and degree in $w \subset v$ bounded by $\delta_{w,1}$, $\delta_{w,2}$ and $\delta_{w,3}$, the final incompatibility has monoid part $S_1 \cdot S_2 \cdot S_3^{2(e_1+e_2)}$ and degree in w bounded by $\delta_{w,1} + \delta_{w,2} + 2(e_1+e_2)(\delta_{w,3} - \deg_w P)$.

Proof. Follows from Lemmas 2.1.16 and 2.1.17. □

Lemma 2.1.19 *Let $P_1, \dots, P_m \in \mathbf{K}[u]$. Then*

$$\vdash \quad \bigvee_{J \subset \{1,\dots,m\}} \Big(\bigwedge_{j \notin J} P_j \neq 0, \ \bigwedge_{j \in J} P_j = 0 \Big).$$

If we have initial incompatibilities in $\mathbf{K}[v]$ where $v \supset u$ with monoid part $S_J \cdot \prod_{j \notin J} P_j^{2e_{J,j}}$, degree in $w \subset v$ bounded by δ_w, and $e_{J,j} \leq e \in \mathbb{N}_*$, the final incompatibility has monoid part

$$\prod_{J \subset \{1,\dots,m\}} S_J^{e'_J}$$

with $e'_J \leq 2^{2^{m+1}-m-2} e^{2^m - 1}$ and degree in w bounded by $2^{2^{m+1}-2} e^{2^m-1} \delta_w$.

Proof. Easy to prove by induction on m using Lemma 2.1.16. □

Lemma 2.1.20 *Let $P_1, \dots, P_m \in \mathbf{K}[u]$. Then*

$$\bigwedge_{1 \leq j \leq m} P_j \neq 0 \quad \vdash \quad \bigvee_{J \subset \{1,\dots,m\}} \Big(\bigwedge_{j \in J} P_j > 0, \ \bigwedge_{j \notin J} P_j < 0 \Big).$$

If we have initial incompatibilities in $\mathbf{K}[v]$ where $v \supset u$ with monoid part $S_J \cdot \prod_j P_j^{2e_{J,j}}$, degree in $w \subset v$ bounded by δ_w, and $e_{J,j} \leq e \in \mathbb{N}$, the final incompatibility has monoid part

$$\prod_{J \subset \{1,\dots,m\}} S_J \cdot \prod_{1 \leq j \leq m} P_j^{2e'_j}$$

with $e'_J \leq 2^m e$ and degree in w bounded by $2^m \delta_w$.

Proof. Easy to prove by induction on m using Lemma 2.1.17. □

Lemma 2.1.21 *Let $P_1, \dots, P_m \in \mathbf{K}[u]$. Then*

$$\vdash \quad \bigvee_{\substack{J \subset \{1,\dots,m\} \\ J' \subset \{1,\dots,m\} \setminus J}} \Big(\bigwedge_{j \in J'} P_j > 0, \ \bigwedge_{j \notin J \cup J'} P_j < 0, \ \bigwedge_{j \in J} P_j = 0 \Big).$$

If we have initial incompatibilities in $\mathbf{K}[v]$ where $v \supset u$ with monoid part $S_{J,J'} \cdot \prod_{j \notin J} P_j^{2e_{J,J',j}}$, degree in $w \subset v$ bounded by δ_w, and $e_{J,J',j} \leq e \in \mathbb{N}_*$, the final incompatibility has monoid part

$$\prod_{\substack{J \subset \{1,\dots,m\} \\ J' \subset \{1,\dots,m\} \setminus J}} S_{J,J'}^{e'_{J,J'}}$$

with $e'_{J,J'} \leq 2^{2^{m+1}+m2^m-2m-2} e^{2^m-1}$ and degree in w bounded by $2^{2^{m+1}+m2^m-2} e^{2^m-1} \delta_w$.

Proof. Follows from Lemmas 2.1.19 and 2.1.20. □

2.2 Weak existence

Weak inferences are constructions to obtain new incompatibilities from other incompatibilities already known. It will be useful sometimes to introduce in the new incompatibilities, new sets of auxiliary variables. Weak existence is a generalization of weak inference which enables us to do so.

Definition 2.2.1 (Weak Existence) *Consider disjoint sets of variables* $u = (u_1, \dots, u_n)$, $t_0 = (t_{0,1}, \dots, t_{0,r_0})$, $t_1 = (t_{1,1}, \dots, t_{1,r_1}), \dots, t_m = (t_{m,1}, \dots, t_{m,r_m})$. *Let* $\mathcal{F}(t_0)$ *be a system of sign conditions in* $\mathbf{K}[u][t_0]$ *and* $\mathcal{F}_1(t_1) \dots, \mathcal{F}_m(t_m)$ *be systems of sign conditions in* $\mathbf{K}[u][t_1], \dots, \mathbf{K}[u][t_m]$. *A* weak existence

$$\exists t_0 \; [\; \mathcal{F}(t_0) \;] \quad \vdash \quad \bigvee_{1 \le j \le m} \exists t_j \; [\; \mathcal{F}_j(t_j) \;]$$

is a construction that, given any system of sign conditions $\mathcal{H}$ *in* $\mathbf{K}[v]$ *with* $v \supset u$, v *disjoint from* $t_0, t_1, \dots, t_m$, *and* initial *incompatibilities*

$$\downarrow \mathcal{F}_1(t_1),\ \mathcal{H}(v) \downarrow_{\mathbf{K}[v][t_1]}, \dots, \downarrow \mathcal{F}_m(t_m),\ \mathcal{H}(v) \downarrow_{\mathbf{K}[v][t_m]}$$

produces an incompatibility

$$\downarrow \mathcal{F}(t_0),\, \mathcal{H}(v) \downarrow_{\mathbf{K}[v][t_0]}$$

called the final *incompatibility.*

Note that the sets of variables $t_1, \dots, t_m$ which appear in the initial incompatibilities have been eliminated in the final incompatibility and also the set of variables t_0 which do not appear in the initial incompatibilities has been introduced in the final incompatibility.

Most of the times, it will not be the case that we want to introduce and eliminate sets of variables simultaneously. So, for instance, we write

$$\mathcal{F} \quad \vdash \quad \bigvee_{1 \le j \le m} \exists t_j \; [\; \mathcal{F}_j(t_j) \;]$$

for a weak existence in which the sets of variables $t_1, \dots, t_m$ have been eliminated but no new set of variables has been introduced. We also write

$$\exists t_0 \; [\; \mathcal{F}(t_0) \;] \quad \vdash \quad \bigvee_{1 \le j \le m} \mathcal{F}_j$$

for a weak existence in which no sets of variables have been eliminated but a new set of variables has been introduced.

We illustrate the concept of weak existence with a few lemmas. In general, we need to make a careful analysis of the degree bounds considering also the auxiliary variables.

Lemma 2.2.2 *Let* $P \in \mathbf{K}[u]$. *Then*

$$P \neq 0 \quad \vdash \quad \exists t \; [\; t \neq 0,\ P \cdot t = 1 \;].$$

Suppose we have an initial incompatibility in $\mathbf{K}[v][t]$ *where* $v \supset u$ *and* $t \notin v$, *with monoid part* $S \cdot t^{2e}$, *degree in* $w \subset v$ *bounded by* δ_w *and degree in* t *bounded by* δ_t. *Let* $\bar{\delta}_t$ *be the smallest even number greater than or equal to* δ_t. *Then, the final incompatibility has monoid part* $S \cdot P^{\bar{\delta}_t - 2e}$ *and degree in* w *bounded by* $\delta_w + \bar{\delta}_t \deg_w P$.

Proof. Consider the initial incompatibility in $\mathbf{K}[v][t]$

$$S \cdot t^{2e} + \sum_i \omega_i V_i^2(t) \cdot N_i + \sum_j W_j(t) \cdot Z_j + W(t) \cdot (P \cdot t - 1) = 0 \tag{22}$$

with $S \in \mathscr{M}(\mathcal{H}_{\neq}{}^2)$, $\omega_i \in \mathbf{K}$, $\omega_i > 0$, $V_i(t) \in \mathbf{K}[v][t]$ and $N_i \in \mathscr{M}(\mathcal{H}_{\geq})$ for every i, $W_j(t) \in \mathbf{K}[v][t]$ and $Z_j \in \mathcal{H}_=$ for every j and $W(t) \in \mathbf{K}[v][t]$, where $\mathcal{H} = [\mathcal{H}_{\neq}, \mathcal{H}_{\geq}, \mathcal{H}_=]$ is a system of sign conditions in $\mathbf{K}[v]$.

For every i, let V_{i0} be the remainder of $P^{\frac{1}{2}\bar{\delta}_t} \cdot V(t)$ in the division by $Pt - 1$ considering t as the main variable; note that $\deg_w V_{i0} \leq \deg_w V_i(t) + \frac{1}{2}\bar{\delta}_t \deg_w P$. Similarly, for every j, let W_{j0} be the remainder of $P^{\bar{\delta}_t} \cdot W_j(t)$ in the division by $Pt - 1$ considering t as the main variable; note that $\deg_w W_{j0} \leq \deg_w W_j(t) + \bar{\delta}_t \deg_w P$.

We multiply (22) by $P^{\bar{\delta}_t}$ and deduce that there exists $W'(t) \in \mathbf{K}[v][t]$ such that

$$S \cdot P^{\bar{\delta}_t - 2e} + \sum_i \omega_i V_{i0}^2 \cdot N_i + \sum_j W_{j0} \cdot Z_j + W'(t) \cdot (P \cdot t - 1) = 0.$$

Looking at the degree in t, we have that $W'(t)$ is the zero polynomial. This proves the claim since $S \cdot P^{\bar{\delta}_t - 2e} \in \mathscr{M}((\mathcal{H}_{\neq} \cup P)^2)$, $\sum \omega_i V_{i0}^2 \cdot N_i \in \mathscr{M}(\mathcal{H}_{\geq})$ and $\sum W_{j0} \cdot Z_j \in \mathcal{H}_=$. The degree bound follows easily. □

Lemma 2.2.3 *Let $P \in \mathbf{K}[u]$. Then*

$$P \geq 0 \quad \vdash \quad \exists t \; [\, t^2 = P \,].$$

If we have an initial incompatibility in $\mathbf{K}[v][t]$ where $v \supset u$ and $t \notin v$, with monoid part S, degree in $w \subset v$ bounded by δ_w and degree in t bounded by δ_t, the final incompatibility has the same monoid part and degree in w bounded by $\delta_w + \frac{1}{2}\delta_t \deg_w P$.

Proof. Consider the initial incompatibility in $\mathbf{K}[v][t]$

$$S + \sum_i \omega_i V_i^2(t) \cdot N_i + \sum_j W_j(t) \cdot Z_j + W(t) \cdot (t^2 - P) = 0 \tag{23}$$

with $S \in \mathscr{M}(\mathcal{H}_{\neq}^2)$, $\omega_i \in \mathbf{K}$, $\omega_i > 0$, $V_i(t) \in \mathbf{K}[v][t]$ and $N_i \in \mathscr{M}(\mathcal{H}_{\geq})$ for every i, $W_j(t) \in \mathbf{K}[v][t]$ and $Z_j \in \mathcal{H}_=$ for every j and $W(t) \in \mathbf{K}[v][t]$, where $\mathcal{H} = [\mathcal{H}_{\neq}, \mathcal{H}_{\geq}, \mathcal{H}_=]$ is a system of sign conditions in $\mathbf{K}[v]$.

For every i, let $V_{i1} \cdot t + V_{i0}$ be the remainder of $V_i(t)$ in the division by $t^2 - P$ considering t as the main variable; note that $\deg_w V_{i0} \leq \deg_w V_i(t) + \frac{1}{4}\delta_t \deg_w P$ and $\deg_w V_{i1} \leq \deg_w V_i(t) + \frac{1}{4}(\delta_t - 2) \deg_w P$. Similarly, for every j, let $W_{j1} \cdot t + W_{j0}$ be the remainder of $W_j(t)$ in the division by $t^2 - P$ considering t as the main variable; note that $\deg_w W_{j0} \leq \deg_w W_j(t) + \frac{1}{2}\delta_t \deg_w P$.

From (23) we deduce that exists $W'(t) \in \mathbf{K}[v][t]$ such that

$$S + \sum_i \omega_i (V_{i1} \cdot t + V_{i0})^2 \cdot N_i + \sum_j (W_{j1} \cdot t + W_{j0}) \cdot Z_j + W'(t) \cdot (t^2 - P) = 0.$$

We rewrite this equation as

$$S + \sum_i \omega_i (V_{i1}^2 \cdot P + V_{i0}^2) \cdot N_i + \sum_j W_{j0} \cdot Z_j + W''' \cdot t + W''(t) \cdot (t^2 - P) = 0.$$

for some $W''' \in \mathbf{K}[v]$ and $W''(t) \in \mathbf{K}[v][t]$.

Looking at the degrees in t, we have that $W''(t)$ is the zero polynomial; and looking again at the degree in t, we have that then also W''' is the zero polynomial. This proves the claim since $S \in \mathscr{M}(\mathcal{H}_{\neq}^2)$, $\sum \omega_i(V_{i1}^2 \cdot P + V_{i0}^2) \cdot N_i \in \mathscr{N}(\mathcal{H}_{\geq} \cup \{P\})$ and $\sum W_{j0} \cdot Z_j \in \mathscr{Z}(\mathcal{H}_{=})$. The degree bound follows easily. □

Lemma 2.2.4 *Let $P \in \mathbf{K}[u]$. Then*

$$P > 0 \quad \vdash \quad \exists t \; [\; t > 0, \; t^2 = P \;].$$

If we have an initial incompatibility in $\mathbf{K}[v][t]$ where $v \supset u$ and $t \notin v$, with monoid part $S \cdot t^{2e}$, degree in $w \subset v$ bounded by δ_w and degree in t bounded by δ_t, the final incompatibility has monoid part $S^2 \cdot P^{2e}$ and degree in w bounded by $2\delta_w + (\max\{1, 2e\} + \delta_t) \deg_w P$.

Proof. Consider the initial incompatibility in $\mathbf{K}[v][t]$

$$S \cdot t^{2e} + N_1(t) + N_2(t)t + Z(t) + W(t) \cdot (t^2 - P) = 0 \tag{24}$$

with $S \in \mathscr{M}(\mathcal{H}_{\neq}^2)$, $N_1(t), N_2(t) \in \mathscr{N}(\mathcal{H}_{\geq})_{\mathbf{K}[v][t]}$, $Z(t) \in \mathscr{Z}(\mathcal{H}_{=})_{\mathbf{K}[v][t]}$ and $W(t) \in \mathbf{K}[v][t]$, where $\mathcal{H}$ is a system of sign conditions in $\mathbf{K}[v]$.

We substitute $t = -t$ in (24) and we obtain

$$\downarrow \; t < 0, \; t^2 = P, \; \mathcal{H} \; \downarrow_{\mathbf{K}[v][t]} \tag{25}$$

with the same monoid part and degree bounds.

Then we apply to (24) and (25) the weak inference

$$t \neq 0 \quad \vdash \quad t > 0 \;\vee\; t < 0.$$

By Lemma 2.1.17, we obtain

$$\downarrow \; t \neq 0, \; t^2 = P, \; \mathcal{H} \; \downarrow_{\mathbf{K}[v][t]}$$

with monoid part $S^2 \cdot t^{4e}$, degree in w bounded by $2\delta_w$ and degree in t bounded by $2\delta_t$. Since the exponent of t in the monoid part is a multiple of 4, this incompatibility is also an incompatibility

$$\downarrow \; t^2 > 0, \; t^2 = P, \; \mathcal{H} \; \downarrow_{\mathbf{K}[v][t]} . \tag{26}$$

Then we apply to (26) the weak inference

$$P > 0, \; t^2 = P \quad \vdash \quad t^2 > 0.$$

By Lemma 2.1.7, we obtain

$$\downarrow \; P > 0, \; t^2 = P, \; \mathcal{H} \; \downarrow_{\mathbf{K}[v][t]} \tag{27}$$

with monoid part $S^2 \cdot P^{2e}$, degree in w bounded by $2\delta_w + \max\{1, 2e\} \deg_w P$ and degree in t bounded by $2\delta_t$.

Finally we apply to (27) the weak inference

$$P \geq 0 \quad \vdash \quad \exists t \; [\; t^2 = P \;].$$

By Lemma 2.2.3, we obtain

$$\downarrow P > 0,\ \mathcal{H} \downarrow_{\mathbf{K}[v]}$$

with the same monoid part and degree in w bounded by $2\delta_w + (\max\{1, 2e\} + \delta_t) \deg_w P$, which serves as the final incompatibility. □

Remark 2.2.5 *In the preceeding lemmas, we have no case of a weak existence with an existential variable to the left. The first example of such a situation appears later in the paper, when we deal with the Intermediate Value Theorem in Section 3.*

2.3 Complex numbers

We introduce the conventions we follow to deal with complex variables in the context of weak inference, which has been originally defined to be well adapted to a real setting.

Notation 2.3.1 (Complex Variables) *A complex variable, always named z, represents two variables corresponding to its real and imaginary parts, always named a and b, so that $z = a+ib$. We also use z to denote a set of complex variables and a and b to denote the set of real and imaginary parts of z.*

Let $z = (z_1, \dots, z_n)$ and $P \in \mathbf{K}[i][u][z]$. We denote by $P_{\mathrm{Re}} \in \mathbf{K}[u][a, b]$ and $P_{\mathrm{Im}} \in \mathbf{K}[u][a, b]$ the real and imaginary parts of P. The expression $P = 0$ is an abbreviation for

$$P_{\mathrm{Re}} = 0,\ P_{\mathrm{Im}} = 0,$$

and the expression $P \neq 0$ is an abbreviation for

$$P_{\mathrm{Re}}^2 + P_{\mathrm{Im}}^2 \neq 0.$$

We illustrate the use of complex variables with some lemmas.

Lemma 2.3.2 *Let $C, D \in \mathbf{K}[u]$. Then*

$$C + iD \neq 0 \quad \vdash \quad \exists z\ [\ z \neq 0,\ z^2 = C + iD\ ],$$

where z is a complex variable (using Notation 2.3.1) If we have an initial incompatibility in $\mathbf{K}[v][a, b]$ where $v \supset u$ and $a, b \notin v$, with monoid part $S\cdot(a^2+b^2)^{2e}$, degree in $w \subset v$ bounded by δ_w and degree in (a, b) bounded by δ_z, the final incompatibility has monoid part $S^4 \cdot (C^2 + D^2)^{2(2e+1)}$ and degree in w bounded by $4\delta_w + (20 + 24e + 8\delta_z) \max\{\deg_w C, \deg_w D\}$.

Proof. Consider the initial incompatibility in $\mathbf{K}[v][a, b]$

$$S \cdot (a^2 + b^2)^{2e} + N(a, b) + Z(a, b) + W_1(a, b) \cdot (a^2 - b^2 - C) + W_2(a, b) \cdot (2a \cdot b - D) = 0 \quad (28)$$

with $S \in \mathscr{M}(\mathcal{H}_{\neq}^2)$, $N(a, b) \in \mathscr{N}(\mathcal{H}_{\geq})_{\mathbf{K}[v][a,b]}$, $Z(a, b) \in \mathscr{Z}(\mathcal{H}_{=})_{\mathbf{K}[v][a,b]}$ and $W_1(a, b), W_2(a, b) \in \mathbf{K}[v][a, b]$, where $\mathcal{H}$ is a system of sign conditions in $\mathbf{K}[v]$.

We substitute $b = -b$ in (28) and we obtain

$$\downarrow z \neq 0,\ z^2 = C - iD,\ \mathcal{H} \downarrow_{\mathbf{K}[v][a,b]} \quad (29)$$

with the same monoid part and degree bounds.

Then we apply to (28) and (29) the weak inference

$$(2a \cdot b)^2 = D^2 \quad \vdash \quad 2a \cdot b = D \ \vee \ 2a \cdot b = -D.$$

By Lemma 2.1.12, we obtain

$$\downarrow z \neq 0,\ a^2 - b^2 = C,\ (2a \cdot b)^2 = D^2,\ \mathcal{H} \downarrow_{\mathbf{K}[v][a,b]} \tag{30}$$

with monoid part $S^2 \cdot (a^2 + b^2)^{4e}$, degree in w bounded by $2\delta_w$ and degree in (a, b) bounded by $2\delta_z$.

We consider a new auxiliary variable t. Taking into account the identities

$$\begin{array}{rcl} a^2 - b^2 - C & = & \Big(a^2 - \frac{1}{2}(t + C)\Big) - \Big(b^2 - \frac{1}{2}(t - C)\Big), \\ (2a \cdot b)^2 - D^2 & = & \Big(a^2 - \frac{1}{2}(t + C)\Big) \cdot 4b^2 + \Big(b^2 - \frac{1}{2}(t - C)\Big) \cdot 2(t + C) + (t^2 - C^2 - D^2), \end{array}$$

we apply to (30) the weak inference

$$a^2 = \frac{1}{2}(t + C),\ b^2 = \frac{1}{2}(t - C),\ t^2 = C^2 + D^2 \quad \vdash \quad a^2 - b^2 = C,\ (2a \cdot b)^2 = D^2.$$

By Lemma 2.1.8, we obtain

$$\Big\downarrow z \neq 0,\ a^2 = \frac{1}{2}(t + C),\ b^2 = \frac{1}{2}(t - C),\ t^2 = C^2 + D^2,\ \mathcal{H} \Big\downarrow_{\mathbf{K}[v][a,b,t]} \tag{31}$$

with monoid part $S^2 \cdot (a^2 + b^2)^{4e}$, degree in w bounded by $2\delta_w + 2\deg_w C$, degree in (a, b) bounded by $2\delta_z$ and degree in t bounded by 2.

Then we apply to (31) the weak inference

$$t \neq 0,\ a^2 = \frac{1}{2}(t + C),\ b^2 = \frac{1}{2}(t - C) \quad \vdash \quad z \neq 0.$$

By Lemma 2.1.6 we obtain

$$\Big\downarrow t \neq 0,\ a^2 = \frac{1}{2}(t + C),\ b^2 = \frac{1}{2}(t - C),\ t^2 = C^2 + D^2,\ \mathcal{H} \Big\downarrow_{\mathbf{K}[v][a,b,t]} \tag{32}$$

with monoid part $S^2 \cdot t^{4e}$, degree in w bounded by $2\delta_w + (2+4e)\deg_w C$, degree in (a, b) bounded by $2\delta_z$ and degree in t bounded by $2 + 4e$.

Then we successively apply to (32) the weak inferences

$$\begin{array}{rcl} t + C \geq 0 & \vdash & \exists a\ [\ a^2 = \frac{1}{2}(t + C)\ ], \\ t - C \geq 0 & \vdash & \exists b\ [\ b^2 = \frac{1}{2}(t - C)\ ]. \end{array}$$

By Lemma 2.2.3, we obtain

$$\downarrow t \neq 0,\ t + C \geq 0,\ t - C \geq 0,\ t^2 = C^2 + D^2,\ \mathcal{H} \downarrow_{\mathbf{K}[v][t]} \tag{33}$$

with monoid part $S^2 \cdot t^{4e}$, degree in w bounded by $2\delta_w + (2 + 4e + 2\delta_z) \deg_w C$, and degree in t bounded by $2 + 4e + 2\delta_z$.

Finally we successively apply to (33) the weak inferences

$$\begin{array}{rcl} t > 0,\ t^2 - C^2 \geq 0 & \vdash & t + C \geq 0,\ t - C \geq 0, \\ D^2 \geq 0,\ t^2 = C^2 + D^2 & \vdash & t^2 - C^2 \geq 0, \\ & \vdash & D^2 \geq 0, \\ C^2 + D^2 > 0 & \vdash & \exists t\ [\ t > 0,\ t^2 = C^2 + D^2\ ]. \end{array}$$

By Lemmas 2.1.11, 2.1.5 (item 15), 2.1.2 (item 3) and 2.2.4, we obtain an incompatibility in $\mathbf{K}[v]$

$$\downarrow C^2 + D^2 > 0,\ \mathcal{H} \downarrow_{\mathbf{K}[v]}$$

with monoid part $S^4 \cdot (C^2 + D^2)^{2(2e+1)}$ and degree in w bounded by $4\delta_w + (20 + 24e + 8\delta_z) \max\{\deg_w C, \deg_w D\}$. Note that this incompatibility is also an incompatibility

$$\downarrow C^2 + D^2 \neq 0,\ \mathcal{H} \downarrow_{\mathbf{K}[v]} \tag{34}$$

with the same degree bound, which serves as the final incompatibility. □

Lemma 2.3.3 *Let $C, D \in \mathbf{K}[u]$. Then*

$$\vdash \quad \exists z\ [\ z^2 = C + iD\ ],$$

where z is a complex variable (using Notation 2.3.1).

If we have an initial incompatibility in $\mathbf{K}[v][a, b]$ where $v \supset u$ and $a, b \notin v$, with monoid part S, degree in $w \subset v$ bounded by δ_w and degree in (a, b) bounded by δ_z, the final incompatibility has monoid part S^8 and degree in w bounded by $8\delta_w + (20 + 8\delta_z) \max\{\deg_w C, \deg_w D\}$.

Proof. Consider the initial incompatibility in $\mathbf{K}[v][a, b]$

$$S + N(a, b) + Z(a, b) + W_1(a, b) \cdot (a^2 - b^2 - C) + W_2(a, b)(2a \cdot b - D) = 0 \tag{35}$$

with $S \in \mathscr{M}(\mathcal{H}_{\neq}^2)$, $N(a, b) \in \mathscr{N}(\mathcal{H}_{\geq})_{\mathbf{K}[v][a,b]}$, $Z(a, b) \in \mathscr{Z}(\mathcal{H}_{=})_{\mathbf{K}[v][a,b]}$ and $W_1(a, b), W_2(a, b) \in \mathbf{K}[v][a, b]$, where $\mathcal{H}$ is a system of sign conditions in $\mathbf{K}[v]$.

We proceed by case by case reasoning. First we consider the case $C^2 + D^2 \neq 0$. We apply to (35) the weak inference

$$C^2 + D^2 \neq 0 \quad \vdash \quad \exists z\ [\ z \neq 0,\ z^2 = C + iD\ ].$$

By Lemma 2.3.2 we obtain

$$\downarrow C^2 + D^2 \neq 0,\ \mathcal{H} \downarrow_{\mathbf{K}[v]} \tag{36}$$

with monoid part $S^4 \cdot (C^2 + D^2)^2$ and degree in w bounded by $4\delta_w + (20 + 8\delta_z) \max\{\deg_w C, \deg_w D\}$.

We consider then the case $C^2 + D^2 = 0$. We evaluate $a = b = 0$ in (35) and we apply the weak inference

$$C^2 + D^2 = 0 \quad \vdash \quad C = 0,\ D = 0.$$

By Lemma 2.1.14, we obtain

$$\downarrow C^2 + D^2 = 0,\ \mathcal{H} \downarrow_{\mathbf{K}[v]} \tag{37}$$

with monoid part S^2 and degree in w bounded by $2\delta_w + 2\max\{\deg_w C, \deg_w D\}$.

Finally we apply to (36) and (37) the weak inference

$$\vdash \quad C^2 + D^2 \neq 0 \ \vee \ C^2 + D^2 = 0.$$

By Lemma 2.1.16, we obtain

$$\downarrow \mathcal{H} \downarrow_{\mathbf{K}[v]}$$

with monoid part S^8 and degree in w bounded by $8\delta_w + (20 + 8\delta_z)\max\{\deg_w C, \deg_w D\}$, which serves as the final incompatibility. □

Lemma 2.3.4 *Let $E = y^2 + G \cdot y + H \in \mathbf{K}[i][u][y]$. Then*

$$\vdash \quad \exists z\ [\ E(z) = 0\ ],$$

where z is a complex variable (using Notation 2.3.1).

If we have an initial incompatibility in $\mathbf{K}[v][a, b]$ where $v \supset u$ and $a, b \notin v$, with monoid part S, degree in $w \subset v$ bounded by δ_w and degree in (a, b) bounded by δ_z, the final incompatibility has monoid part S^8 and degree in w bounded by $8\delta_w + (40 + 24\delta_z)\max\{\deg_w G, \deg_w H\}$.

Proof. Consider the initial incompatibility in $\mathbf{K}[v][a, b]$

$$S + N(a, b) + Z(a, b) + W_1(a, b) \cdot E_{\mathrm{Re}}(a, b) + W_2(a, b) \cdot E_{\mathrm{Im}}(a, b) = 0 \tag{38}$$

with $S \in \mathscr{M}(\mathcal{H}^2_{\neq})$, $N(a, b) \in \mathscr{N}(\mathcal{H}_{\geq})_{\mathbf{K}[v][a,b]}$, $Z(a, b) \in \mathscr{Z}(\mathcal{H}_{=})_{\mathbf{K}[v][a,b]}$ and $W_1(a, b), W_2(a, b) \in \mathbf{K}[v][a, b]$, where $\mathcal{H}$ is a system of sign conditions in $\mathbf{K}[v]$.

Let $C = \frac{1}{4}G^2_{\mathrm{Re}} - \frac{1}{4}G^2_{\mathrm{Im}} - H_{\mathrm{Re}} \in \mathbf{K}[u]$ and $D = \frac{1}{2}G_{\mathrm{Re}}G_{\mathrm{Im}} - H_{\mathrm{Im}} \in \mathbf{K}[u]$. Then we have

$$\begin{aligned} E_{\mathrm{Re}}(a, b) &= a^2 - b^2 + G_{\mathrm{Re}} \cdot a - G_{\mathrm{Im}} \cdot b + H_{\mathrm{Re}} = \left(a + \tfrac{1}{2}G_{\mathrm{Re}}\right)^2 - \left(b + \tfrac{1}{2}G_{\mathrm{Im}}\right)^2 - C, \\ E_{\mathrm{Im}}(a, b) &= 2a \cdot b + G_{\mathrm{Im}} \cdot a + G_{\mathrm{Re}} \cdot b + H_{\mathrm{Im}} = 2\left(a + \tfrac{1}{2}G_{\mathrm{Re}}\right) \cdot \left(b + \tfrac{1}{2}G_{\mathrm{Im}}\right) - D. \end{aligned}$$

We substitute $a = a - \frac{1}{2}G_{\mathrm{Re}}$ and $b = b - \frac{1}{2}G_{\mathrm{Im}}$ in (38) and we obtain

$$\downarrow z^2 = C + iD,\ \mathcal{H} \downarrow_{\mathbf{K}[v][a,b]} \tag{39}$$

with monoid part S, degree in w bounded by $\delta_w + \delta_z \deg_w G$ and degree in (a, b) bounded by δ_z.

Finally we apply to (39) the weak inference

$$\vdash \quad \exists\, z\ [\ z^2 = C + iD\ ].$$

By Lemma 2.3.3, we obtain

$$\downarrow \mathcal{H} \downarrow_{\mathbf{K}[v]}$$

with monoid part S^8 and degree in w bounded by $8\delta_w + (40 + 24\delta_z)\max\{\deg_w G, \deg_w H\}$, which serves as the final incompatibility. □

2.4 Identical polynomials

We introduce the notation we use to deal with polynomial identities in the weak inference context.

Notation 2.4.1 (Identical Polynomials) *Let* $P = \sum_{0\le h\le p} C_h \cdot y^h, Q = \sum_{0\le h\le p} D_h \cdot y^h \in \mathbf{K}[u][y]$*. The expression* $P \equiv Q$ *is an abbreviation for*

$$\bigwedge_{0\le h\le p} C_h = D_h.$$

Note that $P \equiv Q$ is a conjunction of polynomial equalities in $\mathbf{K}[u]$.

We illustrate the use of this notation with a few lemmas.

Lemma 2.4.2 *Let* $P, Q \in \mathbf{K}[u][y]$ *with* $\deg_y P = \deg_y Q$*. Then*

$$P \equiv Q,\ Q > 0 \quad \vdash \quad P > 0.$$

If we have an initial incompatibility in $\mathbf{K}[v]$ *where* $v \supset (u, y)$*, with monoid part* $S \cdot P^{2e}$ *and degree in* $w \subset v$ *bounded by* δ_w*, the final incompatibility has monoid part* $S \cdot Q^{2e}$ *and degree in* w *bounded by*

$$\delta_w + \max\{1, 2e\}\big(\max\{\deg_w P, \deg_w Q\} - \deg_w P\big).$$

Proof. Follows from Lemmas 2.1.2 (item 5) and 2.1.7. □

Lemma 2.4.3 *Let* $P \in \mathbf{K}[u][y]$ *with* $\deg_y P \ge 2$*. Then*

$$P(t_1) = 0,\ \mathrm{Quot}(P, y - t_1)(t_2) = 0 \quad \vdash \quad P \equiv (y - t_1) \cdot (y - t_2) \cdot \mathrm{Quot}(P, (y - t_1)(y - t_2)).$$

If we have an initial incompatibility in $\mathbf{K}[v]$ *where* $v \supset (u, t_1, t_2)$ *with monoid part* S *and degree in* $w \subset v$ *bounded by* δ_w*, the final incompatibility has the same monoid part and degree in* w *bounded by*

$$\delta_w + \max\{\deg_w(t_1 \cdot \mathrm{Quot}(P, y - t_1)(t_2)), \deg_w P(t_1)\} - \deg_w(-t_1 \cdot \mathrm{Quot}(P, y - t_1)(t_2) + P(t_1)).$$

Proof. Because of the identity in $\mathbf{K}[u][t_1, t_2, y]$

$$P = (y-t_1)\cdot(y-t_2)\cdot\mathrm{Quot}(P, (y-t_1)(y-t_2)) + \mathrm{Quot}(P, y-t_1)(t_2)\cdot y - t_1\cdot\mathrm{Quot}(P, y-t_1)(t_2) + P(t_1),$$

the lemma follows from Lemma 2.1.8. □

Lemma 2.4.4 *Let* $P \in \mathbf{K}[u][y]$ *with* $\deg_y P \ge 2$*. Then*

$$P(z) = 0,\ b \ne 0 \quad \vdash \quad P \equiv ((y - a)^2 + b^2) \cdot \mathrm{Quot}(P, (y - a)^2 + b^2).$$

If we have an initial incompatibility in $\mathbf{K}[v]$ *where* $v \supset (u, a, b)$ *with monoid part* S *and degree in* $w \subset v$ *bounded by* δ_w*, the final incompatibility has monoid part* $S \cdot b^2$ *and degree in* w *bounded by* $\delta_w + \deg_w b^2 + \deg_w P$*.*

Proof. Because of the identity in $\mathbf{K}[u][a,b,y]$

$$P = ((y-a)^2+b^2)\cdot \mathrm{Quot}(P,(y-a)^2+b^2) + \frac{P_{\mathrm{Im}}(a,b)}{b}y + \frac{bP_{\mathrm{Re}}(a,b) - a\cdot P_{\mathrm{Im}}(a,b)}{b},$$

the initial incompatibility is of type

$$S + N + Z + W_1\frac{P_{\mathrm{Im}}(a,b)}{b} + W_2\frac{b\cdot P_{\mathrm{Re}}(a,b) - a\cdot P_{\mathrm{Im}}(a,b)}{b} = 0 \tag{40}$$

with $S \in \mathscr{M}(\mathcal{H}_{\neq}^2)$, $N \in \mathscr{N}(\mathcal{H}_{\geq})$, $Z \in \mathscr{Z}(\mathcal{H}_{=})$ and $W_1, W_2 \in \mathbf{K}[v]$, where $\mathcal{H}$ is a system of sign conditions in $\mathbf{K}[v]$.

We multiply (40) by b^2 and we obtain an incompatibility

$$\downarrow b \neq 0,\ b\cdot P_{\mathrm{Im}}(a,b) = 0,\ b^2\cdot P_{\mathrm{Re}}(a,b) - a\cdot b\cdot P_{\mathrm{Im}}(a,b) = 0,\ \mathcal{H} \downarrow_{\mathbf{K}[v]} \tag{41}$$

with monoid part $S\cdot b^2$ and degree in w bounded by $\delta_w + \deg_w b^2$.

Finally we apply to (41) the weak inference

$$P(z) = 0 \quad \vdash \quad b\cdot P_{\mathrm{Im}}(a,b) = 0,\ b^2\cdot P_{\mathrm{Re}}(a,b) - a\cdot b\cdot P_{\mathrm{Im}}(a,b) = 0.$$

By Lemma 2.1.8, we obtain an incompatibility

$$\downarrow P(z) = 0,\ b \neq 0,\ \mathcal{H} \downarrow_{\mathbf{K}[v]}$$

with the same monoid part and, after some analysis, degree in w bounded by $\delta_2 + \deg_w b^2 + \deg_w P$, which serves as the final incompatibility. $\square$

Notation 2.4.5 *We denote*

$$\mathrm{R}(z,z') = \mathrm{Res}_y((y-a)^2+b^2,(y-a')^2+b'^2)$$

where Res_y *is the resultant polynomial in the variable* y*. Note that*

$$\mathrm{R}(z,z') = ((a-a')^2+(b-b')^2)\cdot((a-a')^2+(b+b')^2).$$

Lemma 2.4.6

$$\mathrm{R}(z,z') = 0 \quad \vdash \quad (y-a)^2+b^2 \equiv (y-a')^2+b'^2.$$

If we have an initial incompatibility in $\mathbf{K}[v]$ *where* $v \supset (a,b,a',b')$ *with monoid part* S *and degree in* $w \subset v$ *bounded by* δ_w*, the final incompatibility has monoid part* S^4 *and degree in* w *bounded by*

$$4\Big(\delta_w + \max\{\deg_w a-a', \deg_w b-b'\} - \min\{\deg_w a-a', \deg_w b-b'\}\Big).$$

Proof. Consider the initial incompatibility

$$\Big\downarrow\ a-a' = 0,\ a^2+b^2-a'^2-b'^2 = 0,\ \mathcal{H}\ \Big\downarrow_{\mathbf{K}[v]} \tag{42}$$

where $\mathcal{H}$ is a system of sign conditions in $\mathbf{K}[v]$. On the one hand, we successively apply to (42) the weak inferences

$$\begin{array}{rcl} a^2 - a'^2 = 0,\ b^2 - b'^2 = 0 & \vdash & a^2 + b^2 - a'^2 - b'^2 = 0, \\ a - a' = 0 & \vdash & a^2 - a'^2 = 0, \\ b - b' = 0 & \vdash & b^2 - b'^2 = 0, \\ (a - a')^2 + (b - b')^2 = 0 & \vdash & a - a' = 0,\ b - b' = 0. \end{array}$$

By Lemmas 2.1.5 (item 14), 2.1.2 (item 5) and 2.1.14 we obtain an incompatibility

$$\downarrow\ (a - a')^2 + (b - b')^2 = 0,\ \mathcal{H} \downarrow_{\mathbf{K}[v]} \tag{43}$$

with monoid part S^2 and degree in w bounded by $2(\delta_w + \max\{\deg_w a - a', \deg_w b - b'\} - \min\{\deg_w a - a', \deg_w b - b'\})$. On the other hand, in a similar way we obtain from (42) an incompatibility

$$\downarrow\ (a - a')^2 + (b + b')^2 = 0,\ \mathcal{H} \downarrow_{\mathbf{K}[v]} \tag{44}$$

with the same monoid part and degree bound. Since

$$\mathrm{R}(z, z') = ((a - a')^2 + (b - b')^2) \cdot ((a - a')^2 + (b + b')^2),$$

the proof is finished by applying to (43) and (44) the weak inference

$$\mathrm{R}(z, z') = 0 \quad \vdash \quad (a - a')^2 + (b - b')^2 = 0 \ \vee \ (a - a')^2 + (b + b')^2 = 0.$$

By Lemma 2.1.12, we obtain an incompatibility

$$\downarrow\ \mathrm{R}(z, z') = 0,\ \mathcal{H} \downarrow_{\mathbf{K}[v]}$$

with monoid part S^4 and degree in w bounded by

$$4\Big(\delta_w + \max\{\deg_w a - a', \deg_w b - b'\} - \min\{\deg_w a - a', \deg_w b - b'\}\Big),$$

which serves as the final incompatibility. □

2.5 Matrices

We introduce the notation we use to deal with matrix identities in the context of weak inference.

Notation 2.5.1 (Identical Matrices) *Let* $\boldsymbol{A} = (A_{ij})_{1 \le i,j \le p}$, $\boldsymbol{B} = (B_{ij})_{1 \le i,j \le p} \in \mathbf{K}[u]^{p \times p}$. *The expression* $\boldsymbol{A} \equiv \boldsymbol{B}$ *is an abbreviation for*

$$\bigwedge_{\substack{1 \le i \le p, \\ 1 \le j \le p}} A_{ij} = B_{ij}.$$

We denote by $\mathbf{0}$ *the matrix with all its entries equal to* 0.

We illustrate the use of this notation with two lemmas.

Lemma 2.5.2 *Let* $\boldsymbol{A}, \boldsymbol{B} \in \mathbf{K}[u]^{p\times p}$*. Then*

$$\boldsymbol{A} \equiv \mathbf{0},\ \ \boldsymbol{B} \equiv \mathbf{0} \quad \vdash \quad \boldsymbol{A} + \boldsymbol{B} \equiv \mathbf{0}.$$

If we have an initial incompatibility in $\mathbf{K}[v]$ *where* $v \supset u$ *with monoid part* S *and degree in* $w \subset v$ *bounded by* δ_w*, the final incompatibility has the same monoid part and degree in* w *bounded by*

$$\delta_w + \max\{\max\{\deg_w A_{ij}, \deg_w B_{ij}\} - \deg_w A_{ij} + B_{ij} \,|\, 1 \le i \le p,\, 1 \le j \le p\}.$$

Proof. Follows from Lemma 2.1.8. □

Lemma 2.5.3 *Let* $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C} \in \mathbf{K}[u]^{p\times p}$*. Then*

$$\boldsymbol{A} \equiv \mathbf{0} \quad \vdash \quad \boldsymbol{B} \cdot \boldsymbol{A} \cdot \boldsymbol{C} \equiv \mathbf{0}.$$

If we have an initial incompatibility in $\mathbf{K}[v]$ *where* $v \supset u$ *with monoid part* S *and degree in* $w \subset v$ *bounded by* δ_w*, the final incompatibility has the same monoid part and degree in* w *bounded by* $\delta_w + \deg_w \boldsymbol{B} + \deg_w \boldsymbol{A} + \deg_w \boldsymbol{C}$*.*

Proof. Follows from Lemma 2.1.8. □

3 Intermediate Value Theorem

In this section we prove a weak existence version of the Intermediate Value Theorem for polynomials (Theorem 3.1.3) and we apply it to prove the weak existence of a real root for a polynomial of odd degree (Theorem 3.2.1).

The only result extracted from Section 3 used in the rest of the paper is the last result of the section, which is Theorem 3.2.1 (Real Root of an Odd Degree Polynomial as a weak existence), and is used three times in Section 4.

3.1 Intermediate Value Theorem

We define the following auxiliary function, which plays a key role in the estimates of the growth of degrees in the construction of incompatibilities related to the Intermediate Value Theorem.

Definition 3.1.1 *Let* $\mathrm{g}_1 : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$,

$$\mathrm{g}_1\{k,p\} = 2^{3\cdot 2^k} p^{k+1}.$$

We extend the definition of g_1 *with* $\mathrm{g}_1\{-1,0\} = 2$.

Technical Lemma 3.1.2 *For every* $(k,p) \in \mathbb{N} \times \mathbb{N}$,

$$4p\mathrm{g}_1\{k-1,k\}\mathrm{g}_1\{k,p\} \leq \mathrm{g}_1\{k+1,p\}.$$

Proof. Easy. □

Theorem 3.1.3 (Intermediate Value Theorem as a weak existence) *Let* $P = \sum_{0\leq h\leq p} C_h \cdot y^h \in \mathbf{K}[u][y]$. *Then*

$$\exists(t_1,t_2)\ [\ C_p \neq 0,\ P(t_1)\cdot P(t_2) \leq 0\ ] \quad \vdash \quad \exists t\ [\ P(t) = 0\ ].$$

If we have an initial incompatibility in $\mathbf{K}[v][t]$ *where* $v \supset u$ *and* $t, t_1, t_2 \notin v$, *with monoid part* S, *degree in* $w \subset v$ *bounded by* δ_w *and degree in* t *bounded by* δ_t, *the final incompatibility has monoid part* $S^e \cdot C_p^{2f}$ *with* $e \leq \mathrm{g}_1\{p-1,p\}$, $f \leq \mathrm{g}_1\{p-1,p\}\delta_t$, *degree in* w *bounded by* $\mathrm{g}_1\{p-1,p\}(\delta_w + \delta_t \deg_w P)$ *and the degree in* (t_1,t_2) *bounded by* $\mathrm{g}_1\{p-1,p\}\delta_t$.

Note that the degree estimates obtained are doubly exponential in the degree of P with respect to y.

The proof is based on an induction on the degree of P with respect to y, which is an adaptation of the proof by Artin [1] that if a field is real (i.e. -1 is not a sum of squares) its extension by an irreducible polynomial of odd degree is also real.

Proof: Consider the initial incompatibility in $\mathbf{K}[v][t]$

$$S + \sum_i \omega_i V_i^2(t)\cdot N_i + \sum_j W_j(t)\cdot Z_j + Q(t)\cdot P(t) = 0 \tag{1}$$

with $S \in \mathscr{M}(\mathcal{H}_{\neq}^2)$, $\omega_i \in \mathbf{K}, \omega_i > 0$, $V_i(t) \in \mathbf{K}[v][t]$ and $N_i \in \mathscr{M}(\mathcal{H}_{\geq})$ for every i, $W_j(t) \in \mathbf{K}[v][t]$ and $Z_j \in \mathcal{H}_=$ for every j and $Q(t) \in \mathbf{K}[v][t]$, where $\mathcal{H} = [\mathcal{H}_{\neq}, \mathcal{H}_{\geq}, \mathcal{H}_=]$ is a system of sign conditions in $\mathbf{K}[v]$.

The proof proceeds by induction on p. For $p = 0$, $P(t) = C_0$ and $P(t_1) \cdot P(t_2) = C_0^2$. We evaluate $t = 0$ in (1), we pass the term $Q(0) \cdot C_0$ to the right hand side, we square both sides and we pass $Q^2(0) \cdot C_0^2$ back to the left hand side. We take the result as the final incompatibility.

Suppose now $p \geq 1$. If $Q(t)$ is the zero polynomial, we evaluate $t = 0$ in (1) and we take the result as the final incompatibility. From now, we suppose that $Q(t)$ is not the zero polynomial and therefore, $\delta_t \geq p$. We denote by $\bar{\delta}_t$ the smallest even number greater than or equal to δ_t. For every i, let $\tilde{V}_i(t) \in \mathbf{K}[v][t]$ be the remainder of $C_p^{\frac{1}{2}\bar{\delta}_t} \cdot V_i(t)$ in the division by $P(t)$ considering t as the main variable; then $\deg_w \tilde{V}_i(t) \leq \deg_w V_i(t) + \frac{1}{2}\bar{\delta}_t \deg_w P$. Similarly, for every j, let $\tilde{W}_j(t) \in \mathbf{K}[v][t]$ be the remainder of $C_p^{\bar{\delta}_t} \cdot W_j(t)$ in the division by $P(t)$ considering t as the main variable; then $\deg_w \tilde{W}_j(t) \leq \deg_w W_j(t) + \bar{\delta}_t \deg_w P$.

We multiply (1) by $C_p^{\bar{\delta}_t}$ and we deduce that exists $Q'(t) \in \mathbf{K}[v][t]$ such that

$$S \cdot C_p^{\bar{\delta}_t} + \sum_i \omega_i \tilde{V}_i^2(t) \cdot N_i + \sum_j \tilde{W}_j(t) \cdot Z_j + Q'(t) \cdot P(t) = 0. \qquad (2)$$

Since the degree in w of $S \cdot C_p^{\bar{\delta}_t}$, $\tilde{V}_i^2(t) \cdot N_i$ for every i and $\tilde{W}_j(t) \cdot Z_j$ for every j is bounded by $\delta_w + \bar{\delta}_t \deg_w P$, the degree in w of $Q'(t) \cdot P(t)$ is also bounded by the same quantity.

If $Q'(t)$ is the zero polynomial, we evaluate $t = 0$ in (2) and take the result as the final incompatibility. In particular, for $p = 1$, $\deg_t \tilde{V}_i(t) = 0$ for every i and $\deg_t \tilde{W}_i(t) = 0$ for every j; looking at the degree in t in (2), we deduce that $Q'(t)$ is the zero polynomial and we are done.

From now on, we suppose $p \geq 2$ and that $Q'(t)$ is not the zero polynomial. Let $q = \deg_t \tilde{Q}'(t)$; looking again at the degree in t in (2) we have $q \leq p - 2$. Let $Q'(t) = \sum_{0 \leq \ell \leq q} D_\ell \cdot t^\ell$ and, for $0 \leq k \leq q+1$, $Q'_{k-1}(t) = \sum_{0 \leq \ell \leq k-1} D_\ell \cdot t^\ell$. We will prove, by a new induction on k, that for $0 \leq k \leq q+1$, we have

$$\downarrow \; C_p \neq 0, \; Q'_{k-1}(t_1) \cdot Q'_{k-1}(t_2) \leq 0, \; \bigwedge_{k \leq \ell \leq q} D_\ell = 0, \; \mathcal{H} \; \downarrow_{\mathbf{K}[v][t_1,t_2]}$$

of type

$$S^{e_k} \cdot C_p^{2f_k} + N_{k,1}(t_1,t_2) - N_{k,2}(t_1,t_2) \cdot Q'_{k-1}(t_1) \cdot Q'_{k-1}(t_2) + Z_k(t_1,t_2) + \sum_{k \leq \ell \leq q} D_\ell \cdot R_{k,\ell}(t_1,t_2) = 0 \quad (3)$$

with $N_{k,1}(t_1,t_2), N_{k,2}(t_1,t_2) \in \mathscr{N}(\mathcal{H}_{\geq})_{\mathbf{K}[v][t_1,t_2]}$, $Z_k(t_1,t_2) \in \mathscr{Z}(\mathcal{H}_=)_{\mathbf{K}[v][t_1,t_2]}$, $R_{k,\ell}(t_1,t_2) \in \mathbf{K}[v][t_1,t_2]$ for every ℓ, $e_k \leq \mathrm{g}_1\{k,p\} - 2$, $f_k \leq (\mathrm{g}_1\{k,p\} - 2)\delta_t$, degree in w bounded by $(\mathrm{g}_1\{k,p\} - 4)(\delta_w + \delta_t \deg_w P)$ and degree in (t_1,t_2) bounded by $(\mathrm{g}_1\{k,p\} - 4)\delta_t$.

For $k = 0$, we simply evaluate $t = 0$ in (2). Suppose now that we have an equation like (3) for some $0 \leq k \leq q$. We will obtain an equation like (3) for $k+1$.

- We rewrite (2) in this way:

$$S \cdot C_p^{\bar{\delta}_t} + \sum_i \omega_i \tilde{V}_i(t)^2 \cdot N_i + \sum_j \tilde{W}_j(t) \cdot Z_j + P(t) \cdot \sum_{k+1 \leq \ell \leq q} D_\ell \cdot t^\ell + P(t) \cdot Q'_k(t) = 0$$

to obtain

$$\Big\downarrow C_p \neq 0,\ \bigwedge_{k+1 \leq \ell \leq q} D_\ell = 0,\ Q'_k(t) = 0,\ \mathcal{H} \Big\downarrow_{\mathbf{K}[v][t]} \qquad (4)$$

with degree in w bounded by $\delta_w + \bar{\delta}_t \deg_w P$ and degree in t bounded by $2(p-1)$. Since $k < p$, by the inductive hypothesis on p, we have a procedure to obtain from (4) an incompatibility

$$\Big\downarrow C_p \neq 0,\ D_k \neq 0,\ Q'_k(t_1) \cdot Q'_k(t_2) \leq 0,\ \bigwedge_{k+1 \leq \ell \leq q} D_\ell = 0,\ \mathcal{H} \Big\downarrow_{\mathbf{K}[v][t_1,t_2]} \qquad (5)$$

with monoid part $S^{e'} \cdot C_p^{\bar{\delta}_t e'} \cdot D_k^{2f'}$ with $e' \leq \mathrm{g}_1\{k-1,k\}$, $f' \leq 2\mathrm{g}_1\{k-1,k\}(p-1)$, degree in w bounded by $\mathrm{g}_1\{k-1,k\}(\delta_w + \bar{\delta}_t \deg_w P + 2(p-1)(\delta_w + \bar{\delta}_t \deg_w P)) = \mathrm{g}_1\{k-1,k\}(2p-1)(\delta_w + \bar{\delta}_t \deg_w P)$ and degree in (t_1, t_2) bounded by $2\mathrm{g}_1\{k-1,k\}(p-1)$.

- On the other hand, we substitute

$$Q'_{k-1}(t_1) \cdot Q'_{k-1}(t_2) = Q'_k(t_2) \cdot Q'_k(t_2) + D_k \cdot \big(- t_1^k \cdot Q'_k(t_2) - t_2^k \cdot Q'_k(t_1) + D_k \cdot t_1^k \cdot t_2^k \big)$$

in (3) and we obtain

$$\Big\downarrow C_p \neq 0,\ Q'_k(t_1) \cdot Q'_k(t_2) \leq 0,\ \bigwedge_{k \leq \ell \leq q} D_\ell = 0,\ \mathcal{H} \Big\downarrow_{\mathbf{K}[v][t_1,t_2]} \qquad (6)$$

with monoid part $S^{e_k} \cdot C_p^{2f_k}$, degree in w bounded by $\mathrm{g}_1\{k,p\}(\delta_w + \delta_t \deg_w P)$ and degree in (t_1, t_2) bounded by $(\mathrm{g}_1\{k,p\} - 4)\delta_t + 2k$.

- Finally we apply to (5) and (6) the weak inference

$$\vdash \quad D_k \neq 0 \ \vee \ D_k = 0.$$

By Lemma 2.1.16, we obtain

$$\Big\downarrow C_p \neq 0,\ Q'_k(t_1) \cdot Q'_k(t_2) \leq 0,\ \bigwedge_{k+1 \leq \ell \leq q} D_\ell = 0,\ \mathcal{H} \Big\downarrow_{\mathbf{K}[v][t_1,t_2]}$$

with monoid part $S^{e_{k+1}} \cdot C_p^{2f_{k+1}}$ with $e_{k+1} = e' + 2e_k f'$ and $f_{k+1} = \frac{1}{2}\bar{\delta}_t e' + 2f_k f'$, degree in w bounded by $\mathrm{g}_1\{k-1,k\}(2p-1)(\delta_w + \bar{\delta}_t \deg_w P) + 2f'\mathrm{g}_1\{k,p\}(\delta_w + \delta_t \deg_w P)$ and degree in (t_1, t_2) bounded by $2\mathrm{g}_1\{k-1,k\}(p-1) + 2f'((\mathrm{g}_1\{k,p\} - 4)\delta_t + 2k)$. The bounds $e_{k+1} \leq \mathrm{g}_1\{k+1,p\} - 2$ and $f_{k+1} \leq (\mathrm{g}_1\{k+1,p\} - 2)\delta_t$ follow using Lemma 3.1.2 since

$$\mathrm{g}_1\{k-1,k\} + 4(\mathrm{g}_1\{k,p\} - 2)\mathrm{g}_1\{k-1,k\}(p-1) \leq 4p\mathrm{g}_1\{k-1,k\}\mathrm{g}_1\{k,p\} - 2 \leq \mathrm{g}_1\{k+1,p\} - 2.$$

The degree bounds also follow using Lemma 3.1.2 since

$$2\mathrm{g}_1\{k-1,k\}(2p-1) + 4\mathrm{g}_1\{k-1,k\}\mathrm{g}_1\{k,p\}(p-1) \leq 4p\mathrm{g}_1\{k-1,k\}\mathrm{g}_1\{k,p\} - 4 \leq \mathrm{g}_1\{k+1,p\} - 4$$

and

$$\begin{aligned} & 2\mathrm{g}_1\{k-1,k\}(p-1)+4\mathrm{g}_1\{k-1,k\}((\mathrm{g}_1\{k,p\}-4)\delta_t+2k)(p-1)\leq \\ \leq\ & (4p\mathrm{g}_1\{k-1,k\}\mathrm{g}_1\{k,p\}-4)\delta_t \leq \\ \leq\ & (\mathrm{g}_1\{k+1,p\}-4)\delta_t. \end{aligned}$$

So, for $k=q+1$, we have

$$S^{e_{q+1}}\cdot C_p^{2f_{q+1}}+N_{q+1,1}(t_1,t_2)+Z_{q+1}(t_1,t_2)=N_{q+1,2}(t_1,t_2)\cdot Q'(t_1)\cdot Q'(t_2). \quad (7)$$

On the other hand, substituting $t=t_1$ and $t=t_2$ in (2) we have

$$S\cdot C_p^{\bar{\delta}_t}+\sum_i \omega_i \tilde{V}_i(t_1)^2\cdot N_i+\sum_j \tilde{W}_j(t_1)\cdot Z_j=-Q'(t_1)\cdot P(t_1) \quad (8)$$

and

$$S\cdot C_p^{\bar{\delta}_t}+\sum_i \omega_i \tilde{V}_i(t_2)^2\cdot N_i+\sum_j \tilde{W}_j(t_2)\cdot Z_j=-Q'(t_2)\cdot P(t_2). \quad (9)$$

Multiplying (7), (8) and (9) and passing terms to the left hand side we obtain

$$S^{e_{q+1}+2}\cdot C_p^{2(f_{q+1}+\bar{\delta}_t)}+N(t_1,t_2)-N_{q+1,2}(t_1,t_2)\cdot {Q'}^2(t_1)\cdot {Q'}^2(t_2)\cdot P(t_2)\cdot P(t_2)+Z(t_1,t_2)=0 \quad (10)$$

for some $N(t_1,t_2)\in \mathscr{N}(\mathcal{H}_{\geq})_{\mathbf{K}[v][t_1,t_2]}$ and $Z(t_1,t_2)\in \mathscr{Z}(\mathcal{H}_{=})_{\mathbf{K}[v][t_1,t_2]}$. Equation (10) serves as the final incompatibility, taking into account that $e_{q+1}+2\leq \mathrm{g}_1\{q+1,p\}$, $f_{q+1}+\bar{\delta}_t\leq \mathrm{g}_1\{q+1,p\}\delta_t$, the degree in w is bounded by $(\mathrm{g}_1\{q+1,p\}-4)(\delta_w+\delta_t\deg_w P)+2(\delta_w+\bar{\delta}_t\deg_w P)\leq \mathrm{g}_1\{q+1,p\}(\delta_w+\delta_t\deg_w P)$, the degree in (t_1,t_2) is bounded by $(\mathrm{g}_1\{q+1,p\}-4)\delta_t+4p-4\leq \mathrm{g}_1\{q+1,p\}\delta_t$ and $\mathrm{g}_1\{q+1,p\}\leq \mathrm{g}_1\{p-1,p\}$. □

3.2 Real root of a polynomial of odd degree

Now we prove the weak existence of a real root for a monic polynomial of odd degree as a consequence of Theorem 3.1.3 (Intermediate Value Theorem as a weak existence).

Theorem 3.2.1 (Real Root of an Odd Degree Polynomial as a weak existence) *Let p be an odd number and $P=y^p+\sum_{0\leq h\leq p-1}C_h\cdot y^h\in \mathbf{K}[u][y]$. Then*

$$\vdash \quad \exists t\ [\ P(t)=0\ ].$$

If we have an initial incompatibility in $\mathbf{K}[v][t]$ where $v\supset u$ and $t\notin v$, with monoid part S, degree in $w\subset v$ bounded by δ_w and degree in t bounded by δ_t, the final incompatibility has monoid part S^e with $e\leq \mathrm{g}_1\{p-1,p\}$ and degree in w bounded by $3\mathrm{g}_1\{p-1,p\}(\delta_w+\delta_t\deg_w P)$ (see Definition 3.1.1).

To prove Theorem 3.2.1 we first give in Lemma 3.2.2, for a monic polynomial of odd degree, a real value where it is positive and a real value where it is negative. Then, we apply the weak existence version of the Intermediate Value Theorem from Theorem 3.1.3.

Lemma 3.2.2 *Let p be an odd number, $P = y^p + \sum_{0 \le h \le p-1} C_h \cdot y^h \in \mathbf{K}[u][y]$ and $E = p + \sum_{0 \le h \le p-1} C_h^2 \in \mathbf{K}[u]$. Then both $P(E)$ and $-P(-E)$ are sums of squares in $\mathbf{K}[u]$ multiplied by elements in $\mathbf{K}_+$ plus an element in $\mathbf{K}_+$.*

Proof. We only prove the claim for $P(E)$ and the respective claim for $-P(-E)$ follows by considering the polynomial $-P(-y)$.

We consider the Horner polynomials of P, $\mathrm{Hor}_0(P) = 1$, $\mathrm{Hor}_i(P) = C_{p-i} + y \cdot \mathrm{Hor}_{i-1}(P)$ for $1 \le i \le p$. We will prove by induction on i that for $1 \le i \le p$,

$$\mathrm{Hor}_i(P)(E) = p - i + \sum_{0 \le h \le p-i-1} C_h^2 + N_i + \omega_i \tag{11}$$

with $N_i \in \mathscr{N}(\emptyset)$ and ω_i in $\mathbf{K}_+$.

For $i = 1$ we have

$$\mathrm{Hor}_1(P)(E) = C_{p-1} + p + \sum_{0 \le h \le p-1} C_h^2 = p - 1 + \sum_{0 \le h \le p-2} C_h^2 + \Big(C_{p-1} + \frac{1}{2}\Big)^2 + \frac{3}{4}.$$

Suppose now that we have an equation like (11) for some $1 \le i-1 \le p-1$. Then we have

$$\begin{aligned} \mathrm{Hor}_i(P)(E) &= C_{p-i} + \Big(p + \textstyle\sum_{0 \le h \le p} C_h^2\Big) \cdot \Big(p - i + 1 + \textstyle\sum_{0 \le h \le p-i} C_h^2 + N_{i-1} + \omega_{i-1}\Big) = \\ &= p - i + \textstyle\sum_{0 \le h \le p-i-1} C_h^2 + N_i + \omega_i \end{aligned}$$

by taking

$$N_i = \Big(p - 1 + \sum_{0 \le h \le p} C_h^2\Big) \cdot \Big(p - i + 1 + \sum_{0 \le h \le p-i} C_h^2 + N_{i-1} + \omega_{i-1}\Big) + N_{i-1} + \Big(C_{p-i} + \frac{1}{2}\Big)^2$$

and $\omega_i = \omega_{i-1} + \frac{3}{4}$.

Finally, since $\mathrm{Hor}_p(P) = P$, the claim follows by considering equation (11) for $i = p$. □

Proof of Theorem 3.2.1: We apply to the initial incompatibility the weak inference

$$\exists (t_1, t_2)\ [\ P(t_1) \cdot P(t_2) \le 0\ ] \quad \vdash \quad \exists t\ [\ P(t) = 0\ ].$$

By Theorem 3.1.3 (Intermediate Value Theorem as a weak existence), we obtain an incompatibility with monoid part S^e with $e \le \mathrm{g}_1\{p-1, p\}$, degree in w bounded by $\mathrm{g}_1\{p-1, p\}(\delta_w + \delta_t \deg_w P)$ and degree in (t_1, t_2) bounded by $\mathrm{g}_1\{p-1, p\}\delta_t$. Then we simply substitute $t_1 = E$ and $t_2 = -E$ where E is defined as in Lemma 3.2.2. The degree bound follows easily. □

4 Fundamental Theorem of Algebra

In this section, we follow the approach of a famous algebraic proof of the Fundamental Theorem of Algebra due to Laplace to give a weak existence form of this theorem (Theorem 4.1.8). This approach is based on an induction on the power of 2 appearing in the degree of the polynomial, the base case being the case of polynomials of odd degree.

We then apply Theorem 4.1.8 to obtain a weak disjunction of the possible decompositions of a polynomial into irreducible real factors according to the number of real and complex roots (Theorem 4.2.4). Finally we obtain a weak disjunction of the possible decompositions of a polynomial into irreducible real factors taking into account multiplicities (Theorem 4.3.5).

Apart from many results from Section 2, the only result from Section 3 used in this section is Theorem 3.2.1 (Real Root of an Odd Degree Polynomial as a weak existence), and it is used once in the base case of the induction in the proof of Theorem 4.1.8 (Fundamental Theorem of Algebra as a weak existence), once in the proof of Lemma 4.2.1 and once in the proof of Theorem 4.2.4 (Real Irreducible Factors as a weak existence).

On the other hand, the only result extracted from Section 4 used in the rest of the paper is Theorem 4.3.5 (Real Irreducible Factors with Multiplicities as a weak existence), which is used only once in Section 6.

4.1 Fundamental Theorem of Algebra

In order to prove a weak existence version of the Fundamental Theorem of Algebra in Theorem 4.1.8, we need some auxiliary notation, definitions and results.

Notation 4.1.1 *For $p \in \mathbb{N}_*$, we denote by $\mathrm{r}\{p\}$ the biggest nonnegative integer r such that 2^r divides p and by $\mathrm{n}\{p\}$ the combinatorial number $\binom{p}{2}$.*

Laplace's proof of the Fundamental Theorem of Algebra [37] is very well known (see for example [3]). It is based on an inductive reasoning on $\mathrm{r}\{p\}$, where p is the degree of the polynomial $P \in \mathbf{R}[y]$ for which the existence of a complex root is being proved. The result is true for a polynomials of odd degree for which $\mathrm{r}\{p\} = 0$. An auxiliary polynomial of degree $\mathrm{n}\{p\}$ is constructed, and has a complex root by induction, taking into account that $\mathrm{r}\{\mathrm{n}\{p\}\} = \mathrm{r}\{p\} - 1$. A complex root of P is then produced by solving a quadratic equation.

Following Laplace's approach, we define auxiliary polynomials.

Definition 4.1.2 *Let $p \geq 1$, $c = (c_0, \ldots, c_{p-1})$, $y' = (y'_0, \ldots, y'_{\mathrm{n}\{p\}})$ and $y'' = (y''_{0,1}, \ldots, y''_{0,\mathrm{n}\{p\}}, y''_{1,2}, \ldots, y''_{1,\mathrm{n}\{p\}}, \ldots, y''_{\mathrm{n}\{p\}-1,\mathrm{n}\{p\}})$ be sets of variables. We denote by $\overline{\mathbf{K}(c)}$ the algebraic closure of $\mathbf{K}(c)$. We consider*

- $P = y^p + \sum_{0 \leq h \leq p-1} c_h \cdot y^h \in \mathbf{K}[c][y]$,
- *for* $0 \leq k \leq \mathrm{n}\{p\}$,

$$Q_k = \prod_{1 \leq i < j \leq p} (y'_k - k(t_i + t_j) - t_i t_j) \in \mathbf{K}[c][y'_k]$$

where $t_1, \ldots, t_p \in \overline{\mathbf{K}(c)}$ are the roots of P considering y as the main variable,

- *for* $0 \le k < \ell \le \mathrm{n}\{p\}$,

$$R_{k,\ell} = {y''_{k,\ell}}^2 - \frac{y'_\ell - y'_k}{\ell - k} y''_{k,\ell} + \frac{\ell y'_k - k y'_\ell}{\ell - k} \in \mathbf{K}[y'_k, y'_\ell, y''_{k,\ell}].$$

Remark 4.1.3 *For* $0 \le k \le \mathrm{n}\{p\}$, $p-1$ *of the factors in the definition of* Q_k *have degree in* t_1 *equal to* 1 *and the remaining factors have degree in* t_1 *equal to* 0. *From this, it can be deduced that* $\deg_c Q_k \le p-1$ *and also that* $\deg_{(c,y'_k)} Q_k = \mathrm{n}\{p\}$ *(see [4, Section 2.1]).*

Lemma 4.1.4 *We denote by* $\overline{\mathbf{K}}$ *the algebraic closure of* $\mathbf{K}$. *For any* $\gamma \in \overline{\mathbf{K}}^p$, $\psi' \in \overline{\mathbf{K}}^{\mathrm{n}\{p\}+1}$ *and* $\psi'' \in \overline{\mathbf{K}}^{\binom{\mathrm{n}\{p\}+1}{2}}$, *if* $Q_k(\gamma, \psi'_k) = 0$ *for* $0 \le k \le \mathrm{n}\{p\}$ *and* $R_{k,\ell}(\psi'_k, \psi'_\ell, \psi''_{k,\ell}) = 0$ *for* $0 \le k < \ell \le \mathrm{n}\{p\}$, *then*

$$\prod_{0 \le k < \ell \le \mathrm{n}\{p\}} P(\gamma, \psi''_{k,\ell}) = 0.$$

Proof. For every $0 \le k \le \mathrm{n}\{p\}$, the condition $Q_k(\gamma, \psi'_k) = 0$ implies that there exists a pair of roots $\tau_k, \tau'_k \in \overline{\mathbf{K}}$ of $P(\gamma, y)$ such that $\psi'_k = k(\tau_k + \tau'_k) + \tau_k \tau'_k$. Since there are at most $\mathrm{n}\{p\}$ different pairs of roots of $P(\gamma, y)$, by the pigeon hole principle there exist indices (k, ℓ), $0 \le k < \ell \le \mathrm{n}\{p\}$ and roots $\tau, \tau' \in \overline{\mathbf{K}}$ of $P(\gamma, y)$ such that $\psi'_k = k(\tau + \tau') + \tau\tau'$ and $\psi'_\ell = \ell(\tau + \tau') + \tau\tau'$. Then, we have

$$\tau + \tau' = \frac{\psi'_\ell - \psi'_k}{\ell - k}, \ \tau\tau' = \frac{\ell\psi'_k - k\psi'_\ell}{\ell - k},$$

so that the two roots of $R_{k,\ell}(\psi'_k, \psi'_\ell, y''_{k,\ell})$ are τ and τ' and therefore $\psi''_{k,\ell}$ is a root of $P(\gamma, y)$, what proves the claim. $\square$

The preceding statement is transformed into an algebraic identity using Effective Nullstellensatz ([31, Theorem 1.3]).

Lemma 4.1.5 *There is an identity in* $\mathbf{K}[c][y', y'']$

$$\begin{aligned} \prod_{0 \le k < \ell \le \mathrm{n}\{p\}} P(c, y''_{k,\ell})^m \;\; = & \sum_{0 \le k \le \mathrm{n}\{p\}} W_k(c, y', y'') \cdot Q_k(c, y'_k) \; + \\ + & \sum_{0 \le k < \ell \le \mathrm{n}\{p\}} W_{k,\ell}(c, y', y'') \cdot R_{k,\ell}(y'_k, y'_\ell, y''_{k,\ell}) \end{aligned}$$

such that all the terms have degree in (c, y', y'') *bounded by* $\mathrm{n}\{p\}^{\mathrm{n}\{p\}+1} 2^{\binom{\mathrm{n}\{p\}+1}{2}} (1 + \binom{\mathrm{n}\{p\}+1}{2} p)$.

Proof. Consider an auxiliary variable $\bar{y}$ and the polynomials $P^{[h]}(c, y, \bar{y})$, $Q_k^{[h]}(c, y'_k, \bar{y})$ and $R_{k,\ell}^{[h]}(y'_k, y'_\ell, y''_{k,\ell}, \bar{y})$ obtained respectively from $P(c, y)$, $Q_k(c, y'_k)$ and $R_{k,\ell}(y'_k, y'_\ell, y''_{k,\ell})$ by homogeneization.

It is clear from Lemma 4.1.4 that for any $\gamma \in \overline{\mathbf{K}}^p$, $\psi' \in \overline{\mathbf{K}}^{\mathrm{n}\{p\}+1}$, $\psi'' \in \overline{\mathbf{K}}^{\binom{\mathrm{n}\{p\}+1}{2}}$ and $\bar{\psi} \in \overline{\mathbf{K}}$, if $Q_k^{[h]}(\gamma, \psi'_k, \bar{\psi}) = 0$ for $0 \le k \le \mathrm{n}\{p\}$ and $R_{k,\ell}^{[h]}(\psi'_k, \psi'_\ell, \psi''_{k,\ell}, \bar{\psi}) = 0$ for $0 \le k < \ell \le \mathrm{n}\{p\}$, then

$$\bar{\psi} \prod_{0 \le k < \ell \le \mathrm{n}\{p\}} P^{[h]}(\gamma, \psi''_{k,\ell}, \bar{\psi}) = 0.$$

Following [31, Theorem 1.3], we have an identity

$$\begin{aligned}\bar{y}^m \cdot \prod_{0\le k<\ell\le \mathrm{n}\{p\}} P^{[h]}(c, y''_{k,\ell}, \bar{y})^m &= \sum_{0\le k\le \mathrm{n}\{p\}} W_k^{[h]}(c, y', y'', \bar{y}) \cdot Q_k^{[h]}(c, y'_k, \bar{y}) + \\ &+ \sum_{0\le k<\ell\le \mathrm{n}\{p\}} W_{k,\ell}^{[h]}(c, y', y'', \bar{y}) \cdot R_{k,\ell}^{[h]}(y'_k, y'_\ell, y''_{k,\ell}, \bar{y})\end{aligned} \quad (1)$$

with $m = \mathrm{n}\{p\}^{\mathrm{n}\{p\}+1} 2^{\binom{\mathrm{n}\{p\}+1}{2}}$ and $W_k^{[h]}$ and $W_{k,\ell}^{[h]}$ homogeneous polynomials such that all the terms in (1) have degree in $(c, y', y'', \bar{y})$ equal to $m(1 + \binom{\mathrm{n}\{p\}+1}{2}p)$. The lemma follows by evaluating $\bar{y} = 1$ in (1). □

The following function plays a key role in the estimates of the degrees in the weak inference version of the Fundamental Theorem of Algebra.

Definition 4.1.6 *Using Notation 4.1.1, let* $\mathrm{g}_2 : \mathbb{N}_* \to \mathbb{R}$, $\mathrm{g}_2\{p\} = 2^{2^{3\binom{p}{2}2^{\mathrm{r}\{p\}}}}$.

Technical Lemma 4.1.7 *Let* $p \in \mathbb{N}_*$.

1. *If* $p \geq 3$ *is an odd number, then* $3\mathrm{g}_1\{p-1, p\} \leq \mathrm{g}_2\{p\}$.
2. *If* $p \geq 4$ *is an even number, then* $\frac{3}{16}p^9 m 8^{\binom{\mathrm{n}\{p\}+1}{2}} \mathrm{g}_2^{\mathrm{n}\{p\}+1}\{\mathrm{n}\{p\}\} \leq \mathrm{g}_2\{p\}$, *where* $m = \mathrm{n}\{p\}^{\mathrm{n}\{p\}+1} 2^{\binom{\mathrm{n}\{p\}+1}{2}}$.

Proof. See Section 8. □

Theorem 4.1.8 (Fundamental Theorem of Algebra as a weak existence) *Let* $p \geq 1$ *and* $P = y^p + \sum_{0\le h\le p-1} C_h \cdot y^h \in \mathbf{K}[u][y]$. *Then*

$$\vdash \quad \exists z \; [\, P(z) = 0 \,],$$

where $z = a + ib$ *is a complex variable (see Notation 2.3.1).*

If we have an initial incompatibility in $\mathbf{K}[v][a, b]$ *where* $v \supset u$ *and* $a, b \notin v$, *with monoid part* S, *degree in* $w \subset v$ *bounded by* δ_w *and degree in* (a, b) *bounded by* δ_z, *the final incompatibility has monoid part* S^e *with* $e \leq \mathrm{g}_2\{p\}$, *and degree in* w *bounded by* $\mathrm{g}_2\{p\}(\delta_w + \delta_z \deg_w P)$.

Proof. Consider the initial incompatibility in $\mathbf{K}[v][a, b]$

$$S + N(a, b) + Z(a, b) + W_1(a, b) \cdot P_{\mathrm{Re}}(a, b) + W_2(a, b) \cdot P_{\mathrm{Im}}(a, b) = 0 \quad (2)$$

with $S \in \mathscr{M}(\mathcal{H}^2_{\neq})$, $N(a, b) \in \mathscr{N}(\mathcal{H}_{\geq})_{\mathbf{K}[v][a,b]}$, $Z(a, b) \in \mathscr{Z}(\mathcal{H}_{=})_{\mathbf{K}[v][a,b]}$ and $W_1(a, b)$, $W_2(a, b) \in \mathbf{K}[v][a, b]$, where $\mathcal{H}$ is a system of sign conditions in $\mathbf{K}[v]$.

The proof proceeds by induction on $\mathrm{r}\{p\}$. For $\mathrm{r}\{p\} = 0$, i.e. p is odd, we evaluate $b = 0$ in (2) and, since $P_{\mathrm{Im}}(a, b)$ is a multiple of b and $P_{\mathrm{Re}}(a, 0) = P(a)$, we obtain an incompatibility of type

$$S + N'(a) + Z'(a) + W'(a) \cdot P(a) = 0 \quad (3)$$

with $N'(a) \in \mathscr{N}(\mathcal{H}_{\geq})_{\mathbf{K}[v][a]}$, $Z'(a) \in \mathscr{Z}(\mathcal{H}_{=})_{\mathbf{K}[v][a]}$ and $W'(a) \in \mathbf{K}[v][a]$. For $p = 1$, we substitute $a = -C_0$ and we take the result as the final incompatibility. For odd $p \geq 3$, we apply to (3) the weak inference

$$\vdash \quad \exists a\ [\ P(a) = 0\ ].$$

By Theorem 3.2.1 (Real Root of an Odd Degree Polynomial as a weak existence) we obtain an incompatibility with monoid part S^e with $e \leq \mathrm{g}_1\{p-1,p\}$ and degree in w bounded by $3\mathrm{g}_1\{p-1,p\}(\delta_w + \delta_z \deg_w P)$, which serves as the final incompatibility taking into account Lemma 4.1.7 (item 1).

Suppose now $\mathrm{r}\{p\} \geq 1$, then p is even. If $W_1(a,b)$ and $W_2(a,b)$ in (2) are both the zero polynomial, we evaluate $a = 0$ and $b = 0$ in (2) and we take the result as the final incompatibility. From now, we suppose that $W_1(a,b)$ and $W_2(a,b)$ are not both the zero polynomial and therefore, $\delta_z \geq p$.

For $p = 2$, the result follows from Lemma 2.3.4.

So we suppose $p \geq 4$ and , from now on, we denote $n = \mathrm{n}\{p\}$, and $m = n^{n+1}2^{\binom{n+1}{2}}$.

For $0 \leq k < \ell \leq n$, we substitute $a = a''_{k,\ell}, b = b''_{k,\ell}$ in (2) and we apply the weak inference

$$P^2_{\mathrm{Re}}(a''_{k,\ell}, b''_{k,\ell}) + P^2_{\mathrm{Im}}(a''_{k,\ell}, b''_{k,\ell}) = 0 \quad \vdash \quad P(z''_{k,\ell}) = 0.$$

By Lemma 2.1.14, we obtain

$$\downarrow P^2_{\mathrm{Re}}(a''_{k,\ell}, b''_{k,\ell}) + P^2_{\mathrm{Im}}(a''_{k,\ell}, b''_{k,\ell}) = 0,\ \mathcal{H} \downarrow_{\mathbf{K}[v][a''_{k,\ell}, b''_{k,\ell}]} \tag{4}$$

with monoid part S^2, degree in w bounded by $2(\delta_w + \deg_w C_0)$ and degree in $(a''_{k,\ell}, b''_{k,\ell})$ bounded by $2\delta_z$.

Then we apply to the incompatibilities (4) for $0 \leq k < \ell \leq n$, each one repeated m times, the weak inference

$$\prod_{0 \leq k < \ell \leq n} \big(P^2_{\mathrm{Re}}(a''_{k,\ell}, b''_{k,\ell}) + P^2_{\mathrm{Im}}(a''_{k,\ell}, b''_{k,\ell})\big)^m = 0 \quad \vdash \quad \bigvee_{\substack{0 \leq k < \ell \leq n,\\ 1 \leq j \leq m}} P^2_{\mathrm{Re}}(a''_{k,\ell}, b''_{k,\ell}) + P^2_{\mathrm{Im}}(a''_{k,\ell}, b''_{k,\ell}) = 0.$$

By Lemma 2.1.12, we obtain

$$\left\downarrow \prod_{0 \leq k < \ell \leq n} \big(P^2_{\mathrm{Re}}(a''_{k,\ell}, b''_{k,\ell}) + P^2_{\mathrm{Im}}(a''_{k,\ell}, b''_{k,\ell})\big)^m = 0,\ \mathcal{H} \right\downarrow_{\mathbf{K}[v][a'',b'']} \tag{5}$$

with monoid part $S^{2m\binom{n+1}{2}}$, degree in w bounded by $2m\binom{n+1}{2}(\delta_w + \deg_w C_0)$ and degree in $(a''_{k,\ell}, b''_{k,\ell})$ bounded by $2m\delta_z$ for $0 \leq k < \ell \leq n$.

By Lemma 4.1.5, we have an identity

$$\begin{aligned} &\prod_{0 \leq k < \ell \leq n} \big(P^2_{\mathrm{Re}}(a''_{k,\ell}, b''_{k,\ell}) + P^2_{\mathrm{Im}}(a''_{k,\ell}, b''_{k,\ell})\big)^m = \\ = &\Big(\sum_{0 \leq k \leq n} (W_k)_{\mathrm{Re}} \cdot (Q_k)_{\mathrm{Re}} - (W_k)_{\mathrm{Im}} \cdot (Q_k)_{\mathrm{Im}} + \sum_{0 \leq k < \ell \leq n} (W_{k,\ell})_{\mathrm{Re}} \cdot (R_{k,\ell})_{\mathrm{Re}} - (W_{k,\ell})_{\mathrm{Im}} \cdot (R_{k,\ell})_{\mathrm{Im}}\Big)^2 + \\ + &\Big(\sum_{0 \leq k \leq n} (W_k)_{\mathrm{Re}} \cdot (Q_k)_{\mathrm{Im}} + (W_k)_{\mathrm{Im}} \cdot (Q_k)_{\mathrm{Re}} + \sum_{0 \leq k < \ell \leq n} (W_{k,\ell})_{\mathrm{Re}} \cdot (R_{k,\ell})_{\mathrm{Im}} + (W_{k,\ell})_{\mathrm{Im}} \cdot (R_{k,\ell})_{\mathrm{Re}}\Big)^2 \end{aligned}$$

and then we apply to (5) the weak inference

$$\bigwedge_{0\le k\le n} Q_k(C,z'_k)=0,\ \bigwedge_{0\le k<\ell\le n} R_{k,\ell}(z'_k,z'_\ell,z''_{k,\ell})=0 \quad \vdash$$

$$\vdash \quad \prod_{0\le k<\ell\le n} \big(P^2_{\mathrm{Re}}(a''_{k,\ell},b''_{k,\ell})+P^2_{\mathrm{Re}}(a''_{k,\ell},b''_{k,\ell})\big)^m = 0.$$

By Lemma 2.1.8, we obtain

$$\downarrow \bigwedge_{0\le k\le n} Q_k(C,z'_k)=0,\ \bigwedge_{0\le k<\ell\le n} R_{k,\ell}(z'_k,z'_\ell,z''_{k,\ell})=0,\ \mathcal{H} \downarrow_{\mathbf{K}[v][a',b',a'',b'']} \tag{6}$$

with the same monoid part, degree in w bounded by

$$2m\Big(\binom{n+1}{2}\delta_w+\Big(1+\binom{n+1}{2}p\Big)\deg_w P\Big)\le m\Big(\frac{1}{4}p^4\delta_w+\frac{1}{4}p^5\deg_w P\Big),$$

degree in (a'_k,b'_k) bounded by $2m(1+\binom{n+1}{2}p)\le \frac{1}{4}mp^5$ for $0\le k\le n$ and degree in $(a''_{k,\ell},b''_{k,\ell})$ bounded by $2m(1-p+\binom{n+1}{2}p+\delta_z)\le m(\frac{1}{4}p^5+2\delta_z)$ for $0\le k<\ell\le n$.

Then we fix an arbitrary order $(k_1,\ell_1),\dots,(k_{\binom{n+1}{2}},\ell_{\binom{n+1}{2}})$ of all the pairs (k,ℓ) with $0\le k<\ell\le n$ and we we successively apply to (6) for $1\le h\le\binom{n+1}{2}$ the weak inference

$$\vdash \quad \exists z''_{k_h,\ell_h}\ [\ R_{k_h,\ell_h}(z'_{k_h},z'_{\ell_h},z''_{k_h,\ell_h})=0\ ].$$

By Lemma 2.3.4, we obtain

$$\downarrow \bigwedge_{0\le k\le n} Q_k(C,z'_k)=0,\ \mathcal{H} \downarrow_{\mathbf{K}[v][a',b']} \tag{7}$$

with monoid part $S^{2m\binom{n+1}{2}8^{\binom{n+1}{2}}}$ and degree in w bounded by

$$\delta'_w := m\Big(\frac{1}{4}p^4\delta_w+\frac{1}{4}p^5\deg_w P\Big)8^{\binom{n+1}{2}}.$$

In order to obtain a bound for the degree in (a'_k,b'_k) of (7) for $0\le k\le n$, we do the following analysis. Consider a fixed $0\le k_0\le n$. For $1\le h\le\binom{n+1}{2}$, $\deg_{(a'_{k_0},b'_{k_0})} R_{k_h,\ell_h}=0$ if $k_0\ne k_h,\ell_h$ and $\deg_{(a'_{k_0},b'_{k_0})} R_{k_h,\ell_h}=1$ otherwise. Again by Lemma 2.3.4, there will be $\binom{n}{2}$ values of h for which the bound for the degree in (a'_{k_0},b'_{k_0}) is multiplied by 8 and n values of h for which the bound for the degree in (a'_{k_0},b'_{k_0}) is multiplied by 8 and then increased by $40+m(6p^5+48\delta_z)8^{h-1}$. It is easy to see that the worst case for the degree bound in (a'_{k_0},b'_{k_0}) is when these n values of h are $1,\dots,n$, and that, in this case, after the application of the first $h\le n$ weak inferences, the degree in (a'_{k_0},b'_{k_0}) of the incompatibility we obtain is bounded by

$$\frac{1}{4}mp^5 8^h+40\Big(\sum_{0\le j\le h-1}8^j\Big)+m(6p^5+48\delta_z)h8^{h-1}.$$

From this, we conclude that the degree in (a'_k, b'_k) of (7) is bounded by

$$\frac{1}{4}mp^5 8^{\binom{n+1}{2}} + 40\Big(\sum_{0\le j\le n-1} 8^j\Big)8^{\binom{n}{2}} + m(6p^5 + 48\delta_z)n8^{\binom{n+1}{2}-1} \le m\Big(\frac{3}{8}p^7 + 3p^2\delta_z\Big)8^{\binom{n+1}{2}} =: \delta'_{z'}$$

for $0 \le k \le n$.

Finally we successively apply to (7) for every $0 \le k \le n$ the weak inference

$$\vdash \quad \exists z'_k \ [\ Q_k(C, z'_k) = 0\ ].$$

Since $\mathrm{r}\{\mathrm{n}\{p\}\} = \mathrm{r}\{p\} - 1$, by the inductive hyphotesis, we obtain

$$\downarrow \mathcal{H} \downarrow_{\mathbf{K}[v]} \tag{8}$$

with monoid part $S^{2m\binom{n+1}{2}8^{\binom{n+1}{2}}e'^{n+1}}$ with $e' \le \mathrm{g}_2\{n\}$. Also, when applying the weak inference corresponding to the index k, the bound for the degree in w is increased by $\mathrm{g}_2^k\{n\}\delta'_{z'}(p-1)\deg_w P$ and then multiplied by $\mathrm{g}_2\{n\}$ (see Remark 4.1.3). It is easy to see that, after the application of this weak inference, the degree in w of the incompatibility we obtain is bounded by

$$\mathrm{g}_2^{k+1}\{n\}(\delta'_w + (k+1)\delta'_{z'}(p-1)\deg_w P).$$

Therefore, the degree in w of (8) is bounded by

$$\mathrm{g}_2^{n+1}\{n\}(\delta'_w + (n+1)\delta'_{z'}(p-1)\deg_w P) \le \mathrm{g}_2^{n+1}\{n\}m\Big(\frac{1}{4}p^4\delta_w + \frac{3}{16}p^9\delta_z\deg_w P\Big)8^{\binom{n+1}{2}}.$$

The incompatibility (8) serves as the final incompatibility since

$$2m\binom{n+1}{2}8^{\binom{n+1}{2}}\mathrm{g}_2^{n+1}\{n\} \le \frac{1}{4}p^4 m 8^{\binom{n+1}{2}}\mathrm{g}_2^{n+1}\{n\} \le \frac{3}{16}p^9 m 8^{\binom{n+1}{2}}\mathrm{g}_2^{n+1}\{n\} \le \mathrm{g}_2\{p\}$$

and

$$\mathrm{g}_2^{n+1}\{n\}m\Big(\frac{1}{4}p^4\delta_w + \frac{3}{16}p^9\delta_z\deg_w P\Big)8^{\binom{n+1}{2}} \le$$
$$\le \mathrm{g}_2^{n+1}\{n\}\frac{3}{16}p^9 m\Big(\delta_w + \delta_z\deg_w P\Big)8^{\binom{n+1}{2}} \le \mathrm{g}_2\{p\}(\delta_w + \delta_z\deg_w P)$$

using Lemma 4.1.7 (item 2). □

4.2 Decomposition of a polynomial into irreducible real factors

We obtain now a weak disjunction on the possible decompositions of a polynomial into irreducible real factors.

We prove first an auxiliary lemma.

Lemma 4.2.1 *Let $p \ge 2$ be an even number and $P = y^p + \sum_{0\le h\le p-1} C_h \cdot y^h \in \mathbf{K}[u][y]$. Then*

$$\vdash \quad \exists (t_1, t_2)\ [\ P \equiv (y-t_1)\cdot(y-t_2)\cdot \mathrm{Quot}(P, (y-t_1)(y-t_2))\ ]\ \vee$$
$$\vee\ \exists z\ [\ P \equiv ((y-a)^2 + b^2)\cdot \mathrm{Quot}(P, (y-a)^2 + b^2),\ b \ne 0\ ],$$

where $z = a + ib$ is a complex variable (see Notation 2.3.1).

Suppose we have initial incompatibilities in $\mathbf{K}[v][t_1, t_2]$ and $\mathbf{K}[v][a, b]$ where $v \supset u$ and $t_1, t_2, a, b \notin v$, with monoid part S_1 and $S_2 \cdot b^{2e}$ and degree in $w \subset v$ bounded by δ_w. Suppose also that the first initial incompatibility has degree in t_1 and degree in t_2 bounded by δ_t and the second initial incompatibility has degree in (a, b) bounded by δ_z. Then, the final incompatibility has monoid part $S_1^{2(e+1)f} \cdot S_2^{f'}$ with $f \le \mathrm{g}_1\{p-2, p-1\}\mathrm{g}_2\{p\}$ and $f' \le \mathrm{g}_2\{p\}$ and degree in w bounded by

$$\mathrm{g}_2\{p\}\Big((1+6\mathrm{g}_1\{p-2,p-1\}(e+1))\delta_w + \Big(3+\delta_z+6\mathrm{g}_1\{p-2,p-1\}(e+1)(2+(p+1)\delta_t)\Big)\deg_w P\Big),$$

Proof. Consider the initial incompatibilities,

$$\downarrow P \equiv (y - t_1) \cdot (y - t_2) \cdot \mathrm{Quot}(P, (y - t_1)(y - t_2)),\ \mathcal{H} \downarrow_{\mathbf{K}[v][t_1,t_2]} \tag{9}$$

and

$$\downarrow P \equiv ((y - a)^2 + b^2) \cdot \mathrm{Quot}(P, (y - a)^2 + b^2),\ b \neq 0,\ \mathcal{H} \downarrow_{\mathbf{K}[v][a,b]}, \tag{10}$$

where $\mathcal{H}$ is a system of sign conditions in $\mathbf{K}[v]$.

We successively apply to (9) the weak inferences

$$\begin{aligned} P(t_1) = 0,\ \mathrm{Quot}(P, y - t_1)(t_2) = 0 \quad &\vdash \quad P \equiv (y - t_1) \cdot (y - t_2) \cdot \mathrm{Quot}(P, (y - t_1)(y - t_2)), \\ &\vdash \quad \exists t_2\ [\ \mathrm{Quot}(P, y - t_1)(t_2) = 0\ ]. \end{aligned}$$

By Lemma 2.4.3 and Theorem 3.2.1 (Real Root of an Odd Degree Polynomial as a weak existence), we obtain

$$\downarrow P(t_1) = 0,\ \mathcal{H} \downarrow_{\mathbf{K}[v][t_1]} \tag{11}$$

with monoid part $S_1^{e'}$ with $e' \le \mathrm{g}_1\{p-2, p-1\}$ and, after some analysis, degree in w bounded by $3\mathrm{g}_1\{p-2, p-1\}(\delta_w + (1+\delta_t)\deg_w P)$ and degree in t_1 bounded by $3\mathrm{g}_1\{p-2, p-1\}(1+p\delta_t)$.

Then we substitute $t_1 = a$ in (11) and, taking into account that $P_{\mathrm{Re}}(a, b) - P(a)$ is a multiple of b, we apply the weak inference

$$P(z) = 0,\ b = 0 \quad \vdash \quad P(a) = 0.$$

By Lemma 2.1.8, we obtain

$$\downarrow P(z) = 0,\ b = 0,\ \mathcal{H} \downarrow_{\mathbf{K}[v][a,b]} \tag{12}$$

with the same monoid part and bound for the degree in w and degree in (a, b) bounded by $3\mathrm{g}_1\{p-2, p-1\}(1+p\delta_t)$.

On the other hand, we apply to (10) the weak inference

$$P(z) = 0,\ b \neq 0 \quad \vdash \quad P \equiv ((y - a)^2 + b^2) \cdot \mathrm{Quot}(P, (y - a)^2 + b^2).$$

By Lemma 2.4.4, we obtain

$$\downarrow P(z) = 0,\ b \neq 0,\ \mathcal{H} \downarrow_{\mathbf{K}[v][a,b]} \tag{13}$$

with monoid part $S_2 \cdot b^{2(e+1)}$, degree in w bounded by $\delta_w + \deg_w P$ and degree in (a, b) bounded by $\delta_z + 2$.

Then we apply to (13) and (12) the weak inference

$$\vdash \quad b \neq 0 \ \vee \ b = 0.$$

By Lemma 2.1.16, we obtain

$$\downarrow P(z) = 0, \ \mathcal{H} \downarrow_{\mathbf{K}[v][a,b]} \tag{14}$$

with monoid part $S_1^{2(e+1)e'} \cdot S_2$, degree in w bounded by

$$\delta_w + \deg_w P + 6\mathrm{g}_1\{p-2, p-1\}(e+1)(\delta_w + (1+\delta_t)\deg_w P)$$

and degree in (a, b) bounded by

$$\delta_z + 2 + 6\mathrm{g}_1\{p-2, p-1\}(e+1)(1 + p\delta_t).$$

Finally we apply to (14) the weak inference

$$\vdash \quad \exists z \ [\ P(z) = 0\ ].$$

By Theorem 4.1.8 (Fundamental Theorem of Algebra as a weak existence), we obtain

$$\downarrow \mathcal{H} \downarrow_{\mathbf{K}[v]}$$

with monoid part $S_1^{2(e+1)e'f'} \cdot S_2^{f'}$ with $f' \leq \mathrm{g}_2\{p\}$ and degree in w bounded by

$$\mathrm{g}_2\{p\}\Big((1+6\mathrm{g}_1\{p-2,p-1\}(e+1))\delta_w + \Big(3+\delta_z+6\mathrm{g}_1\{p-2,p-1\}(e+1)(2+(p+1)\delta_t)\Big)\deg_w P\Big),$$

which serves as the final incompatibility. □

We define a new auxiliary function.

Definition 4.2.2 *Let* $\mathrm{g}_3 : \mathbb{N} \to \mathbb{R}$, $\mathrm{g}_3\{p\} = 2^{2^{3\binom{p}{2}p+1}}$.

Technical Lemma 4.2.3 *Let* $p \in \mathbb{N}_*$.

1. *If* $p \geq 3$ *is an odd number, then* $3(2p+1)\mathrm{g}_1\{p-1, p\}\mathrm{g}_3\{p-1\} \leq \mathrm{g}_3\{p\}$.
2. *If* $p \geq 4$ *is an even number, then* $6p^3\mathrm{g}_1\{p-2, p-1\}\mathrm{g}_2\{p\}\mathrm{g}_3^2\{p-2\} \leq \mathrm{g}_3\{p\}$.

Proof. See Section 8. □

We now prove the weak disjunction on the possible decompositions taking into account only the number of real and complex roots.

Theorem 4.2.4 (Real Irreducible Factors as a weak existence) *Let $p \geq 1$ and $P = y^p + \sum_{0 \leq h \leq p-1} C_h \cdot y^h \in \mathbf{K}[u][y]$. Then*

$$\vdash \quad \bigvee_{m+2n=p} \exists (t_m, z_n) \ \Big[\ P \equiv \prod_{1 \leq j \leq m} (y - t_{m,j}) \cdot \prod_{1 \leq k \leq n} ((y - a_{n,k})^2 + b_{n,k}^2), \ \bigwedge_{1 \leq k \leq n} b_{n,k} \neq 0 \ \Big],$$

where $t_m = (t_{m,1}, \dots, t_{m,m})$ is a set of variables and $z_n = (z_{n,1}, \dots, z_{n,n})$ is set of complex variables with $z_{n,k} = a_{n,k} + i b_{n,k}$ (see Notation 2.3.1).

Suppose we have initial incompatibilities in $\mathbf{K}[v][t_m, a_n, b_n]$ where $v \supset u$ and t_m, a_n, b_n are disjoint from v, with monoid part $S_{m,n} \cdot \prod_{1 \leq k \leq n} b_{n,k}^{2e_{n,k}}$ with $e_{n,k} \leq e$, degree in $w \subset v$ bounded by δ_w, degree in $t_{m,j}$ bounded by δ_t for $1 \leq j \leq m$ and degree in $(a_{n,k}, b_{n,k})$ bounded by δ_z for $1 \leq k \leq n$. Then, the final incompatibility has monoid part $\prod_{m+2n=p} S_{m,n}^{f_{m,n}}$ with $f_{m,n} \leq (e+1)^{2^{\lfloor \frac{p}{2} \rfloor - 1}} \mathrm{g}_3\{p\}$ and degree in w bounded by $(e+1)^{2^{\lfloor \frac{p}{2} \rfloor - 1}} \mathrm{g}_3\{p\} (\delta_w + \max\{\delta_t, \delta_z\} \deg_w P)$.

Proof. Consider for $m, n \in \mathbb{N}$ such that $m + 2n = p$ the initial incompatibility

$$\Big\downarrow \ P \equiv \prod_{1 \leq j \leq m} (y - t_{m,j}) \cdot \prod_{1 \leq k \leq n} ((y - a_{n,k})^2 + b_{n,k}^2), \ \bigwedge_{1 \leq k \leq n} b_{n,k} \neq 0, \ \mathcal{H} \ \Big\downarrow_{\mathbf{K}[v][t_m, a_n, b_n]} \tag{15}$$

where $\mathcal{H}$ is a system of sign conditions in $\mathbf{K}[v]$. If $\max\{\delta_t, \delta_z\} = 0$, the result follows by simply taking any of the initial incompatibilities as the final incompatibility. So from now we suppose $\max\{\delta_t, \delta_z\} \geq 1$.

We first prove the result for even p by induction. For $p = 2$ the result follows from Lemma 4.2.1. Suppose now $p \geq 4$.

For $m, n \in \mathbb{N}$ such that $m + 2n = p$ with $m \geq 2$, we apply to (15) the weak inference

$$\begin{gathered} P \equiv (y - t_{m,1}) \cdot (y - t_{m,2}) \cdot \mathrm{Quot}(P, (y - t_{m,1})(y - t_{m,2})), \\ \mathrm{Quot}(P, (y - t_{m,1}) \cdot (y - t_{m,2})) \equiv \prod_{3 \leq j \leq m} (y - t_{m,j}) \cdot \prod_{1 \leq k \leq n} ((y - a_{n,k})^2 + b_{n,k}^2) \quad \vdash \\ \vdash \quad P \equiv \prod_{1 \leq j \leq m} (y - t_{m,j}) \cdot \prod_{1 \leq k \leq n} ((y - a_{n,k})^2 + b_{n,k}^2). \end{gathered}$$

which is a particular case of the weak inference in Lemma 2.1.8. After a careful analysis, we obtain

$$\begin{gathered} \Big\downarrow \ P \equiv (y - t_{m,1}) \cdot (y - t_{m,2}) \cdot \mathrm{Quot}(P, (y - t_{m,1}) \cdot (y - t_{m,2})), \\ \mathrm{Quot}(P, (y - t_{m,1}) \cdot (y - t_{m,2})) \equiv \prod_{3 \leq j \leq m} (y - t_{m,j}) \cdot \prod_{1 \leq k \leq n} ((y - a_{n,k})^2 + b_{n,k}^2), \\ \bigwedge_{1 \leq k \leq n} b_{n,k} \neq 0, \ \mathcal{H} \ \Big\downarrow_{\mathbf{K}[v][t_m, a_n, b_n]} \end{gathered} \tag{16}$$

with the same monoid part, degree in w bounded by $\delta_w + \deg_w P$, degree in $t_{m,1}$ and in $t_{m,2}$ bounded by $\delta_t + p - 2$, degree in $t_{m,j}$ bounded by δ_t for $3 \leq j \leq m$ and degree in $(a_{n,k}, b_{n,k})$ bounded by δ_z for $1 \leq k \leq n$.

Then we substitute $t_{m,1} = t_1$ and $t_{m,2} = t_2$ in the incompatibilities (16) and we apply to these incompatibilities the weak inference

$$\vdash \bigvee_{\substack{m+2n=p,\\ m\geq 2}} \exists(t'_m, z_n) \Big[\operatorname{Quot}(P, (y-t_1)\cdot(y-t_2)) \equiv \prod_{3\leq j\leq m}(y - t_{m,j}) \cdot \prod_{1\leq k\leq n}((y-a_{n,k})^2 + b_{n,k}^2), \bigwedge_{1\leq k\leq n} b_{n,k} \neq 0 \Big]$$

where $t'_m = (t_{m,3}, \dots, t_{m,m})$. Since $\deg_y \operatorname{Quot}(P, (y-t_1)\cdot(y-t_2)) = p-2$, by the inductive hyphotesis we obtain

$$\downarrow P \equiv (y-t_1)\cdot(y-t_2)\cdot \operatorname{Quot}(P, (y-t_1)(y-t_2)),\ \mathcal{H} \downarrow_{\mathbf{K}[v][t_1,t_2]} \tag{17}$$

with monoid part

$$\prod_{\substack{m+2n=p,\\ m\geq 2}} S_{m,n}^{f_{m-2,n}}$$

with $f_{m-2,n} \leq (e+1)^{2^{\frac{p-2}{2}}-1} \mathrm{g}_3\{p-2\}$, degree in w bounded by

$$\delta'_w := (e+1)^{2^{\frac{p-2}{2}}-1} \mathrm{g}_3\{p-2\}(\delta_w + (1+\max\{\delta_t,\delta_z\})\deg_w P),$$

and degree in t_1 and degree in t_2 bounded by

$$\delta'_t := (e+1)^{2^{\frac{p-2}{2}}-1} \mathrm{g}_3\{p-2\}(\delta_t + (1+\max\{\delta_t,\delta_z\})(p-2)).$$

On the other hand, we obtain in a similar way, from the initial incompatibilities (15) for $m, n \in \mathbb{N}$ such that $m + 2n = p$ with $n \geq 1$,

$$\downarrow P \equiv ((y-a)^2 + b^2)\cdot \operatorname{Quot}(P, (y-a)^2 + b^2),\ b \neq 0,\ \mathcal{H} \downarrow_{\mathbf{K}[v][a,b]} \tag{18}$$

with, defining $E = \sum_{m+2n=p,\, n\geq 1} e_{n,1} f_{m,n-1}$, monoid part

$$\prod_{\substack{m+2n=p,\\ n\geq 1}} S_{m,n}^{f_{m,n-1}} \cdot b^{2E}$$

with $f_{m,n-1} \leq (e+1)^{2^{\frac{p-2}{2}}-1} \mathrm{g}_3\{p-2\}$, degree in w bounded by δ'_w and degree in (a,b) bounded by

$$\delta'_z := (e+1)^{2^{\frac{p-2}{2}}-1} \mathrm{g}_3\{p-2\}(\delta_z + (1+\max\{\delta_t,\delta_z\})(p-2)).$$

Finally, we apply to (17) and (18) the weak inference

$$\begin{aligned} \vdash\quad & \exists(t_1,t_2)\ [\ P \equiv (y-t_1)\cdot(y-t_2)\cdot \operatorname{Quot}(P, (y-t_1)\cdot(y-t_2))\ ]\ \vee \\ & \vee\ \exists z\ [\ P \equiv ((y-a)^2+b^2)\cdot \operatorname{Quot}(P, (y-a)^2+b^2),\ b\neq 0\ ]. \end{aligned}$$

By Lemma 4.2.1, we obtain

$$\downarrow \mathcal{H} \downarrow_{\mathbf{K}[v]} \tag{19}$$

with monoid part

$$\Big(\prod_{\substack{m+2n=p,\\ m\geq 2}} S_{m,n}^{f_{m-2,n}}\Big)^{2(E+1)f}\cdot\Big(\prod_{\substack{m+2n=p,\\ n\geq 1}} S_{m,n}^{f_{m,n-1}}\Big)^{f'},$$

with $f \leq \mathrm{g}_1\{p-2,p-1\}\mathrm{g}_2\{p\}$ and $f' \leq \mathrm{g}_2\{p\}$. Therefore, for $m \geq 2$ and $n \geq 1$, we take

$$f_{m,n} = 2f_{m-2,n}(E+1)f + f_{m,n-1}f' \leq (e+1)^{2^{\frac{p}{2}}-1} p\,\mathrm{g}_1\{p-2,p-1\}\mathrm{g}_2\{p\}\mathrm{g}_3^2\{p-2\} \leq (e+1)^{2^{\frac{p}{2}}-1}\mathrm{g}_3\{p\}$$

using Lemma 4.2.3 (item 2). Also we take $f_{0,\frac{p}{2}} = f_{0,\frac{p}{2}-1}f' \leq (e+1)^{2^{\frac{p}{2}}-1}\mathrm{g}_3\{p\}$ and $f_{p,0} = 2f_{p-2,0}(E+1)f \leq (e+1)^{2^{\frac{p}{2}}-1}\mathrm{g}_3\{p\}$ in a similar way. Again by Lemma 4.2.1, the degree in w of (19) is bounded by

$$\begin{aligned}
& \mathrm{g}_2\{p\}\Big((1+6\mathrm{g}_1\{p-2,p-1\}(E+1))\delta'_w + \\
& + \Big(3+\delta'_z+6\mathrm{g}_1\{p-2,p-1\}(E+1)(2+(p+1)\delta'_t)\Big)\deg_w P\Big) \leq \\
\leq\ & (e+1)^{2^{\frac{p}{2}}-1} 6p^3 \mathrm{g}_1\{p-2,p-1\}\mathrm{g}_2\{p\}\mathrm{g}_3^2\{p-2\}(\delta_w + \max\{\delta_t,\delta_z\}\deg_w P) \leq \\
\leq\ & (e+1)^{2^{\frac{p}{2}}-1}\mathrm{g}_3\{p\}(\delta_w + \max\{\delta_t,\delta_z\}\deg_w P)
\end{aligned}$$

using Lemma 4.2.3 (item 2). Therefore (19) serves as the final incompatibility.

Now we prove the result for odd p. For $p = 1$ note that we only have to consider $m = 1$ and $n = 0$; therefore we can take $e = 0$. We simply substitute $t_{1,1} = -C_1$ in (15) and take the result as the final incompatibility. Suppose now $p \geq 3$.

For $m, n \in \mathbb{N}$ such that $m + 2n = p$ we apply to (15) the weak inference

$$\begin{aligned}
P \equiv (y - t_{m,1}) \cdot \mathrm{Quot}(P, y - t_{m,1}), \\
\mathrm{Quot}(P, y - t_{m,1}) \equiv \prod_{2\leq j\leq m}(y - t_{m,j}) \cdot \prod_{1\leq k\leq n}((y-a_{n,k})^2 + b_{n,k}^2) \quad \vdash \\
\vdash \quad P \equiv \prod_{1\leq j\leq m}(y - t_{m,j}) \cdot \prod_{1\leq k\leq n}((y-a_{n,k})^2 + b_{n,k}^2).
\end{aligned}$$

which is a particular case of the weak inference in Lemma 2.1.8. After a careful analysis, we obtain

$$\begin{gathered}
\downarrow P(t_{m,1}) = 0, \\
\mathrm{Quot}(P, y - t_{m,1}) \equiv \textstyle\prod_{2\leq j\leq m}(y - t_{m,j}) \cdot \prod_{1\leq k\leq n}((y-a_{n,k})^2 + b_{n,k}^2), \\
\textstyle\bigwedge_{1\leq k\leq n} b_{n,k} \neq 0,\ \mathcal{H} \downarrow_{\mathbf{K}[v][t_m,a_n,b_n]}
\end{gathered} \tag{20}$$

with the same monoid part, degree in w bounded by $\delta_w + \deg_w P$, degree in $t_{m,1}$ bounded by $\delta_t + p - 1$, degree in $t_{m,j}$ bounded by δ_t for $2 \leq j \leq m$ and degree in $(a_{n,k}, b_{n,k})$ bounded by δ_z for $1 \leq k \leq n$.

Then we substitute $t_{m,1} = t$ in the incompatibilities (20) and we apply to these incompatibilities the weak inference

$$\vdash \bigvee_{m+2n=p} \exists(t'_m, z_n)\,\Big[\ \mathrm{Quot}(P, y-t) \equiv \prod_{2\leq j\leq m}(y-t_{m,j})\cdot \prod_{1\leq k\leq n}((y-a_{n,k})^2+b_{n,k}^2),\ \bigwedge_{1\leq k\leq n} b_{n,k} \neq 0\ \Big]$$

where $t'_m = (t_{m,2}, \ldots, t_{m,m})$. Since $\deg_y \operatorname{Quot}(P, y-t)$ is an even number greater than or equal to 2, we obtain

$$\downarrow P(t) = 0,\ \mathcal{H} \downarrow_{\mathbf{K}[v][t]} \tag{21}$$

with monoid part $\prod_{m+2n=p} S_{m,n}^{f_{m-1,n}}$ with $f_{m-1,n} \le (e+1)^{2^{\frac{p-1}{2}}-1} \mathrm{g}_3\{p-1\}$, degree in w bounded by

$$\delta''_w := (e+1)^{2^{\frac{p-1}{2}}-1} \mathrm{g}_3\{p-1\}(\delta_w + (1+\max\{\delta_t, \delta_z\}) \deg_w P)$$

and degree in t bounded by

$$\delta''_t := (e+1)^{2^{\frac{p-1}{2}}-1} \mathrm{g}_3\{p-1\}(\delta_t + (1+\max\{\delta_t, \delta_z\})(p-1)).$$

Finally, since p is odd, we apply to (21) the weak inference

$$\vdash \quad \exists t\ [\ P(t) = 0\ ].$$

By Theorem 3.2.1 (Real Root of an Odd Degree Polynomial as a weak existence) we obtain

$$\downarrow \mathcal{H} \downarrow_{\mathbf{K}[v]} \tag{22}$$

with monoid part $(\prod_{m+2n=p} S_{m,n}^{f_{m-1,n}})^{e'}$ with $e' \le \mathrm{g}_1\{p-1,p\}$. Therefore, for every m and n, we take $f_{m,n} = f_{m-1,n}e' \le (e+1)^{2^{\frac{p-1}{2}}-1} \mathrm{g}_1\{p-1,p\}\mathrm{g}_3\{p-1\} \le (e+1)^{2^{\frac{p-1}{2}}-1} \mathrm{g}_3\{p\}$ using Lemma 4.2.3 (item 1). Again by Theorem 3.2.1, the degree in w of (22) is bounded by

$$\begin{aligned} & 3\mathrm{g}_1\{p-1,p\}(\delta''_w + \delta''_t \deg_w P) \le \\ \le\ & (e+1)^{2^{\frac{p-1}{2}}-1} 3(2p+1)\mathrm{g}_1\{p-1,p\}\mathrm{g}_3\{p-1\}(\delta_w + \max\{\delta_t, \delta_z\} \deg_w P) \le \\ \le\ & (e+1)^{2^{\frac{p-1}{2}}-1} \mathrm{g}_3\{p\}(\delta_w + \max\{\delta_t, \delta_z\} \deg_w P). \end{aligned}$$

using Lemma 4.2.3 (item 1). Therefore (22) serves as the final incompatibility. □

4.3 Decomposition of a polynomial into irreducible real factors with multiplicities

In order to prove the weak inference of the decomposition into irreducible factors taking multiplicities into account, we introduce some notation and definitions.

Notation 4.3.1 *Let $m \in \mathbb{N}$. We introduce the following notation: For $m \in \mathbb{N}_*$,*

$$\Lambda_m = \{\boldsymbol{\mu} = (\mu_1 \ge \cdots \ge \mu_{\#\boldsymbol{\mu}}) \mid \mu_i \in \mathbb{N}_* \text{ for } 1 \le i \le \#\boldsymbol{\mu},\ |\boldsymbol{\mu}| = \sum_{1 \le i \le \#\boldsymbol{\mu}} \mu_i = m\};$$

Λ_0 is the set with a single element equal to an empty vector.

Definition 4.3.2 *Let $p \ge 1$, $P = y^p + \sum_{0 \le h \le p-1} C_h \cdot y^h \in \mathbf{K}[u][y]$, $(\boldsymbol{\mu}, \boldsymbol{\nu}) \in \Lambda_m \times \Lambda_n$ with $m + 2n = p$, $t = (t_1, \ldots, t_{\#\boldsymbol{\mu}})$ and $z = (z_1, \ldots, z_{\#\boldsymbol{\nu}})$ a set of complex variables with $z_k = a_k + ib_k$ (see Notation 2.3.1). We define*

$$\mathrm{F}^{\boldsymbol{\mu},\boldsymbol{\nu}} = y^p + \sum_{0 \le h \le p-1} \mathrm{F}_h^{\boldsymbol{\mu},\boldsymbol{\nu}} \cdot y^h = \prod_{1 \le j \le \#\boldsymbol{\mu}} (y - t_j)^{\mu_j} \cdot \prod_{1 \le k \le \#\boldsymbol{\nu}} ((y - a_k)^2 + b_k^2)^{\nu_k} \in \mathbb{Z}[t, a, b][y].$$

Using Notation 2.4.5, we define the system of sign conditions

$$\mathrm{Fact}(P)^{\boldsymbol{\mu},\boldsymbol{\nu}}(t,z)$$

in $\mathbf{K}[u][t,a,b]$ *describing the decomposition of* P *into irreducible real factors:*

$$P \equiv \mathrm{F}^{\boldsymbol{\mu},\boldsymbol{\nu}}, \quad \bigwedge_{1\le j<j'\le \#\boldsymbol{\mu}} t_j \neq t_{j'}, \quad \bigwedge_{1\le k\le \#\boldsymbol{\nu}} b_k \neq 0, \quad \bigwedge_{1\le k<k'\le \#\boldsymbol{\nu}} \mathrm{R}(z_k, z_{k'}) \neq 0.$$

Before proving the weak disjunction on the possible decompositions taking multiplicities into account, we define a new auxiliary function.

Definition 4.3.3 *Let* $\mathrm{g}_4 : \mathbb{N} \to \mathbb{R}$, $\mathrm{g}_4\{p\} = 2^{2^{3(\frac{p}{2})^p+2}}$.

Technical Lemma 4.3.4 *For every* $p \in \mathbb{N}_*$, $2^{(p^2-p+2)2^{\frac{1}{2}p^2}} \mathrm{g}_3\{p\} \le \mathrm{g}_4\{p\}$.

Proof. Easy. □

Theorem 4.3.5 (Real Irreducible Factors with Multiplicities as a weak existence) *Let* $p \ge 1$ *and* $P = y^p + \sum_{0\le h\le p-1} C_h \cdot y^h \in \mathbf{K}[u][y]$. *Then*

$$\vdash \bigvee_{\substack{m+2n=p \\ (\boldsymbol{\mu},\boldsymbol{\nu})\in\Lambda_m\times\Lambda_n}} \exists (t_{\boldsymbol{\mu}}, z_{\boldsymbol{\nu}}) \ [\ \mathrm{Fact}(P)^{\boldsymbol{\mu},\boldsymbol{\nu}}(t_{\boldsymbol{\mu}}, z_{\boldsymbol{\nu}})\ ],$$

where $t_{\boldsymbol{\mu}} = (t_{\boldsymbol{\mu},1}, \ldots, t_{\boldsymbol{\mu},\#\boldsymbol{\mu}})$ *is a set of variables and* $z_{\boldsymbol{\nu}} = (z_{\boldsymbol{\nu},1}, \ldots, z_{\boldsymbol{\nu},\#\boldsymbol{\nu}})$ *is a set of complex variables with* $z_{\boldsymbol{\nu},k} = a_{\boldsymbol{\nu},k} + i b_{\boldsymbol{\nu},k}$ *(see Notation 2.3.1).*

Suppose we have initial incompatibilities in $\mathbf{K}[v][t_{\boldsymbol{\mu}}, a_{\boldsymbol{\nu}}, b_{\boldsymbol{\nu}}]$ *where* $v \supset u$, *and* $t_{\boldsymbol{\mu}}, a_{\boldsymbol{\nu}}, b_{\boldsymbol{\nu}}$ *are disjoint from* v, *with monoid part*

$$S_{\boldsymbol{\mu},\boldsymbol{\nu}} \cdot \prod_{1\le j<j'\le \#\boldsymbol{\mu}} (t_{\boldsymbol{\mu},j} - t_{\boldsymbol{\mu},j'})^{2e^{\boldsymbol{\mu},\boldsymbol{\nu}}_{j,j'}} \cdot \prod_{1\le k\le \#\boldsymbol{\nu}} b_{\boldsymbol{\nu},k}^{2f^{\boldsymbol{\mu},\boldsymbol{\nu}}_k} \cdot \prod_{1\le k<k'\le \#\boldsymbol{\nu}} \mathrm{R}(z_{\boldsymbol{\nu},k}, z_{\boldsymbol{\nu},k'})^{2g^{\boldsymbol{\mu},\boldsymbol{\nu}}_{k,k'}},$$

with $e^{\boldsymbol{\mu},\boldsymbol{\nu}}_{j,j'} \le e \in \mathbb{N}_*$ *for* $1 \le j < j' \le \#\boldsymbol{\mu}$, $f^{\boldsymbol{\mu},\boldsymbol{\nu}}_k \le f \in \mathbb{N}_*$ *for* $1 \le k \le \#\boldsymbol{\nu}$ *and* $g^{\boldsymbol{\mu},\boldsymbol{\nu}}_{k,k'} \le g \in \mathbb{N}_*$ *for* $1 \le k < k' \le \#\boldsymbol{\nu}$, *degree in* $w \subset v$ *bounded by* δ_w, *degree in* $t_{\boldsymbol{\mu},j}$ *bounded by* $\delta_t \ge p$ *for* $1 \le j \le \#\boldsymbol{\mu}$, *and degree in* $(a^{\boldsymbol{\nu}}_k, b^{\boldsymbol{\nu}}_k)$ *bounded by* $\delta_z \ge p$ *for* $1 \le k \le \#\boldsymbol{\nu}$. *Then, the final incompatibility has monoid part*

$$\prod_{\substack{m+2n=p \\ (\boldsymbol{\mu},\boldsymbol{\nu})\in\Lambda_m\times\Lambda_n}} S_{\boldsymbol{\mu},\boldsymbol{\nu}}^{h_{\boldsymbol{\mu},\boldsymbol{\nu}}}$$

with $h_{\boldsymbol{\mu},\boldsymbol{\nu}} \le \max\{e,g\}^{2^{\frac{1}{2}p^2}} f^{2^{\frac{1}{2}p}} \mathrm{g}_4\{p\}$ *and degree in* w *bounded by* $\max\{e,g\}^{2^{\frac{1}{2}p^2}} f^{2^{\frac{1}{2}p}} \mathrm{g}_4\{p\}(\delta_w + \max\{\delta_t, \delta_z\} \deg_w P)$.

For the proof of Theorem 4.3.5, we need an auxiliary notation and lemma.

Notation 4.3.6 *To $J \subset \{(j,j') \mid 1 \le j < j' \le m\}$, we associate the smallest equivalence relation $\simeq_J$ on $\{1,\dots,m\}$ such that $(j,j') \in J$ implies $j \simeq_J j'$. We define $\boldsymbol{\mu}_J \in \Lambda_m$ as the non-increasing vector of cardinalities of the equivalence classes for $\simeq_J$ and $\mathcal{C}_1,\dots,\mathcal{C}_{\#\boldsymbol{\mu}_J}$ the equivalence classes defined by $\simeq_J$.*

Similarly, to $K \subset \{(k,k') \mid 1 \le k < k' \le n\}$, we associate the smallest equivalence relation $\simeq_K$ on $\{1,\dots,n\}$ such that $(k,k') \in K$ implies $k \simeq_K k'$. We define $\boldsymbol{\nu}_K \in \Lambda_m$ as the non-increasing vector of cardinalities of the equivalence classes for $\simeq_K$ and $\mathcal{C}'_1,\dots,\mathcal{C}'_{\#\boldsymbol{\nu}_K}$ the equivalence classes defined by $\simeq_K$.

Lemma 4.3.7 *Let $p \ge 1$, $P = y^p + \sum_{0 \le h \le p-1} C_h \cdot y^h \in \mathbf{K}[u][y]$, $m,n \in \mathbb{N}$ with $m+2n = p$, $J \subset \{(j,j') \mid 1 \le j < j' \le m\}$ and $K \subset \{(k,k') \mid 1 \le k < k' \le n\}$. Then*

$$\exists (t',z') \; \Big[\; P \equiv \prod_{1 \le j' \le m} (y - t'_{j'}) \cdot \prod_{1 \le k' \le n} ((y - a'_{k'})^2 + {b'_{k'}}^2), \; \bigwedge_{\substack{1 \le j'_1 < j'_2 \le m,\\ (j'_1,j'_2) \in J}} t'_{j'_1} = t'_{j'_2}, \; \bigwedge_{\substack{1 \le j'_1 < j'_2 \le m,\\ (j'_1,j'_2) \notin J}} t'_{j'_1} \ne t'_{j'_2},$$

$$\bigwedge_{1 \le k' \le n} b'_{k'} \ne 0, \; \bigwedge_{\substack{1 \le k'_1 < k'_2 \le n,\\ (k'_1,k'_2) \in K}} \mathrm{R}(z'_k, z'_{k'}) = 0, \; \bigwedge_{\substack{1 \le k'_1 < k'_2 \le n,\\ (k'_1,k'_2) \notin K}} \mathrm{R}(z'_k, z'_{k'}) \ne 0 \; \Big] \quad \vdash$$

$$\vdash \quad \exists (t,z) \; [\; \mathrm{Fact}(P)^{\boldsymbol{\mu}_J,\boldsymbol{\nu}_K}(t,z) \;],$$

where $t' = (t'_1,\dots,t'_m)$, $z' = (z'_1,\dots,z'_n)$ is a set of complex variables with $z'_{k'} = a'_{k'} + ib'_{k'}$ $t = (t_1,\dots,t_{\#\boldsymbol{\mu}_J})$ and $z = (z_1,\dots,z_{\#\boldsymbol{\nu}_K})$ is a set of complex variables with $z_k = a_k + ib_k$ (see Notation 2.3.1).

Suppose we have an initial incompatibility in $\mathbf{K}[v][t,a,b]$ where $v \supset u$ and t,a,b are disjoint from v, with monoid part

$$S \cdot \prod_{1 \le j < j' \le \#\boldsymbol{\mu}_J} (t_j - t_{j'})^{2e_{j,j'}} \cdot \prod_{1 \le k \le \#\boldsymbol{\nu}_K} b_k^{2f_k} \cdot \prod_{1 \le k < k' \le \#\boldsymbol{\nu}_K} \mathrm{R}(z_k, z_{k'}),^{2g_{k,k'}},$$

with $e_{j,j'} \le e$ for $1 \le j < j' \le \#\boldsymbol{\mu}_J$, $f_k \le f$ for $1 \le k \le \#\boldsymbol{\nu}_K$ and $g_{k,k'} \le g$ for $1 \le k < k' \le \#\boldsymbol{\nu}_K$, degree in $w \subset v$ bounded by δ_w, degree in t_j bounded by $\delta_t \ge p$ for $1 \le j \le \#\boldsymbol{\mu}_J$, and degree in (a_k,b_k) bounded by $\delta_z \ge p$ for $1 \le k \le \#\boldsymbol{\nu}_K$. Then, the final incompatibility has monoid part

$$S^h \cdot \prod_{\substack{1 \le j'_1 < j'_2 \le m,\\ (j'_1,j'_2) \notin J}} (t'_{j'_1} - t'_{j'_2})^{2e'_{j'_1,j'_2}} \cdot \prod_{1 \le k' \le n} {b'_{k'}}^{2f'_{k'}} \cdot \prod_{\substack{1 \le k'_1 < k'_2 \le n,\\ (k'_1,k'_2) \notin K}} \mathrm{R}(z'_k, z'_{k'})^{2g'_{k'_1,k'_2}}$$

with $h \le 2^{n(n-1)}$, $e'_{j'_1,j'_2} \le 2^{n(n-1)} e$ for $1 \le j'_1 < j'_2 \le m, (j'_1,j'_2) \notin J$, $f'_{k'} \le 2^{n(n-1)} f$ for $1 \le k' \le n$ and $g'_{k'_1,k'_2} \le 2^{n(n-1)} g$ for $1 \le k'_1 < k'_2 \le n, (k'_1,k'_2) \notin K$, degree in w bounded by $2^{n(n-1)}\delta_w$, degree in $t'_{j'}$ bounded by $2^{n(n-1)}\delta_t$ for $1 \le j' \le m$, and degree in $(a'_{k'},b'_{k'})$ bounded by $2^{n(n-1)}\delta_z$ for $1 \le k' \le n$.

Proof. Consider the initial incompatibility

$$\downarrow \mathrm{Fact}(P)^{\boldsymbol{\mu}_J,\boldsymbol{\nu}_K}(t,z), \; \mathcal{H} \downarrow_{\mathbf{K}[v][t,a,b]} \tag{23}$$

where $\mathcal{H}$ is a system of sign conditions in $\mathbf{K}[v]$.

First, for $1 \le j \le \#\boldsymbol{\mu}_J$ and $1 \le k \le \#\boldsymbol{\nu}_K$, we choose $\alpha(j) \in \mathcal{C}_j$ and $\beta(k) \in \mathcal{C}'_k$ (using Notation 4.3.6) and we substitute $t_j = t'_{\alpha(j)}$ and $(a_k, b_k) = (a'_{\beta(k)}, b'_{\beta(k)})$ in (23). Then we apply the weak inference

$$P \equiv \prod_{1\le j'\le m} (y - t'_{j'}) \cdot \prod_{1\le k'\le n} ((y-a'_{k'})^2 + {b'_{k'}}^2), \bigwedge_{\substack{1\le j'_1<j'_2\le m,\\ (j'_1,j'_2)\in J}} t'_{j'_1} = t'_{j'_2},$$

$$\bigwedge_{\substack{1\le k'_1<k'_2\le n,\\ (k'_1,k'_2)\in K}} (y-a'_{k'_1})^2 + {b'_{k'_1}}^2 \equiv (y-a'_{k'_2})^2 + {b'_{k'_2}}^2 \quad \vdash$$

$$\vdash \quad P \equiv \mathrm{F}^{\boldsymbol{\mu}_J, \boldsymbol{\nu}_K}.$$

By Lemma 2.1.8, we obtain

$$\Big\downarrow\ P \equiv \prod_{1\le j'\le m} (y - t'_{j'}) \cdot \prod_{1\le k'\le n} ((y-a'_{k'})^2 + {b'_{k'}}^2) \bigwedge_{\substack{1\le j'_1<j'_2\le m,\\ (j'_1,j'_2)\in J}} t'_{j'_1} = t'_{j'_2},$$
$$\bigwedge_{1\le j<j'\le \#\boldsymbol{\mu}_J} t'_{\alpha(j)} \neq t'_{\alpha(j')}, \bigwedge_{1\le k\le \#\boldsymbol{\nu}_K} b'_{\beta(k)} \neq 0, \bigwedge_{\substack{1\le k'_1<k'_2\le n,\\ (k'_1,k'_2)\in K}} (y-a'_{k'_1})^2 + {b'_{k'_1}}^2 \equiv (y-a'_{k'_2})^2 + {b'_{k'_2}}^2,$$
$$\bigwedge_{1\le k<k'\le \#\boldsymbol{\nu}_K} \mathrm{R}(z'_{\beta(k)}, z'_{\beta(k)}) \neq 0,\ \mathcal{H}\ \Big\downarrow_{\mathbf{K}[v][t',a',b']} \tag{24}$$

with monoid part

$$S \cdot \prod_{1\le j<j'\le \#\boldsymbol{\mu}_J} (t'_{\alpha(j)} - t'_{\alpha(j')})^{2e_{j,j'}} \cdot \prod_{1\le k\le \#\boldsymbol{\nu}_K} {b'_{\beta(k)}}^{2f_k} \cdot \prod_{1\le k<k'\le \#\boldsymbol{\nu}_K} \mathrm{R}(z'_{\beta(k)}, z'_{\beta(k')})^{2g_{k,k'}}$$

and, after some analysis, degree in w bounded by δ_w, degree in $t'_{j'}$ bounded by δ_t for $1 \le j' \le m$, and degree in $(a'_{k'}, b'_{k'})$ bounded by δ_z for $1 \le k' \le n$ (using $\delta_t \ge p$ and $\delta_z \ge p$). Note that for $1 \le j < j' \le \#\boldsymbol{\mu}_J$, if $\alpha(j) < \alpha(j')$ then $(\alpha(j), \alpha(j')) \notin J$ and if $\alpha(j') < \alpha(j)$ then $(\alpha(j'), \alpha(j)) \notin J$, and a similar fact holds for $1 \le k < k' \le \#\boldsymbol{\nu}_K$.

Finally, we successively apply to (24) for $(k'_1, k'_2) \in K$ the weak inference

$$\mathrm{R}(z'_{k'_1}, z'_{k'_1}) = 0 \quad \vdash \quad (y-a'_{k'_1})^2 + {b'_{k'_1}}^2 \equiv (y-a'_{k'_2})^2 + {b'_{k'_2}}^2.$$

The proof is easily finished using Lemma 2.4.6. □

Proof of Theorem 4.3.5. Consider for $(\boldsymbol{\mu}, \boldsymbol{\nu}) \in \Lambda_m \times \Lambda_n$ the initial incompatibility

$$\downarrow \mathrm{Fact}(P)^{\boldsymbol{\mu},\boldsymbol{\nu}}(t_{\boldsymbol{\mu}}, z_{\boldsymbol{\nu}}),\ \mathcal{H} \downarrow_{\mathbf{K}[v][t_{\boldsymbol{\mu}}, a_{\boldsymbol{\nu}}, b_{\boldsymbol{\nu}}]} \tag{25}$$

where $\mathcal{H}$ is a system of sign conditions in $\mathbf{K}[v]$.

For each m and n, for each $J \subset \{(j, j') \mid 1 \le j < j' \le m\}$ and $K \subset \{(k, k') \mid 1 \le k < k' \le n\}$, we apply to the incompatibility (25) corresponding to $(\boldsymbol{\mu}_J, \boldsymbol{\nu}_K)$ (see Notation 4.3.6) the weak inference

$$\exists (t_m, z_n)\ \Big[\ P \equiv \prod_{1\le j\le m} (y - t_{m,j}) \cdot \prod_{1\le k\le n} ((y-a_{n,k})^2 + b_{n,k}^2), \bigwedge_{\substack{1\le j<j'\le m,\\ (j,j')\in J}} t_{m,j} = t_{m,j'},$$

$$\bigwedge_{\substack{1\le j<j'\le m,\\(j,j')\notin J}} t_{m,j}\neq t_{m,j'},\ \bigwedge_{1\le k\le n} b_{n,k}\neq 0,\ \bigwedge_{\substack{1\le k<k'\le n,\\(k,k')\in K}} \mathrm{R}(z_{n,k},z_{n,k'})=0,\ \bigwedge_{\substack{1\le k<k'\le n,\\(k,k')\notin K}} \mathrm{R}(z_{n,k},z_{n,k'})\neq 0\ \Big]\ \vdash$$

$$\vdash\quad \exists(t_{\boldsymbol{\mu}_J},z_{\boldsymbol{\nu}_K})\ [\ \mathrm{Fact}(P)^{\boldsymbol{\mu}_J,\boldsymbol{\nu}_K}(t_{\boldsymbol{\mu}_J},z_{\boldsymbol{\nu}_K})\ ],$$

where $t_m=(t_{m,1},\dots,t_{m,m})$ and $z_n=(z_{n,1},\dots,z_{n,n})$. By Lemma 4.3.7 we obtain

$$\begin{aligned}\Big\downarrow P\equiv \prod_{1\le j\le m}(y-t_{m,j})\cdot\prod_{1\le k\le n}((y-a_{n,k})^2+b_{n,k}^2),\ \bigwedge_{\substack{1\le j<j'\le m,\\(j,j')\in J}} t_{m,j}=t_{m,j'},\\ \bigwedge_{\substack{1\le j<j'\le m,\\(j,j')\notin J}} t_{m,j}\neq t_{m,j'},\ \bigwedge_{1\le k\le n} b_{n,k}\neq 0,\\ \bigwedge_{\substack{1\le k<k'\le n,\\(k,k')\in K}} \mathrm{R}(z_{n,k},z_{n,k'})=0,\ \bigwedge_{\substack{1\le k<k'\le n,\\(k,k')\notin K}} \mathrm{R}(z_{n,k},z_{n,k'})\neq 0,\ \mathcal{H}\Big\downarrow_{\mathbf{K}[v][t_m,a_n,b_n]}\end{aligned}\tag{26}$$

with monoid part

$$S_{\boldsymbol{\mu}_J,\boldsymbol{\nu}_K}^{h_{J,K}}\cdot\prod_{\substack{1\le j<j'\le m,\\(j,j')\notin J}}(t_{m,j}-t_{m,j'})^{2e_{J,K,j,j'}}\cdot\prod_{1\le k\le n} b_{n,k}^{2f_{J,K,k}}\cdot\prod_{\substack{1\le k<k'\le n,\\(k,k')\notin K}}\mathrm{R}(z_{n,k},z_{n,k'})^{2g_{J,K,k,k'}}$$

with $h_{J,K}\le 2^{n(n-1)}$, $e_{J,K,j,j'}\le 2^{n(n-1)}e$ for $1\le j<j'\le m,(j,j')\notin J$, $f_{J,K,k}\le 2^{n(n-1)}f$ for $1\le k\le n$ and $g_{J,K,k,k'}\le 2^{n(n-1)}g$ for $1\le k<k'\le n,(k,k')\notin K$, degree in w bounded by $2^{n(n-1)}\delta_w$, degree in $t_{m,j}$ bounded by $2^{n(n-1)}\delta_t$ for $1\le j\le m$ and degree in $(a_{n,k},b_{n,k})$ bounded by $2^{n(n-1)}\delta_z$ for $1\le k\le n$.

Then, for each m and n, we apply to incompatibilities (26) for every $J\subset\{(j,j')\mid 1\le j<j'\le m\}$ and $K\subset\{(k,k')\mid 1\le k<k'\le n\}$, the weak inference

$$P\equiv \prod_{1\le j\le m}(y-t_{m,j})\cdot\prod_{1\le k\le n}((y-a_{n,k})^2+b_{n,k}^2),\ \bigwedge_{1\le k\le n} b_{n,k}\neq 0\quad\vdash$$

$$\begin{aligned}\vdash\ \bigvee_{J,K}\Big(P\equiv \prod_{1\le j\le m}(y-t_{m,j})\cdot\prod_{1\le k\le n}((y-a_{n,k})^2+b_{n,k}^2),\ \bigwedge_{\substack{1\le j<j'\le m,\\(j,j')\in J}} t_{m,j}=t_{m,j'},\ \bigwedge_{\substack{1\le j<j'\le m,\\(j,j')\notin J}} t_{m,j}\neq t_{m,j'},\\ \bigwedge_{1\le k\le n} b_{n,k}\neq 0,\ \bigwedge_{\substack{1\le k<k'\le n,\\(k,k')\in K}} \mathrm{R}(z_{n,k},z_{n,k'})=0,\ \bigwedge_{\substack{1\le k<k'\le n,\\(k,k')\notin K}} \mathrm{R}(z_{n,k},z_{n,k'})\neq 0\Big).\end{aligned}$$

By Lemma 2.1.19 and taking into account that there are at most $2^{\frac{1}{2}p(p-1)}$ pairs of subsets (J,K) and many different pairs may lead to the same pair of vectors $(\boldsymbol{\mu}_J,\boldsymbol{\nu}_K)$, we obtain

$$\Bigg\downarrow P\equiv \prod_{1\le j\le m}(y-t_{m,j})\cdot\prod_{1\le k\le n}((y-a_{n,k})^2+b_{n,k}^2),\ \bigwedge_{1\le k\le n} b_{n,k}\neq 0,\ \mathcal{H}\Bigg\downarrow_{\mathbf{K}[v][t_m,a_n,b_n]}\tag{27}$$

with monoid part

$$\prod_{(\boldsymbol{\mu},\boldsymbol{\nu})\in\Lambda_m\times\Lambda_n} S_{\boldsymbol{\mu},\boldsymbol{\nu}}^{h'_{\boldsymbol{\mu},\boldsymbol{\nu}}}\cdot\prod_{1\le k\le n} b_{n,k}^{2f'_{n,k}}$$

with $h'_{\boldsymbol{\mu},\boldsymbol{\nu}} \leq \max\{e,g\}^{2^{2^{\frac{1}{2}p(p-1)}-1}2^{(n^2-n+2)2^{\frac{1}{2}p(p-1)}-2}}$ and $f'_{n,k} \leq \max\{e,g\}^{2^{2^{\frac{1}{2}p(p-1)}-1}} f 2^{(n^2-n+2)2^{\frac{1}{2}p(p-1)}-2}$ for $1 \leq k \leq n$, degree in w bounded by $\max\{e,g\}^{2^{2^{\frac{1}{2}p(p-1)}-1}2^{(n^2-n+2)2^{\frac{1}{2}p(p-1)}-2}}\delta_w$, degree in $t_{m,j}$ bounded by $\max\{e,g\}^{2^{2^{\frac{1}{2}p(p-1)}-1}2^{(n^2-n+2)2^{\frac{1}{2}p(p-1)}-2}}\delta_t$ for $1 \leq j \leq m$ and degree in $(a_{n,k}, b_{n,k})$ bounded by $\max\{e,g\}^{2^{2^{\frac{1}{2}p(p-1)}-1}2^{(n^2-n+2)2^{\frac{1}{2}p(p-1)}-2}}\delta_z$.

Finally, we apply to incompatibilities (27) for every m and n such that $m+2n=p$ the weak inference

$$\vdash \bigvee_{m+2n=p} \exists(t_m, z_n) \left[P \equiv \prod_{1\leq j\leq m}(y-t_{m,j}) \cdot \prod_{1\leq k\leq n}((y-a_{n,k})^2 + {b_{n,k}}^2), \bigwedge_{1\leq k\leq n} b_{n,k} \neq 0 \right].$$

By Theorem 4.2.4 (Real Irreducible Factors as a weak existence) and using Lemma 4.3.4, we obtain

$$\downarrow \mathcal{H} \downarrow_{\mathbf{K}[v]}$$

with monoid part

$$\prod_{\substack{m+2n=p \\ (\boldsymbol{\mu},\boldsymbol{\nu})\in\Lambda_m\times\Lambda_n}} S_{\boldsymbol{\mu},\boldsymbol{\nu}}^{h_{\boldsymbol{\mu},\boldsymbol{\nu}}}$$

with $h_{\boldsymbol{\mu},\boldsymbol{\nu}} \leq \max\{e,g\}^{2^{2^{\frac{1}{2}p^2}}} f^{2^{2^{\frac{1}{2}p}}} \mathrm{g}_4\{p\}$ and degree in w bounded by $\max\{e,g\}^{2^{2^{\frac{1}{2}p^2}}} f^{2^{2^{\frac{1}{2}p}}} \mathrm{g}_4\{p\}(\delta_w + \max\{\delta_t, \delta_z\} \deg_w P)$, which serves as the final incompatibility. ☐

5 Hermite's Theory

In this section we study Hermite's theory and Sylvester's inertia law in the context of weak inferences and incompatibilities. Hermite's theory has two aspects: on one hand, the rank and signature of Hermite's quadratic form determine the number of real roots, and on the other hand, sign conditions on the principal minors of Hermite's quadratic form also determine its rank and signature.

In Subsection 5.1, we explain how the rank and signature of Hermite's quadratic form is related to real root counting (Theorem 5.1.3) and we transform this statement into a weak inference of a diagonalization formula (Theorem 5.1.11). In Subsection 5.2, we explain that the rank and signature of Hermite's quadratic form are also determined by sign conditions on principal minors, which are closely related to subresultants (Theorem 5.2.2) and we transform this statement into a weak inference of a different diagonalization formula (Theorem 5.2.17). In Subsection 5.3, we produce an incompatibility for Sylvester's inertia law, expressing the impossibility for a quadratic form to have two diagonal forms with distinct rank and signature (Theorem 5.3.6). Finally in Subsection 5.4, combining results from the preceding subsections, we produce an incompatibility expressing the impossibility for a polynomial to have a number of real roots in conflict with the rank and signature of its Hermite's quadratic form predicted by the signs of its principal minors (Theorem 5.4.3).

In this section we use many results from Section 2, but it is absolutely independent from the results from Section 3 and Section 4.

On the other hand, the only result extracted from Section 5 used in the rest of the paper is Theorem 5.4.3 (Hermite's Theory as an incompatibility), which produces an incompatibility used only twice in Section 6.

5.1 Signature of Hermite's quadratic form and real root counting

In this section, $\mathbf{K}$ is as usual an ordered field and $\mathbf{R}$ is a real closed field containing $\mathbf{K}$. Moreover, $\mathbf{D}$ is a domain and $\mathbf{F}$ is a field of characteristic 0 containing $\mathbf{D}$. A typical example of this situation is the following: $\mathbf{K}$ is the field of rational numbers, $\mathbf{R}$ the field of real algebraic numbers, $\mathbf{D} = \mathbf{K}[c]$ the polynomials in a finite number of variables with coefficients in $\mathbf{K}$ and $\mathbf{F}$ the corresponding field of fractions.

We now recall the definition of Hermite's quadratic form [26, 4] and its role in real root counting.

Notation 5.1.1 *For a symmetric matrix $\boldsymbol{A} \in \mathbf{K}^{p\times p}$, we denote by $\mathrm{Si}(\boldsymbol{A})$ and $\mathrm{Rk}(\boldsymbol{A})$ the signature and rank of $\boldsymbol{A}$ respectively.*

Definition 5.1.2 (Hermite Quadratic Form) *Let $P, Q \in \mathbf{D}[y]$ with $\deg P = p \geq 1$ and P monic. The Hermite's matrix $\mathrm{Her}(P;Q) \in \mathbf{D}^{p\times p}$ is the matrix defined for $1 \leq j_1, j_2 \leq p$ by*

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

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

Theorem 5.1.3 (Hermite's Theory (1)) *Let $P, Q \in \mathbf{K}[y]$ with $= p \geq 1$, P monic. Then*

$$\begin{aligned} \mathrm{Rk}(\mathrm{Her}(P;Q)) &= \#\{\alpha + i\beta \in \mathbf{R}[i] \mid P(\alpha+i\beta) = 0, Q(\alpha+i\beta) \neq 0\}, \\ \mathrm{Si}(\mathrm{Her}(P;Q)) &= \#\{\theta \in \mathbf{R} \mid P(\theta) = 0, Q(\theta) > 0\} - \#\{\theta \in \mathbf{R} \mid P(\theta) = 0, Q(\theta) < 0\}. \end{aligned}$$

Even though this result is well known, we give here a detailed proof of Theorem 5.1.3 which we will follow later on to obtain a weak inference counterpart of it. We introduce first some more auxiliary notation and definitions.

Definition 5.1.4 *For $\alpha \in \mathbf{R}$, its sign is defined as follows:*

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

From now on, for $P \in \mathbf{K}[v], \tau \in \{-1, 0, 1\}$, we freely use $\mathrm{sign}(P) = \tau$, *to mean*

$$\begin{cases} P = 0 & \text{if } \tau = 0, \\ P > 0 & \text{if } \tau = 1, \\ P < 0 & \text{if } \tau = -1. \end{cases}$$

Similarly we define the invertibility of an element of $\mathbf{R}[i]$.

Definition 5.1.5 *For $\alpha + i\beta \in \mathbf{R}[i]$, its invertibility is defined as follows:*

$$\begin{cases} \mathrm{inv}(\alpha + i\beta) = 0 & \text{if } \alpha = 0,\ \beta = 0, \\ \mathrm{inv}(\alpha + i\beta) = 1 & \text{if } \alpha^2 + \beta^2 \neq 0. \end{cases}$$

From now on, for $P(z) = P_{\mathrm{Re}}(a,b) + iP_{\mathrm{Im}}(a,b) \in \mathbf{K}[i][v][z], \kappa \in \{0,1\}$, we freely use $\mathrm{inv}(P) = \kappa$, *to mean*

$$\begin{cases} P_{\mathrm{Re}}(a,b) = 0,\ P_{\mathrm{Im}}(a,b) = 0 & \text{if } \kappa = 0, \\ P_{\mathrm{Re}}(a,b)^2 + P_{\mathrm{Im}}(a,b)^2 \neq 0 & \text{if } \kappa = 1. \end{cases}$$

Remark 5.1.6 *If $\boldsymbol{D} \in \mathbf{K}^{p \times p}$ is a diagonal matrix, with diagonal elements $D_1, \ldots, D_p$,*

$$\begin{aligned} \mathrm{Rk}(\boldsymbol{D}) &= \sum_{1 \leq i \leq p} \mathrm{inv}(D_i), \\ \mathrm{Si}(\boldsymbol{D}) &= \sum_{1 \leq i \leq p} \mathrm{sign}(D_i). \end{aligned}$$

Notation 5.1.7

- *For $p \in \mathbb{N}_*$ and $j \in \mathbb{N}$ we denote by $\mathrm{A}_{p,j} \in \mathbb{Z}[c_0, \ldots, c_{p-1}]$ the unique polynomial such that*

$$\mathrm{A}_{p,j}\Big(\mathrm{Coef}(y_1, \ldots, y_p)\Big) = \sum_{1 \leq k \leq p} y_k^j \in \mathbb{Z}[y_1, \ldots, y_p],$$

where $\mathrm{Coef}(y_1,\dots,y_p)$ *is the vector whose* j*-th entry,* $j=0,\dots,p-1$*, is*

$$\mathrm{Coef}_j(y_1,\dots,y_p)=(-1)^{p-j}\sum_{\substack{K\subset\{1,\dots,p\}\\|K|=p-j}}\prod_{k\in K}y_k.$$

Note that $\deg \mathrm{A}_{p,j}=j$ *(see [13, Proof of Theorem 3, Chapter 7]).*

- *For* $j\in\mathbb{N}$ *and* $(\boldsymbol{\mu},\boldsymbol{\nu})\in\Lambda_m\times\Lambda_n$*, let* $t=(t_1,\dots,t_{\#\boldsymbol{\mu}})$ *,* $a=(a_1,\dots,a_{\#\boldsymbol{\nu}})$*,* $b=(b_1,\dots,b_{\#\boldsymbol{\nu}})$ *be sets of variables ,* $z_i=a_i+b_i$ *and* $z=(z_1,\dots,z_{\#\boldsymbol{\nu}})$*. We denote by* $\mathrm{N}_j^{\boldsymbol{\mu},\boldsymbol{\nu}}\in\mathbb{Z}[t,a,b]$ *the Newton sum polynomial*

$$\mathrm{N}_j^{\boldsymbol{\mu},\boldsymbol{\nu}}=\sum_{1\le i\le\#\boldsymbol{\mu}}\mu_i t_i^j+\sum_{1\le k\le\#\boldsymbol{\nu}}2\nu_k(z_k^j)_{\mathrm{Re}}.$$

Remark 5.1.8

- *Let* $p\in\mathbb{N}_*$*,* $(\boldsymbol{\mu},\boldsymbol{\nu})\in\Lambda_m\times\Lambda_n$ *with* $m+2n=p$*,* $t=(t_1,\dots,t_{\#\boldsymbol{\mu}})$ *is a set of variables and* $z=(z_1,\dots,z_{\#\boldsymbol{\nu}})$ *is a set of complex variables. Following Definition 4.3.2, for* $j\in\mathbb{N}$ *we have*

$$\mathrm{A}_{p,j}(\mathrm{F}_0^{\boldsymbol{\mu},\boldsymbol{\nu}}(t,z),\dots,\mathrm{F}_{p-1}^{\boldsymbol{\mu},\boldsymbol{\nu}}(t,z))=\mathrm{N}_j^{\boldsymbol{\mu},\boldsymbol{\nu}}(t,z)$$

in $\mathbb{Z}[t,a,b]$.

- *Let* $p\in\mathbb{N}_*$*,* $P=y^p+\sum_{0\le h\le p-1}\gamma_h y^h$*,* $Q=\sum_{0\le h\le q}\gamma'_h y^h\in\mathbf{D}[y]$*. For* $1\le j_1,j_2\le p$*,*

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

(see [4, Proposition 4.54]).

Notation 5.1.9 *Let* $p\in\mathbb{N}_*$*,* $(\boldsymbol{\mu},\boldsymbol{\nu})\in\Lambda_m\times\Lambda_n$ *with* $m+2n=p$*,* $t=(t_1,\dots,t_{\#\boldsymbol{\mu}})$ *and* $z=(z_1,\dots,z_{\#\boldsymbol{\nu}})$*.*

- *For* $\boldsymbol{\kappa}\in\{0,1\}^{\{1,\dots,\#\boldsymbol{\nu}\}}$*, we denote* $\mathrm{Di}_Q^{\boldsymbol{\mu},\boldsymbol{\nu},\boldsymbol{\kappa}}(t)$ *the diagonal matrix with entries*

$$(\mu_1 Q(t_1),\dots,\mu_{\#\boldsymbol{\mu}}Q(t_{\#\boldsymbol{\mu}}),\nu_1\kappa_1,-\nu_1\kappa_1,\dots,\dots,\nu_{\#\boldsymbol{\nu}}\kappa_{\#\boldsymbol{\nu}},-\nu_{\#\boldsymbol{\nu}}\kappa_{\#\boldsymbol{\nu}},0,\dots,0).$$

- *We denote by* $\mathrm{V}(t,z)$ *the* $p \times p$ *matrix*

$$\begin{pmatrix}
1 & \dots & 1 & 1 & 0 & \dots & \dots & 1 & 0 & 0 & \dots & 0 \\
t_1 & \dots & t_{\#\boldsymbol{\mu}} & a_1 & b_1 & \dots & \dots & a_{\#\boldsymbol{\nu}} & b_{\#\boldsymbol{\nu}} & 0 & \dots & 0 \\
\vdots & & \vdots & \vdots & \vdots & & & \vdots & \vdots & \vdots & & \vdots \\
\vdots & & \vdots & \vdots & \vdots & & & \vdots & \vdots & \vdots & & \vdots \\
\vdots & & \vdots & \vdots & \vdots & & & \vdots & \vdots & \vdots & & \vdots \\
\vdots & & \vdots & \vdots & \vdots & & & \vdots & \vdots & \vdots & & \vdots \\
\vdots & & \vdots & \vdots & \vdots & & & \vdots & \vdots & \vdots & & \vdots \\
\vdots & & \vdots & \vdots & \vdots & & & \vdots & \vdots & \vdots & & \vdots \\
\vdots & & \vdots & \vdots & \vdots & & & \vdots & \vdots & 0 & & 0 \\
\vdots & & \vdots & \vdots & \vdots & & & \vdots & \vdots & 1 & \dots & 0 \\
\vdots & & \vdots & \vdots & \vdots & & & \vdots & \vdots & \vdots & \ddots & \vdots \\
t_1^{p-1} & \dots & t_{\#\boldsymbol{\mu}}^{p-1} & (z_1^{p-1})_{\mathrm{Re}} & (z_1^{p-1})_{\mathrm{Im}} & \dots & \dots & (z_{\#\boldsymbol{\nu}}^{p-1})_{\mathrm{Re}} & (z_{\#\boldsymbol{\nu}}^{p-1})_{\mathrm{Im}} & 0 & \dots & 1
\end{pmatrix}.$$

- *For* $\boldsymbol{\kappa} \in \{0,1\}^{\{1,\dots,\#\boldsymbol{\nu}\}}$ *and* $z' = (z'_k)_{\kappa_k=1}$ *we denote by* $\mathrm{Sq}_{\boldsymbol{\kappa}}(z')$ *the* $p \times p$ *block diagonal matrix having the first* $\#\boldsymbol{\mu}$ *diagonal elements equal* 1*, the next* $\#\boldsymbol{\nu}$ *diagonal blocks of size* 2 *equal to*

$$\begin{cases} \begin{pmatrix} a'_k & b'_k \\ -b'_k & a'_k \end{pmatrix} & \text{if } \kappa_k = 1, \\ \text{the identity matrix of size } 2 & \text{if } \kappa_k = 0, \end{cases}$$

and the last $p - \#\boldsymbol{\mu} - 2\#\boldsymbol{\nu}$ *diagonal elements equal to* 1.

- *We denote by* $\mathrm{B}_{\boldsymbol{\kappa}}(t,z,z')$ *the matrix* $\mathrm{V}(t,z) \cdot \mathrm{Sq}_{\boldsymbol{\kappa}}(z')$.

Lemma 5.1.10

$$\det(\mathrm{V}(t,z)) = \prod_{1 \le j < j' \le \#\boldsymbol{\mu}} (t_{j'} - t_j) \cdot \prod_{\substack{1 \le j \le \#\boldsymbol{\mu}, \\ 1 \le k \le \#\boldsymbol{\nu}}} ((a_k - t_j)^2 + b_k^2) \cdot \prod_{1 \le k \le \#\boldsymbol{\nu}} b_k \cdot \prod_{1 \le k < k' \le \#\boldsymbol{\nu}} \mathrm{R}(z_k, z_{k'}).$$

Proof. Easy computation from the formula for the usual Vandermonde determinant. □

We can now give a proof of Theorem 5.1.3 (Hermite's Theory (1)).

Proof of Theorem 5.1.3. Consider the decomposition of P into irreducible factors in $\mathbf{R}[y]$

$$P = \prod_{1 \le j \le \#\boldsymbol{\mu}} (y - \theta_j)^{\mu_j} \cdot \prod_{1 \le k \le \#\boldsymbol{\nu}} ((y - \alpha_k)^2 + \beta_k^2)^{\nu_k},$$

with $\theta = (\theta_1, \dots, \theta_{\#\boldsymbol{\mu}}) \in \mathbf{R}^{\#\boldsymbol{\mu}}, \alpha = (\alpha_1, \dots, \alpha_{\#\boldsymbol{\nu}}) \in \mathbf{R}^{\#\boldsymbol{\nu}}$ and $\beta = (\beta_1, \dots, \beta_{\#\boldsymbol{\nu}}) \in \mathbf{R}^{\#\boldsymbol{\nu}}$ and $\boldsymbol{\kappa} \in \{0,1\}^{\{1,\dots,\#\boldsymbol{\nu}\}}$ defined by $\kappa_k = 1$ if $Q(\alpha_k + i\beta_k) \neq 0$ and $\kappa_k = 0$ otherwise.

For $1 \leq k \leq \#\boldsymbol{\nu}$ with $\kappa_k = 1$, we consider a square root $\alpha'_k + i\beta'_k$ of $2Q(\alpha_k + i\beta_k)$. Since $\det(\mathrm{V}(\theta, \alpha + i\beta)) \neq 0$ by Lemma 5.1.10 and $\det(\mathrm{Sq}_{\boldsymbol{\kappa}}(\alpha' + i\beta')) \neq 0$ by an easy computation, we have that $\det(\mathrm{B}_{\boldsymbol{\kappa}}(\theta, \alpha + i\beta, \alpha' + i\beta')) \neq 0$.

Using Remark 5.1.8, it can be checked that

$$\mathrm{Her}(P; Q) = \mathrm{B}_{\boldsymbol{\kappa}}(\theta, \alpha + i\beta, \alpha' + i\beta') \cdot \mathrm{Di}_Q^{\boldsymbol{\mu},\boldsymbol{\nu},\boldsymbol{\kappa}}(\theta) \cdot \mathrm{B}_{\boldsymbol{\kappa}}(\theta, \alpha + i\beta, \alpha' + i\beta')^{\mathrm{t}}.$$

The proof concludes then by simply noting that, by Remark 5.1.6,

$$\begin{aligned} \mathrm{Rk}(\mathrm{Di}_Q^{\boldsymbol{\mu},\boldsymbol{\nu},\boldsymbol{\kappa}}(\theta)) &= \#\{\alpha + i\beta \in \mathbf{R}[i] \mid P(\alpha + i\beta) = 0, Q(\alpha + i\beta) \neq 0\}, \\ \mathrm{Si}(\mathrm{Di}_Q^{\boldsymbol{\mu},\boldsymbol{\nu},\boldsymbol{\kappa}}(\theta)) &= \#\{\theta \in \mathbf{R} \mid P(\theta) = 0, Q(\theta) > 0\} - \#\{\theta \in \mathbf{R} \mid P(\theta) = 0, Q(\theta) < 0\}. \end{aligned}$$

□

Now we give a weak inference version of Theorem 5.1.3 (Hermite's Theory (1)), using Definition 4.3.2. Note that for the first time in this paper, the set of variables w in the statement of the theorem is not an arbitrary set of variables included in v. This is enough for our purposes and enables us to obtain a more precise result. In fact, many times from here on we will make a similar distinction for the set of variables w.

Theorem 5.1.11 (Hermite's Theory (1) as a weak existence) *Let* $p \geq 1$, $P = y^p + \sum_{0 \leq h \leq p-1} C_h \cdot y^h \in \mathbf{K}[u][y]$, m, $n \in \mathbb{N}$ *with* $m + 2n = p$, $(\boldsymbol{\mu}, \boldsymbol{\nu}) \in \Lambda_m \times \Lambda_n$, $t = (t_1, \ldots, t_{\#\boldsymbol{\mu}})$, $z = (z_1, \ldots, z_{\#\boldsymbol{\nu}})$, $Q = \sum_{0 \leq h \leq q} D_h \cdot y^h \in \mathbf{K}[u][y]$, $\boldsymbol{\kappa} \in \{0, 1\}^{\{1, \ldots, \#\boldsymbol{\nu}\}}$ *and* $s(\boldsymbol{\kappa}) = \#\{k \mid 1 \leq k \leq \#\boldsymbol{\nu}, \kappa_k = 1\}$. *Then*

$$\mathrm{Fact}(P)^{\boldsymbol{\mu},\boldsymbol{\nu}}(t, z), \quad \bigwedge_{1 \leq k \leq \#\boldsymbol{\nu}} \mathrm{inv}(Q(z_k)) = \kappa_k \quad \vdash$$

$$\vdash \quad \exists z' \; [\, \mathrm{Her}(P; Q) \equiv \mathrm{B}_{\boldsymbol{\kappa}}(t, z, z') \cdot \mathrm{Di}_Q^{\boldsymbol{\mu},\boldsymbol{\nu},\boldsymbol{\kappa}}(t) \cdot \mathrm{B}_{\boldsymbol{\kappa}}(t, z, z')^{\mathrm{t}}, \; \det(\mathrm{B}_{\kappa}(t, z, z')) \neq 0 \,]$$

where $z' = (z'_k)_{\kappa_k = 1}$.

Suppose we have an initial incompatibility in variables (v, a', b') *where* $v \supset (u, t, a, b)$ *and* (a', b') *are disjoint from* v, *with monoid part* $S \cdot \det(\mathrm{B}_{\boldsymbol{\kappa}}(t, z, z'))^{2e}$, *degree in* w *bounded by* δ_w *for some subset of variables* $w \subset v$ *disjoint from* (t, a, b), *degree in* t_j *bounded by* δ_t, *degree in* (a_k, b_k) *bounded by* δ_z *and degree in* (a'_k, b'_k) *bounded by* $\delta_{z'}$. *Then the final incompatibility has monoid part*

$$S^{2^{2s(\boldsymbol{\kappa})}} \cdot \prod_{1 \leq j < j' \leq \#\boldsymbol{\mu}} (t_{j'} - t_j)^{2^{2s(\boldsymbol{\kappa})+1} e} \cdot \prod_{1 \leq k \leq \#\boldsymbol{\nu}} b_k^{2^{2s(\boldsymbol{\kappa})+1}(2\#\boldsymbol{\mu}+1)e} \cdot$$

$$\cdot \prod_{1 \leq k < k' \leq \#\boldsymbol{\nu}} \mathrm{R}(z_k, z_{k'})^{2^{2s(\boldsymbol{\kappa})+1} e} \cdot \prod_{\substack{1 \leq k \leq \#\boldsymbol{\nu}, \\ \kappa_k = 1}} (Q^2_{\mathrm{Re}}(z_k) + Q^2_{\mathrm{Im}}(z_k))^{2e'_k}$$

with $e'_k \leq 2^{2s(\boldsymbol{\kappa})-2}(2e+1)$, *degree in* w *bounded by*

$$2^{2s(\boldsymbol{\kappa})} \Big(\delta_w + (2s(\boldsymbol{\kappa})(3e + \delta_{z'}) + q + 2p + 6) \max\{\deg_w P, \deg_w Q\} \Big),$$

degree in t_j *bounded by* $2^{2s(\boldsymbol{\kappa})}(\delta_t + q + 2p - 2)$ *and degree in* (a_k, b_k) *bounded by* $2^{2s(\boldsymbol{\kappa})}(\delta_z + (6 + 2(3e + \delta_{z'}))q + 2p - 2)$.

Proof. We apply to the initial incompatibility the weak inference

$$\mathrm{Fact}(P)^{\boldsymbol{\mu},\boldsymbol{\nu}}(t,z),\quad \bigwedge_{\substack{1\le j\le \#\boldsymbol{\mu},\\ 1\le k\le \#\boldsymbol{\nu}}} (a_k-t_j)^2+b_k^2\neq 0,\quad \bigwedge_{\substack{1\le k\le \#\boldsymbol{\nu},\\ \kappa_k=1}} z'_k\neq 0 \quad\vdash\quad \det(\mathrm{B}_{\boldsymbol{\kappa}}(t,z,z'))\neq 0.$$

By Lemma 2.1.2 (item 6) according to Lemma 5.1.10, we obtain an incompatibility with monoid part

$$S\cdot\Big(\prod_{1\le j<j'\le\#\boldsymbol{\mu}}(t_{j'}-t_j)\cdot\prod_{\substack{1\le j\le \#\boldsymbol{\mu},\\ 1\le k\le \#\boldsymbol{\nu}}}((a_k-t_j)^2+b_k^2)\cdot\prod_{1\le k\le\#\boldsymbol{\nu}} b_k\cdot\prod_{1\le k<k'\le\#\boldsymbol{\nu}}\mathrm{R}(z_k,z_{k'})\cdot\prod_{\substack{1\le k\le \#\boldsymbol{\nu},\\ \kappa_k=1}}({a'_k}^2+{b'_k}^2)\Big)^{2e}$$

and the same degree bounds.

Then we successively apply for $1\le j\le\#\boldsymbol{\mu}$ and $1\le k\le\#\boldsymbol{\nu}$ the weak inferences

$$\begin{aligned}
(a_k-t_j)^2+b_k^2>0 \quad&\vdash\quad (a_k-t_j)^2+b_k^2\neq 0,\\
(a_k-t_j)^2\ge 0,\ b_k^2>0 \quad&\vdash\quad (a_k-t_j)^2+b_k^2>0,\\
&\vdash\quad (a_k-t_j)^2\ge 0,\\
b_k\neq 0 \quad&\vdash\quad b_k^2>0.
\end{aligned}$$

By Lemmas 2.1.2 (items 2, 3 and 4) and 2.1.7, we obtain an incompatibility with monoid part

$$S\cdot\prod_{1\le j<j'\le\#\boldsymbol{\mu}}(t_{j'}-t_j)^{2e}\cdot\prod_{1\le k\le\#\boldsymbol{\nu}} b_k^{2(2\#\boldsymbol{\mu}+1)e}\cdot\prod_{1\le k<k'\le\#\boldsymbol{\nu}}\mathrm{R}(z_k,z_{k'})^{2e}\cdot\prod_{\substack{1\le k\le \#\boldsymbol{\nu},\\ \kappa_k=1}}({a'_k}^2+{b'_k}^2)^{2e}$$

and the same degree bounds.

For $1\le j_1,j_2\le p$, by Remark 5.1.8, we have

$$\begin{aligned}
&\mathrm{Her}(P;Q)_{j_1,j_2}-(\mathrm{B}_{\boldsymbol{\kappa}}(t,z,z')\cdot \mathrm{Di}_Q^{\boldsymbol{\mu},\boldsymbol{\nu},\boldsymbol{\kappa}}(t)\cdot\mathrm{B}_{\boldsymbol{\kappa}}(t,z,z')^{\mathrm{t}})_{j_1,j_2}=\\
&=\sum_{0\le h\le q} D_h\cdot\Big(\mathrm{A}_{p,h+j_1+j_2-2}(C_0,\ldots,C_{p-1})-\mathrm{A}_{p,h+j_1+j_2-2}(\mathrm{F}_0^{\boldsymbol{\mu},\boldsymbol{\nu}}(t,z),\ldots,\mathrm{F}_{p-1}^{\boldsymbol{\mu},\boldsymbol{\nu}}(t,z))\Big)+\\
&+\sum_{\substack{1\le k\le \#\boldsymbol{\nu},\\ \kappa_k=0}} 2\nu_k\Big(Q(z_k)_{\mathrm{Re}}(z_k^{j_1+j_2-2})_{\mathrm{Re}}-Q(z_k)_{\mathrm{Im}}(z_k^{j_1+j_2-2})_{\mathrm{Im}}\Big)+\\
&+\sum_{\substack{1\le k\le \#\boldsymbol{\nu},\\ \kappa_k=1}} \nu_k\Big(\big(2Q(z_k)_{\mathrm{Re}}-({a'_k}^2-{b'_k}^2)\big)\cdot(z_k^{j_1+j_2-2})_{\mathrm{Re}}-\big(2Q(z_k)_{\mathrm{Im}}-2a'_kb'_k\big)\cdot(z_k^{j_1+j_2-2})_{\mathrm{Im}}\Big).
\end{aligned}$$

Therefore, we apply the weak inference

$$\begin{aligned}
\mathrm{Fact}(P)^{\boldsymbol{\mu},\boldsymbol{\nu}}(t,z),\quad \bigwedge_{\substack{1\le k\le \#\boldsymbol{\nu},\\ \kappa_k=0}} Q(z_k)=0,\quad \bigwedge_{\substack{1\le k\le \#\boldsymbol{\nu},\\ \kappa_k=1}} {z'_k}^2=2Q(z_k)\quad\vdash&\\
\vdash\quad \mathrm{Her}(P;Q)\equiv \mathrm{B}_{\boldsymbol{\kappa}}(t,z,z')\cdot\mathrm{Di}_Q^{\boldsymbol{\mu},\boldsymbol{\nu},\boldsymbol{\kappa}}(t)\cdot\mathrm{B}_{\boldsymbol{\kappa}}(t,z,z')^{\mathrm{t}}.&
\end{aligned}$$

By Lemma 2.1.8, after some analysis, we obtain an incompatibility with the same monoid part, degree in w bounded by $\delta_w+\deg_w Q+(q+2p-2)\deg_w P$, degree in t_j bounded by $\delta_t+q+2p-2$, degree in (a_k,b_k) bounded by $\delta_z+q+2p-2$ and degree in (a'_k,b'_k) bounded by $\delta_{z'}$.

Suppose that $\{k \mid 1 \leq k \leq \#\boldsymbol{\nu}, \kappa_k = 1\} = \{k_1, \dots, k_{s(\boldsymbol{\kappa})}\}$. Finally we apply for $1 \leq s \leq s(\boldsymbol{\kappa})$ the weak inference

$$Q(z_{k_s}) \neq 0 \quad \vdash \quad \exists z'_{k_s} \ [\ z'_{k_s} \neq 0,\ {z'_{k_s}}^2 = 2Q(z_{k_s})\ ].$$

Using Lemma 2.3.2, it is easy to prove by induction on s that, for $1 \leq s \leq s(\boldsymbol{\kappa})$, after the application of the weak inference corresponding to index s, we obtain an incompatibility with monoid part

$$S^{2^{2s}} \cdot \prod_{1 \leq j < j' \leq \#\boldsymbol{\mu}} (t_{j'} - t_j)^{2^{2s+1}e} \cdot \prod_{1 \leq k \leq \#\boldsymbol{\nu}} b_k^{2^{2s+1}(2\#\boldsymbol{\mu}+1)e} \cdot$$

$$\cdot \prod_{1 \leq k < k' \leq \#\boldsymbol{\nu}} \mathrm{R}(z_k, z_{k'})^{2^{2s+1}e} \cdot \prod_{1 \leq i \leq s} (Q^2_{\mathrm{Re}}(z_{k_i}) + Q^2_{\mathrm{Im}}(z_{k_i}))^{2^{2s}e + 2^{2s-2i+1}} \cdot \prod_{s+1 \leq i \leq s(\boldsymbol{\kappa})} ({a'_{k_i}}^2 + {b'_{k_i}}^2)^{2^{2s+1}e},$$

degree in w bounded by $2^{2s}(\delta_w + \deg_w Q + (q + 2p - 2)\deg_w P) + (\frac{20}{3}(2^{2s} - 1) + s2^{2s+1}(3e + \delta_{z'}))\deg_w Q$, degree in t_j bounded by $2^{2s}(\delta_t + q + 2p - 2)$, degree in (a_k, b_k) bounded by $2^{2s}(\delta_z + q + 2p - 2)$, degree in (a_{k_i}, b_{k_i}) bounded by $2^{2s}(\delta_z + q + 2p - 2) + 2^{2(s-i)}(20 + 2^{2i+1}(3e + \delta_{z'}))q$ for $1 \leq i \leq s$, degree in (a_{k_i}, b_{k_i}) bounded by $2^{2s}(\delta_z + q + 2p - 2)$ for $s + 1 \leq i \leq s(\boldsymbol{\kappa})$ and degree in (a'_{k_i}, b'_{k_i}) bounded by $2^{2s}\delta_{z'}$ for $s + 1 \leq i \leq s(\boldsymbol{\kappa})$. Therefore, the incompatibility we obtain after the application of the $s(\boldsymbol{\kappa})$ weak inferences serves as the final incompatibility. □

5.2 Signature of Hermite's quadratic form and signs of principal minors

The preceeding method to compute the signature of the Hermite's quadratic form is based on the factorization of P over a real closed field; therefore, it involves algebraic numbers. We explain now another way to compute this signature using only operations in the ring of coefficients of P and Q, through the principal minors of the Hermite's matrix. Most of these results are classical [20, 4] but we need them under precise algebraic identity form.

Notation 5.2.1

- *Let $P, Q \in \mathbf{D}[y]$ with $\deg P = p \geq 1$ and P monic. For $0 \leq j \leq p-1$, we denote by $\mathrm{HMi}_j(P;Q)$ the $(p-j)$-th principal minor of $\mathrm{Her}(P;Q)$ and by $\mathrm{HMi}(P;Q)$ the list $[\mathrm{HMi}_0(P;Q), \dots, \mathrm{HMi}_{p-1}(P;Q)]$ in $\mathbf{D}$. We additionally define $\mathrm{HMi}_p(P;Q) = 1$.*
- *Given a sign condition $\tau \in \{-1, 0, 1\}^{\{0,\dots,p-1\}}$ we denote by $d(\tau)$ the strictly decreasing sequence $(d_0, \dots, d_s)$ of natural numbers defined by $d_0 = p$ and $\{d_1, \dots, d_s\} = \{j \mid 0 \leq j \leq p-1, \tau(j) \neq 0\}$.*
- *For $k \in \mathbb{N}, \varepsilon_k = (-1)^{k(k-1)/2}$.*

Theorem 5.2.2 (Hermite's Theory (2)) *Let $P, Q \in \mathbf{K}[y]$ with $\deg P = p \geq 1$, P monic, $\tau \in \{-1, 0, 1\}^{\{0,\dots,p-1\}}$ be the sign condition defined by $\tau(i) = \mathrm{sign}(\mathrm{HMi}_i(P;Q))$ and $d(\tau) = (d_0, \dots, d_s)$. Then*

$$\begin{aligned} \mathrm{Rk}(\mathrm{Her}(P;Q)) &= p - d_s, \\ \mathrm{Si}(\mathrm{Her}(P;Q)) &= \sum_{\substack{1 \leq i \leq s, \\ d_{i-1} - d_i \text{ odd}}} \varepsilon_{d_{i-1} - d_i} \tau(d_{i-1}) \tau(d_i). \end{aligned}$$

As in the previous subsection, even though this result is well known, we give here a detailed proof of Theorem 5.2.2 which we will follow later on to obtain a weak inference counterpart of it. First, we introduce some more notations and definitions, in order to make a link between Hermite's matrix and subresultants.

Definition 5.2.3 (Subresultants) *Let $P, R \in \mathbf{D}[y]$ with $\deg P = p \geq 1$ and $\deg R = r < p$.*

- *For $0 \leq j \leq r$, the Sylvester-Habicht matrix $\mathrm{SyHa}_j(P,R) \in \mathbf{D}^{(p+r-2j)\times(p+r-j)}$ is the matrix whose rows are the polynomials*
$$y^{r-j-1} \cdot P, \ldots, P, R, \ldots, y^{p-j-1} \cdot R,$$
expressed in the monomial basis $y^{p+r-j-1}, \ldots, y, 1$.

- *For $0 \leq j \leq r$, the j-th subresultant polynomial of P, R, $\mathrm{sResP}_j(P,R) \in \mathbf{D}[y]$ is the polynomial determinant of $\mathrm{SyHa}_j(P,R)$, i.e.*
$$\mathrm{sResP}_j(P,R) = \sum_{0 \leq i \leq j} \det(\mathrm{SyHa}_{j,i}(P,R)) \cdot y^i$$
where $\mathrm{SyHa}_{j,i}(P,R) \in \mathbf{D}^{(p+r-2j)\times(p+r-2j)}$ is the matrix obtained by taking the $p+r-2j-1$ first columns and the $(p+r-j-i)$-th column of $\mathrm{SyHa}_j(P,R)$.

  By convention, we extend this definition with
$$\begin{aligned} \mathrm{sResP}_p(P,R) &= P, \\ \mathrm{sResP}_{p-1}(P,R) &= R, \\ \mathrm{sResP}_j(P,R) &= 0 \qquad \text{for } r < j < p-1. \end{aligned}$$

- *For $0 \leq j \leq r$, the j-th signed subresultant coefficient of P and R, $\mathrm{sRes}_j(P,R) \in \mathbf{D}$ is the coefficient of y^j in $\mathrm{sResP}_j(P,R)$.*

  By convention, we extend this definition with
$$\begin{aligned} \mathrm{sRes}_p(P,R) &= 1, \\ \mathrm{sRes}_j(P,R) &= 0 \qquad \text{for } r < j \leq p-1. \end{aligned}$$

- *For $0 \leq j \leq p$, $\mathrm{sResP}_j(P,R)$ is said to be defective if $\deg \mathrm{sResP}_j(P,R) < j$ or, equivalently, if $\mathrm{sRes}_j(P,R) = 0$.*

- *For $0 \leq j \leq r$, the j-th subresultant cofactors of P, R, $\mathrm{sResU}_j(P,R), \mathrm{sResV}_j(P,R) \in \mathbf{D}[y]$ are the determinants of the matrices obtained by taking the first $p+r-2j-1$ first columns of $\mathrm{SyHa}_j(P,R)$ and a last column equal to $(y^{r-j-1}, \ldots, 1, 0, \ldots, 0)$ and equal to $(0, \ldots, 0, 1, \ldots, y^{p-j-1})$, respectively.*

  By convention we extend these definitions with
$$\begin{aligned} \mathrm{sResU}_p(P,R) &= 1, & \mathrm{sResV}_p(P,R) &= 0, \\ \mathrm{sResU}_{p-1}(P,R) &= 0, & \mathrm{sResV}_{p-1}(P,R) &= 1, \\ \mathrm{sResU}_j(P,R) &= 0, & \mathrm{sResV}_j(P,R) &= 0 \qquad \text{for } r < j < p-1, \\ \mathrm{sResU}_{-1}(P,R) &= -\mathrm{sRes}_0(P,R) \cdot R, & \mathrm{sResV}_{-1}(P,R) &= \mathrm{sRes}_0(P,R) \cdot P. \end{aligned}$$

Remark 5.2.4 *When P is monic, the definitions of subresultant polynomials, signed subresultant coefficients and subresultant cofactors, are independent of the degree $r < p$ of R (see for instance [21]). Therefore, we can artificially consider the degree of R as $p-1$, specialize its first $p-r-1$ coefficients as 0 and obtain the same result.*

The connection between the subresultant coefficients and the Hermite's matrix is the following.

Proposition 5.2.5 *Let $P, Q \in \mathbf{D}[y]$ with $\deg P = p \geq 1$, P monic and let R be the remainder of $P' \cdot Q$ in the division by P. Then for $0 \leq j \leq p$*

$$\mathrm{HMi}_j(P;Q) = \mathrm{sRes}_j(P,R).$$

Proof. See [4, Lemma 9.26 and Proposition 4.55]. □

We now explain how to diagonalize Hermite's matrix using an alternative method. The first step is to transform it into a block Hankel triangular matrix, using subresultants.

Notation 5.2.6

- *Given $\alpha = (\alpha_1, \ldots, \alpha_p) \in \mathbf{D}^p$, we denote by $\mathrm{HanT}_p(\alpha) \in \mathbf{D}^{p \times p}$ the Hankel triangular matrix defined for $1 \leq i, j \leq p$ by $\mathrm{HanT}_p(\alpha)_{ij} = 0$ if $i + j \leq p$ and $\mathrm{HanT}_p(\alpha)_{ij} = \alpha_{2p+1-i-j}$ if $i + j \geq p + 1$.*
- *Given $S = \sum_{0 \leq h \leq p} \alpha_h y^h \in \mathbf{D}[y]$, we denote by $\mathrm{HanT}_p(S) \in \mathbf{D}^{p \times p}$ the Hankel triangular matrix $\mathrm{HanT}_p(\alpha_1, \ldots, \alpha_p)$.*

Notation 5.2.7 *Let $P, R \in \mathbf{D}[y]$ with $\deg P = p \geq 1$ and $\deg R = r < p$. Let $d = (d_0, \ldots, d_s)$ be the sequence of degrees of the non-defective subresultant polynomials of P and R and $d_{-1} = p+1$. Note that $d_0 = p$ and $d_1 = r$.*

- *For $1 \leq i \leq s$, let $R_i = \mathrm{sResP}_{d_{i-1}-1}(P,R) \in \mathbf{D}[y]$. By the Structure Theorem for Subresultants ([4, Theorem 8.30]), $\deg R_i = d_i$.*
- *For $1 \leq i \leq s$,*

$$\begin{aligned} \mathrm{sR}_{d_i} &= \mathrm{sRes}_{d_i}(P,R) \in \mathbf{D}, \\ T_{d_{i-1}-1} &= \mathrm{lcoeff}(\mathrm{sResP}_{d_{i-1}-1}(P,R)) \in \mathbf{D}. \end{aligned}$$

  We extend this definiton with

$$\begin{aligned} \mathrm{sR}_p &= 1 \in \mathbf{D}, \\ T_p &= 1 \in \mathbf{D}. \end{aligned}$$

- *For $1 \leq i \leq s$,*

$$\begin{aligned} \tilde{F}_{d_i-1} &= \mathrm{sResU}_{d_{i-2}-1}(P,R) \cdot \mathrm{sResV}_{d_i-1}(P,R) - \\ &\quad -\mathrm{sResU}_{d_i-1}(P,R) \cdot \mathrm{sResV}_{d_{i-2}-1}(P,R) \in \mathbf{D}[y], \\ F_{d_i-1} &= \frac{1}{\mathrm{sR}_{d_i} \cdot \mathrm{sR}_{d_{i-1}} \cdot T_{d_{i-1}-1} \cdot T_{d_{i-2}-1}} \cdot \tilde{F}_{d_i-1} \in \mathbf{F}[y]. \end{aligned}$$

As seen in the proof of [4, Proposition 8.36], $\tilde{F}_{d_i-1}$ *is the quotient of* $T_{d_{i-1}-1} \cdot \mathrm{sR}_{d_i} \cdot \mathrm{sResP}_{d_{i-2}-1}(P,R)$ *in the division by* $\mathrm{sResP}_{d_{i-1}-1}(P,R)$*; therefore, for* $1 \leq i \leq s$*,* $\deg_y \tilde{F}_{d_i-1} = \deg_y F_{d_i-1} = d_{i-1} - d_i$*,* $\mathrm{lcoeff}(\tilde{F}_{d_i-1}) = \mathrm{sR}_{d_i} \cdot T_{d_{i-2}-1}$ *and* $\mathrm{lcoeff}(F_{d_i-1}) = \frac{1}{\mathrm{sR}_{d_{i-1}} \cdot T_{d_{i-1}-1}}$.

- *Let* $\mathrm{HanB}_{P;R} \in \mathbf{F}^{p\times p}$ *be a block Hankel triangular matrix composed by* s *or* $s+1$ *blocks according to* $d_s = 0$ *or* $d_s > 0$*. For* $1 \leq i \leq s$*, the* i*-th block of* $\mathrm{HanB}_{P;R} \in \mathbf{F}^{p\times p}$*, of size* $d_{i-1} - d_i$*, is* $\mathrm{HanT}_{d_{i-1}-d_i}(F_{d_i-1})$ *and, if* $d_s > 0$*, there is a final* 0 *block of size* d_s*.*

- *Let us take now* P *monic and let* $Q \in \mathbf{D}[y]$*. Consider* $R \in \mathbf{D}[y]$ *to be the remainder of* $P' \cdot Q$ *in the division by* P*. Let* $\mathrm{M}_{P;Q} \in \mathbf{D}^{p\times p}$ *be the matrix of the basis* $\mathcal{R} :=$

  $$\{y^{d_0-d_1-1} \cdot R_1, \ldots, R_1, \ldots, y^{d_{i-1}-d_i-1} \cdot R_i, \ldots, R_i, \ldots, y^{d_{s-1}-d_s-1} \cdot R_s, \ldots, R_s, y^{d_s-1}, \ldots, 1\}$$

  of the subspace of $\mathbf{F}[y]$ *of polynomials of degree less than* p*, in the Horner basis of* P*,*

  $$\mathrm{Hor}(P) := \{y^{p-1} + \sum_{0\leq h\leq p-2} \gamma_{h+1} y^h, \ldots, 1\}.$$

In order to prove Theorem 5.2.2 (Hermite's Theory (2)), we also use Bezoutians, which we recall now.

Definition 5.2.8 (Bezoutian) *Let* $P, R \in \mathbf{D}[y]$*, with* $\deg P = p \geq 1$ *and* $\deg R = r < p$*. The Bezoutian of* P *and* R *is defined as*

$$\mathrm{Bez}(P,R) = \frac{P(x)\cdot R(y) - R(x)\cdot P(y)}{x-y} \in \mathbf{D}[x,y].$$

If $\mathcal{B} = \{b_1, \ldots b_p\}$ *is a basis of* $\mathbf{F}[y]/P$*,* $\mathrm{Bez}(P,R)$ *can be uniquely written as*

$$\mathrm{Bez}(P,R) = \sum_{1\leq i,j\leq p} \alpha_{i,j} \cdot b_i(x) \cdot b_j(y).$$

The Bezoutian matrix $\mathrm{Bez}_{\mathcal{B}}(P;R) \in \mathbf{F}^{p\times p}$ *is the symmetric matrix with* (i,j)*-th entry equal to the coefficient* $\alpha_{i,j}$ *of* $b_i(x)\cdot b_j(y)$ *in* $\mathrm{Bez}(P,R)$*.*

Lemma 5.2.9 *Following Notation 5.2.7,*

$$\mathrm{Bez}_{\mathcal{R}}(P;R) = \mathrm{HanB}_{P;R}.$$

Proof. Since for any $S = \sum_{0\leq h\leq p} \alpha_h y^h \in \mathbf{D}[y]$ we have that

$$\frac{S(x)-S(y)}{x-y} = \sum_{1\leq i\leq p} \sum_{p+1-i\leq j\leq p} \alpha_{2p+1-i-j} \cdot x^{p-i} \cdot y^{p-j},$$

in order to prove the claim we have to prove that

$$\mathrm{Bez}(P,R) = \sum_{1\leq i\leq s} \frac{F_{d_i-1}(x) - F_{d_i-1}(y)}{x-y} \cdot R_i(x) \cdot R_i(y).$$

This will be done by induction on s, which, by the Structure Theorem for Subresultants ([4, Theorem 8.30]) is equal to the length of the remainder sequence of P and R.

If $s = 0$ then R is the zero polynomial and the statement is clear. Now suppose that $s \geq 1$, therefore R is not the zero polynomial, and let S be the remainder of P in the division by R. Note that S is the zero polynomial if and only if $s = 1$. We also have that $R = R_1$ and, since $\mathrm{sR}_p = T_p = 1$, F_{r-1} is the quotient of P in the division by R, this is to say

$$P = F_{r-1} \cdot R_1 + S$$

and therefore

$$\mathrm{Bez}(P, R) = \frac{F_{r-1}(x) - F_{r-1}(y)}{x - y} \cdot R_1(x) \cdot R_1(y) + \mathrm{Bez}(R, -S). \tag{1}$$

For $s = 1$ equation (1) proves the claim. Suppose now that $s \geq 2$. We define $R'_2, \dots, R'_s$, $\mathrm{sR}'_{d_1}, \dots, \mathrm{sR}'_{d_s}, T'_{d_1}, T'_{d_1-1}, \dots, T'_{d_{s-1}-1}$ and $F'_{d_2-1}, \dots, F'_{d_s-1}$ as we did in Notation 5.2.7, but this time we consider all definitions depending on the polynomials R and $-S$ instead of P and R. If β is the leading coefficient of R, we have

$$\begin{aligned} R_2 &= -\varepsilon_{p-r} \cdot \beta^{p-r+1} \cdot S, \\ \mathrm{sR}_{d_1} &= \varepsilon_{p-r} \cdot \beta^{p-r}, \\ T_{d_0-1} &= \beta, \\ R'_2 &= -S. \end{aligned}$$

In addition, by Proposition [4, 8.35], there exists $\lambda \in \mathbf{D}, \lambda \neq 0$, such that

$$\begin{aligned} \mathrm{sR}_{d_i} &= \lambda \cdot \mathrm{sR}'_{d_i} && \text{for } 2 \leq i \leq s, \\ T_{d_{i-1}-1} &= \lambda \cdot T'_{d_{i-1}-1} && \text{for } 3 \leq i \leq s, \\ R_i &= \lambda \cdot R'_i && \text{for } 3 \leq i \leq s. \end{aligned}$$

From this we first deduce that

$$F_{d_2-1} = \frac{1}{\mathrm{sR}_{d_1} T_{d_0-1}} \cdot \mathrm{Quot}(R_1, R_2) = \frac{1}{\varepsilon_{p-r} \cdot \beta^{p-r+1}} \cdot \mathrm{Quot}(R, -\varepsilon_{p-r} \cdot \beta^{p-r+1} \cdot S) =$$

$$= \frac{1}{(\varepsilon_{p-r} \cdot \beta^{p-r+1})^2} \cdot \mathrm{Quot}(R, -S) = \frac{1}{(\varepsilon_{p-r} \cdot \beta^{p-r+1})^2} \cdot F'_{d_2-1},$$

second, since T_{d_1-1} and T'_{d_1-1} are the leading coefficients of R_2 and R'_2 respectively, that

$$F_{d_3-1} = \frac{1}{\mathrm{sR}_{d_2} \cdot T_{d_1-1}} \cdot \mathrm{Quot}(R_2, R_3) = \frac{1}{\lambda \cdot \mathrm{sR}'_{d_2} \cdot T'_{d_1-1}} \cdot \mathrm{Quot}(R'_2, \lambda \cdot R_3) = \frac{1}{\lambda^2} \cdot F'_{d_3-1},$$

and finally, that for $4 \leq i \leq s$,

$$F_{d_i-1} = \frac{1}{\mathrm{sR}_{d_{i-1}} \cdot T_{d_{i-2}-1}} \cdot \mathrm{Quot}(R_{i-1}, R_i) = \frac{1}{\lambda^2 \cdot \mathrm{sR}'_{d_{i-1}} \cdot T'_{d_{i-2}-1}} \cdot \mathrm{Quot}(\lambda \cdot R'_{i-1}, \lambda \cdot R'_i) = \frac{1}{\lambda^2} \cdot F'_{d_i-1}.$$

Therefore for $2 \leq i \leq s$ we have that

$$(F_{d_i-1}(x) - F_{d_i-1}(y)) \cdot R_i(x) \cdot R_i(y) = \left(F'_{d_i-1}(x) - F'_{d_i-1}(y)\right) \cdot R'_i(x) \cdot R'_i(y).$$

Finally, using equation (1) and the inductive hypothesis, since the length of the remainder sequence of R and $-S$ is $s-1$, we have that

$$\begin{aligned}
\mathrm{Bez}(P,R) &= \frac{F_{r-1}(x) - F_{r-1}(y)}{x-y} \cdot R_1(x) \cdot R_1(y) + \mathrm{Bez}(R,-S) = \\
&= \frac{F_{r-1}(x) - F_{r-1}(y)}{x-y} \cdot R_1(x) \cdot R_1(y) + \sum_{2 \leq i \leq s} \frac{F'_{d_i-1}(x) - F'_{d_i-1}(y)}{x-y} \cdot R'_i(x) \cdot R'_i(y) = \\
&= \sum_{1 \leq i \leq s} \frac{F_{d_i-1}(x) - F_{d_i-1}(y)}{x-y} \cdot R_i(x) \cdot R_i(y)
\end{aligned}$$

as we wanted to prove. □

Lemma 5.2.10 *Following Notation 5.2.7 with R the remainder of $P' \cdot Q$ in the division by P,*

$$\mathrm{Her}(P;Q) = \mathrm{M}_{P;Q} \cdot \mathrm{HanB}_{P;R} \cdot \mathrm{M}^{\mathrm{t}}_{P;Q}.$$

Proof. The claim follows from Lemma 5.2.9 and the fact that

$$\mathrm{Her}(P;Q) = \mathrm{Bez}_{\mathrm{Hor}(P)}(P;R) = \mathrm{M}_{P;Q} \cdot \mathrm{Bez}_{\mathcal{R}}(P;R) \cdot \mathrm{M}^{\mathrm{t}}_{P;Q}$$

(see [4, Proposition 9.20 and Proposition 4.55]). □

We introduce some more definitions to transform the preceeding block Hankel form into a diagonal form.

Definition 5.2.11 *For $p \in \mathbb{N}_*$ and a variable c, we define the diagonal matrix $\mathrm{Di}_p \in \mathbb{Q}[c]^{p \times p}$ as follows:*

- *If p is odd, Di_p has c in the first $\frac{1}{2}(p-1)$ diagonal entries, $\frac{1}{2}c$ in the next diagonal entry and $-c$ in the last $\frac{1}{2}(p-1)$ diagonal entries.*
- *If p is even, Di_p has c in the first $\frac{1}{2}p$ diagonal entries and $-c$ in last $\frac{1}{2}p$ diagonal entries.*

We also define for $c = (c_1, \ldots, c_p)$ the matrix $\mathrm{E}_p \in \mathbb{Q}[c]^{p \times p}$ as follows:

- $\mathrm{E}_1 = \begin{pmatrix} 2 \end{pmatrix}$,
- $\mathrm{E}_2 = \begin{pmatrix} c_2 & 0 \\ \frac{1}{2}c_1 & c_2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$,
- *For odd $p \geq 3$,* $\mathrm{E}_p =$

$$\left(\begin{array}{c|c|c} c_p & 0 & 0 \\ \hline c_{p-1} & & \\ \vdots & c_p \cdot \mathrm{Id} & 0 \\ c_2 & & \\ \hline \frac{1}{2}c_1 & 0 & c_p \end{array}\right) \left(\begin{array}{c|c|c} 1 & 0 & 1 \\ \hline 0 & \mathrm{Id} & 0 \\ \hline 1 & 0 & -1 \end{array}\right) \left(\begin{array}{c|c|c} c_p^{\frac{1}{2}(p-3)} & 0 & 0 \\ \hline 0 & \mathrm{E}_{p-2}(c') & 0 \\ \hline 0 & 0 & c_p^{\frac{1}{2}(p-3)} \end{array}\right)$$

with $c' = (c_3, \ldots, c_p)$.

- *For even* $p \geq 4$, $\mathrm{E}_p =$

$$\left(\begin{array}{c|c|c} c_p & 0 & 0 \\ \hline c_{p-1} & & \\ \vdots & c_p \cdot \mathrm{Id} & 0 \\ c_2 & & \\ \hline \frac{1}{2}c_1 & 0 & c_p \end{array}\right)\left(\begin{array}{c|c|c} 1 & 0 & 1 \\ \hline 0 & \mathrm{Id} & 0 \\ \hline 1 & 0 & -1 \end{array}\right)\left(\begin{array}{c|c|c} c_p^{\frac{1}{2}(p-2)} & 0 & 0 \\ \hline 0 & \mathrm{E}_{p-2}(c') & 0 \\ \hline 0 & 0 & c_p^{\frac{1}{2}(p-2)} \end{array}\right)$$

with $c' = (c_3, \ldots, c_p)$.

Finally, for $S = \sum_{0 \leq h \leq p} c_h \cdot y^h \in \mathbb{Q}[c_0, \ldots, c_p][y]$, *we denote by* $\mathrm{E}_p(S) \in \mathbb{Q}[c_1, \ldots, c_p]^{p \times p}$ *the matrix* $\mathrm{E}_p(c_1, \ldots, c_p)$.

Lemma 5.2.12

- *For odd* $p \in \mathbb{N}_*$ *the degree of the entries of the matrix* E_p *is* $\frac{1}{2}(p-1)$, $\det(\mathrm{E}_p) = (-1)^{\frac{1}{2}(p-1)} 2^{\frac{1}{2}(p+1)} c_p^{\frac{1}{2}p(p-1)}$ *and*

$$\mathrm{HanT}_p = \mathrm{E}_p \cdot \mathrm{Di}_p\left(\frac{1}{2}c_p^{2-p}\right) \cdot \mathrm{E}_p^{\mathrm{t}}.$$

- *For even* $p \in \mathbb{N}_*$ *the degree of the entries of the matrix* E_p *is* $\frac{1}{2}p$, $\det(\mathrm{E}_p) = (-2)^{\frac{1}{2}p} c_p^{\frac{1}{2}p^2}$ *and*

$$\mathrm{HanT}_p = \mathrm{E}_p \cdot \mathrm{Di}_p\left(\frac{1}{2}c_p^{1-p}\right) \cdot \mathrm{E}_p^{\mathrm{t}}.$$

Proof. Easy to prove by induction on p. □

We can prove now Theorem 5.2.2 (Hermite's Theory (2)).

Proof of Theorem 5.2.2. Following Notation 5.2.7, by Lemmas 5.2.10 and 5.2.12, it is clear that

$$\begin{aligned} \mathrm{Rk}(\mathrm{Her}(P;Q)) &= p - d_s, \\ \mathrm{Si}(\mathrm{Her}(P;Q)) &= \sum_{\substack{1 \leq i \leq s, \\ d_{i-1}-d_i \text{ odd}}} \mathrm{sign}(\mathrm{sR}_{d_{i-1}} \cdot T_{d_{i-1}-1}). \end{aligned}$$

By the Structure Theorem for Subresultants ([4, Theorem 8.30]), for $1 \leq i \leq s$,

$$\mathrm{sR}_{d_i} = \varepsilon_{d_{i-1}-d_i} \frac{T_{d_{i-1}-1}^{d_{i-1}-d_i}}{\mathrm{sR}_{d_{i-1}}^{d_{i-1}-d_i-1}}.$$

Therefore, for $1 \leq i \leq s$ such that $d_{i-1} - d_i$ is odd, $\mathrm{sign}(T_{d_{i-1}-1}) = \varepsilon_{d_{i-1}-d_i} \mathrm{sign}(\mathrm{sR}_{d_i})$. The conclusion follows using Proposition 5.2.5. □

Before proving a related weak inference in Theorem 5.2.17 (Hermite's Theory (2) as a weak existence), we give some auxiliary definitions.

Definition 5.2.13 *Let $p, q \in \mathbb{N}$, $p \geq 1$. Let $c = (c_0, \ldots, c_{p-1})$ be variables representing the coefficients of P, $c' = (c'_0, \ldots, c'_q)$ be variables represeting the coefficients of Q. In the following definitions, we always consider y as the main variable.*

- $P = y^p + \sum_{0 \leq h \leq p-1} c_h \cdot y^h \in \mathbf{K}[c][y]$,
- $Q = \sum_{0 \leq h \leq q} c'_h \cdot y^h \in \mathbf{K}[c'][y]$,
- $R \in \mathbf{K}[c, c'][y]$ *is the remainder of* $P' \cdot Q$ *in the division by* P,
- *for* $0 \leq j \leq p$, $\mathrm{sResP}_j \in \mathbf{K}[c, c'][y]$ *is the j-th subresultant polynomial of P and R,*
- *for* $0 \leq j \leq p$, $\mathrm{sR}_j \in \mathbf{K}[c, c']$ *is the j-th signed subresultant coefficient of P and R,*
- *for* $-1 \leq j \leq p$, $\mathrm{sResU}_j \in \mathbf{K}[c, c'][y]$ *and* $\mathrm{sResV}_j \in \mathbf{K}[c, c'][y]$ *are the j-th subresultant cofactors of P and R.*

Let now $\tau \in \{-1, 0, 1\}^{\{0, \ldots, p-1\}}$ be a sign condition, $d(\tau) = (d_0, \ldots, d_s)$ and $d_{-1} = p + 1$.

- *for* $0 \leq i \leq s$, $T^\tau_{d_{i-1}-1} \in \mathbf{K}[c, c']$ *is the coefficient of degree d_i in* $\mathrm{sResP}_{d_{i-1}-1}$,
- *for* $1 \leq i \leq s$, $R^\tau_i \in \mathbf{K}[c, c'][y]$ *is the remainder of* $\mathrm{sResP}_{d_{i-1}-1}$ *in the division by* y^{d_i+1},
- $\mathrm{M}^\tau_{P;Q} \in \mathbf{K}[c, c']^{p \times p}$ *is the matrix of*

  $$\{y^{d_0-d_1-1} \cdot R^\tau_1, \ldots, R^\tau_1, \ldots, y^{d_{i-1}-d_i-1} \cdot R^\tau_i, \ldots, R^\tau_i, \ldots, y^{d_{s-1}-d_s-1} \cdot R^\tau_s, \ldots, R^\tau_s, y^{d_s-1}, \ldots, 1\}$$

  in the Horner basis of P, $\{y^{p-1} + \sum_{0 \leq h \leq p-2} c_{h+1} \cdot y^h, \ldots, 1\}$,
- *for* $1 \leq i \leq s$, $\tilde{F}^\tau_{d_i-1} = \sum_j \tilde{F}^\tau_{d_i-1,j} \cdot y^j \in \mathbf{K}[c, c'][y]$ *is*

  $$\mathrm{sResU}_{d_{i-2}-1} \cdot \mathrm{sResV}_{d_i-1} - \mathrm{sResU}_{d_i-1} \cdot \mathrm{sResV}_{d_{i-2}-1}.$$

In order to avoid dealing with rational functions, we consider variables $\ell = (\ell_1, \ldots, \ell_s)$ representing the inverses of $(\mathrm{sR}_{d_i})_{1 \leq i \leq s}$ and $\ell' = (\ell'_1, \ldots, \ell'_s)$ variables representing the inverses of $(T^\tau_{d_{i-1}-1})_{1 \leq i \leq s}$. We additionally define $\ell_0 = \ell'_0 = 1$. We also consider variables $a = (a_i)_{1 \leq i \leq s,\, d_{i-1}-d_i\, even}$ and $b = (b_i)_{1 \leq i \leq s,\, d_{i-1}-d_i\, even}$ which only purpose is to fix the sign of the diagonal elements in the even size blocks in the diagonal matrix $\mathrm{Di}^\tau_{P;Q}$ defined below.

- *For* $1 \leq i \leq s$, $F^\tau_{d_i-1} \in \mathbf{K}[c, c'][\ell, \ell'][y]$ *is*

  $$\ell_{i-1} \cdot \ell'_i \cdot y^{d_{i-1}-d_i} + \ell_i \cdot \ell_{i-1} \cdot \ell'_i \cdot \ell'_{i-1} \Big(\sum_{0 \leq j \leq d_{i-1}-d_i-1} \tilde{F}^\tau_{d_i-1,j} \cdot y^j \Big),$$

- $\mathrm{E}^\tau_{P;Q} \in \mathbf{K}[c, c'][\ell, \ell']^{p \times p}$ *is the block diagonal matrix composed by s or $s+1$ blocks according to $d_s = 0$ or $d_s > 0$; for $1 \leq i \leq s$ the i-th block is the matrix $\mathrm{E}_{d_{i-1}-d_i}(F^\tau_{d_i-1})$, if $d_s > 0$ the last block is the identity matrix of size d_s.*

- $\mathrm{E}'^{\tau} \in \mathbf{K}[a,b]^{p\times p}$ *is the block diagonal matrix composed by* s *or* $s+1$ *blocks according to* $d_s = 0$ *or* $d_s > 0$*; for* $1 \le i \le s$*, the* i*-th block is the identity matrix of size* $d_{i-1} - d_i$ *if* $d_{i-1} - d_i$ *is odd and the matrix*

$$\begin{pmatrix} a_i & 0 & \dots & \dots & 0 & b_i \\ 0 & \ddots & & & \iddots & 0 \\ \vdots & & a_i & b_i & & \vdots \\ \vdots & & -b_i & a_i & & \vdots \\ 0 & \iddots & & & \ddots & \\ -b_i & 0 & \dots & \dots & 0 & a_i \end{pmatrix}$$

of size $d_{i-1} - d_i$ *if* $d_{i-1} - d_i$ *is even, if* $d_s > 0$ *the last block is the identity matrix of size* d_s*.*

- $\mathrm{B}^{\tau}_{P;Q} = \mathrm{M}^{\tau}_{P;Q} \cdot \mathrm{E}^{\tau}_{P;Q} \cdot \mathrm{E}'^{\tau} \in \mathbf{K}[c,c'][\ell,\ell',a,b]^{p\times p}$.

- $\mathrm{Di}^{\tau}_{P;Q} \in \mathbf{K}[c,c'][\ell,\ell']^{p\times p}$ *is the diagonal matrix defined by blocks, composed by* s *or* $s+1$ *blocks according to* $d_s = 0$ *or* $d_s > 0$*; for* $1 \le i \le s$*, the* i*-th block is the diagonal matrix*

$$\mathrm{Di}_{d_{i-1}-d_i}\left(\frac{1}{2}\varepsilon_{d_{i-1}-d_i}\ell_{i-1}^2 \cdot {\ell'_i}^2 \cdot \mathrm{sR}_{d_{i-1}}^{2(d_{i-1}-d_i)-1} \cdot \mathrm{sR}_{d_i}\right)$$

if $d_{i-1} - d_i$ *is odd and the matrix*

$$\mathrm{Di}_{d_{i-1}-d_i}\left(\frac{1}{2}\right)$$

if $d_{i-1} - d_i$ *is even, if* $d_s > 0$ *the last block is the zero block of size* d_s*.*

Remark 5.2.14 *Following Definition 5.2.3 and Definition 5.2.13 and taking into account Remark 5.1.8, it can be proved that:*

- $\deg_c \mathrm{Her}(P;Q) \le q + 2p - 2$, $\deg_{c'} \mathrm{Her}(P;Q) \le 1$, *then* $\deg_{(c,c')} \mathrm{Her}(P;Q) \le q + 2p - 1$,
- $\deg_{(c,c')} R \le q + 2$,
- *for* $0 \le j \le p-1$, $\deg_{(c,c')} \mathrm{sR}_j \le (p-j)(q+3) - 1$, $\deg_{(c,c')} \mathrm{sR}_p = 0$,
- *for* $1 \le i \le s$, $\deg_{(c,c')} R^{\tau}_i \le (p - d_{i-1} + 1)(q+3) - 1$,
- $\deg_{(c,c')} \mathrm{M}^{\tau}_{P;Q} \le p(q+3) - 1$,
- *for* $1 \le i \le s$, $\deg_{(c,c',\ell,\ell')} F^{\tau}_{d_i-1} \le (2p - d_i - d_{i-2} + 1)(q+3) + 2 \le (2p-1)(q+3) + 2$,
- $\deg_{(c,c',\ell,\ell')} \mathrm{E}^{\tau}_{P;Q} \le \frac{1}{2}p((2p-1)(q+3)+2)$,
- $\deg_{(a,b)} \mathrm{E}'^{\tau} \le 1$,
- $\deg_{(c,c',\ell,\ell')} \mathrm{Di}^{\tau}_{P;Q} \le 4 + 2p(p(q+3) - 1)$.

We will use these degree bounds in Lemmas 5.2.15 and 5.2.16; but, in fact, a separate degree analysis on the set of variables (c, c') and each variable ℓ_i and ℓ'_i, which can be easily done, will be needed in Theorem 5.4.3 (Hermite's Theory as an incompatibility).

We prove two auxiliary algebraic identities, using Effective Nullstellensatz ([31, Theorem 1.3]).

Lemma 5.2.15 *Let $p, q \in \mathbb{N}$, $p \geq 1$, $\tau \in \{-1, 0, 1\}^{\{0,\dots,p-1\}}$ be a sign condition, $d(\tau) = (d_0, \dots, d_s)$, $c = (c_0, \dots, c_{p-1})$, $c' = (c'_0, \dots, c'_q)$, $1 \leq i \leq s$ and $e = (p(q+3)-1)^{d_{i-1}-d_i}$. Following Definition 5.2.13, there is an identity in $\mathbf{K}[c, c']$*

$$(\mathrm{sR}_{d_{i-1}} \cdot \mathrm{sR}_{d_i})^e = \sum_{d_i+1 \leq j \leq d_{i-1}-1} \mathrm{sR}_j \cdot W_j + T_{d_{i-1}-1} \cdot W$$

such that all the terms have degree in (c, c') bounded by $2ep(q+3)$.

Proof. We denote by $\overline{\mathbf{K}}$ the algebraic closure of $\mathbf{K}$. By the Structure Theorem for Subresultants ([4, Theorem 8.30]), for any $\gamma \in \overline{\mathbf{K}}^p, \gamma' \in \overline{\mathbf{K}}^{q+1}$, such that

$$\mathrm{sR}_{d_{i-1}}(\gamma, \gamma') \neq 0, \bigwedge_{d_{i-1}<j<d_i} \mathrm{sR}_j(\gamma, \gamma') = 0, \ \mathrm{sR}_{d_i}(\gamma, \gamma') \neq 0$$

we have

$$T_{d_{i-1}-1}(\gamma, \gamma') \neq 0.$$

The claim follows from a similar use of [31, Theorem 1.3] as in the proof of Lemma 4.1.5. □

Lemma 5.2.16 *Let $p, q \in \mathbb{N}$, $p \geq 1$, $\tau \in \{-1, 0, 1\}^{\{0,\dots,p-1\}}$ be a sign condition, $d(\tau) = (d_0, \dots, d_s)$, $c = (c_0, \dots, c_{p-1})$, $c' = (c'_0, \dots, c'_q)$, $\ell = (\ell_1, \dots, \ell_s)$, $\ell' = (\ell'_1, \dots, \ell'_s)$, $a = (a_i)_{1 \leq i \leq s,\, d_{i-1}-d_i\, even}$, $b = (b_i)_{1 \leq i \leq s,\, d_{i-1}-d_i\, even}$ and $e = 2^{2p}p^{4p}(q+3)^{3p}$. Following Definition 5.2.13, for $1 \leq j_1, j_2 \leq p$, there is an identity in $\mathbf{K}[c, c'][\ell, \ell', a, b]$*

$$\begin{aligned}
&\Big(\mathrm{Her}(P;Q)_{j_1,j_2} - \big(\mathrm{B}^\tau_{P;Q} \cdot \mathrm{Di}^\tau_{P;Q} \cdot {\mathrm{B}^\tau_{P;Q}}^{\mathrm{t}}\big)_{j_1,j_2}(\ell, \ell', a, b)\Big)^e = \\
= &\sum_{\substack{0 \leq j \leq p-1, \\ \tau(j)=0}} \mathrm{sR}_j \cdot W_j(\ell, \ell', a, b) + \sum_{1 \leq i \leq s} (\ell_i \cdot \mathrm{sR}_{d_i} - 1) \cdot W'_i(\ell, \ell', a, b) + \\
+ &\sum_{1 \leq i \leq s} (\ell'_i \cdot T_{d_{i-1}-1} - 1) \cdot W''_i(\ell, \ell', a, b) + \\
+ &\sum_{\substack{1 \leq i \leq s, \\ d_{i-1}-d_i\, even}} (a_i^2 - b_i^2 - (\mathrm{sR}_{d_{i-1}} \cdot T_{d_{i-1}-1})^{d_{i-1}-d_i-1}) \cdot W'''_i(\ell, \ell', a, b) + \\
+ &\sum_{\substack{1 \leq i \leq s, \\ d_{i-1}-d_i\, even}} a_i \cdot b_i \cdot W''''_i(\ell, \ell', a, b)
\end{aligned}$$

such that all the terms have degree in $(c, c', \ell, \ell', a, b)$ bounded by $e(4p^2(q+3) + p(q+3) + 5)$.

Proof. We denote by $\overline{\mathbf{K}}$ the algebraic closure of $\mathbf{K}$. By the Structure Theorem for Subresultants ([4, Theorem 8.30]), Lemma 5.2.10 and Lemma 5.2.12, for any $\gamma \in \overline{\mathbf{K}}^p, \gamma' \in \overline{\mathbf{K}}^{q+1}$, $\lambda, \lambda' \in \overline{\mathbf{K}}^s$, $\alpha, \beta \in \overline{\mathbf{K}}^{\#\{1\le i\le s,\, d_{i-1}-d_i \text{even}\}}$ such that

$$\bigwedge_{0\le j\le p-1} \mathrm{inv}(\mathrm{sR}_j(\gamma,\gamma')) = \tau(j)^2, \quad \bigwedge_{1\le i\le s} \lambda_i \cdot \mathrm{sR}_{d_i}(\gamma,\gamma') = 1, \quad \bigwedge_{1\le i\le s} \lambda'_i \cdot T_{d_{i-1}-1}(\gamma,\gamma') = 1,$$

$$\bigwedge_{\substack{1\le i\le s,\\ d_{i-1}-d_i \text{even}}} \alpha_i^2 - \beta_i^2 = (\mathrm{sR}_{d_{i-1}}(\gamma,\gamma')\cdot T_{d_{i-1}-1}(\gamma,\gamma'))^{d_{i-1}-d_i-1}, \quad \bigwedge_{\substack{1\le i\le s,\\ d_{i-1}-d_i \text{even}}} \alpha_i\cdot\beta_i = 0,$$

we have $\mathrm{Her}(P;Q)(\gamma,\gamma') = \mathrm{B}^{\tau}_{P;Q}\cdot \mathrm{Di}^{\tau}_{P;Q}\cdot {\mathrm{B}^{\tau}_{P;Q}}^{\mathrm{t}}(\gamma,\gamma',\lambda,\lambda',\alpha,\beta) \in \overline{\mathbf{K}}^{p\times p}$. Moreover, for $1\le i\le s$, the condition $\lambda_i \cdot \mathrm{sR}_{d_i}(\gamma,\gamma') = 1$ clearly implies $\mathrm{inv}(\mathrm{sR}_{d_i}(\gamma,\gamma')) = 1$. The claim follows from a similar use of [31, Theorem 1.3] as in the proof of Lemma 4.1.5. □

From now on, we make a slight abuse of notation, denoting by $\mathrm{B}^{\tau}_{P;Q}(\ell,\ell',z)$ the matrix $\mathrm{B}^{\tau}_{P;Q}(\ell,\ell',a,b)$ where $z = a+ib$ is a complex variable,

We prove now the following related weak inference.

Theorem 5.2.17 (Hermite's Theory (2) as a weak existence) *Let* $p \ge 1$, $P = y^p + \sum_{0\le h\le p-1} C_h\cdot y^h \in \mathbf{K}[u][y]$, $Q = \sum_{0\le h\le q} D_h \cdot y^h \in \mathbf{K}[u][y]$, $\tau \in \{-1,0,1\}^{\{0,\dots,p-1\}}$ *be a sign condition,* $d(\tau) = (d_0,\dots,d_s)$, *and* $d'_i = d_{i-1}-d_i$ *for* $i = 1,\dots,s$. *Then*

$$\bigwedge_{0\le i\le p-1} \mathrm{sign}(\mathrm{HMi}_i(P;Q)) = \tau(i) \quad \vdash$$

$$\vdash \quad \exists(\ell,\ell',z)\ [\ \mathrm{Her}(P;Q) \equiv \mathrm{B}^{\tau}_{P;Q}(\ell,\ell',z)\cdot \mathrm{Di}^{\tau}_{P;Q}(\ell,\ell')\cdot {\mathrm{B}^{\tau}_{P;Q}}^{\mathrm{t}}(\ell,\ell',z),\ \det(\mathrm{B}^{\tau}_{P;Q}(\ell,\ell',z)) \ne 0,$$
$$\bigwedge_{\substack{1\le i\le s,\\ d'_i\, odd}} \mathrm{sign}(\ell_{i-1}^2\cdot {\ell'_i}^2 \cdot \mathrm{HMi}_{d_{i-1}}(P;Q)^{2d'_i-1}\cdot \mathrm{HMi}_{d_i}(P;Q)) = \tau_{d_{i-1}}\tau_{d_i}\ ]$$

where $\ell = (\ell_1,\dots,\ell_s), \ell' = (\ell'_1,\dots,\ell'_s), z = (z_i)_{1\le i\le s,\, d'_i\, even}$.

Suppose we have an initial incompatibility in $\mathbf{K}[v][\ell,\ell',a,b]$ *where* $v\supset u$ *and* (ℓ,ℓ',a,b) *are disjoint from* v, *with monoid part*

$$S\cdot \det(\mathrm{B}^{\tau}_{P;Q}(\ell,\ell',z))^{2e}\cdot \prod_{\substack{1\le i\le s,\\ d'_i\, odd}} (\ell_{i-1}^2\cdot {\ell'_i}^2\cdot \mathrm{HMi}_{d_{i-1}}(P;Q)^{2d'_i-1}\cdot \mathrm{HMi}_{d_i}(P;Q))^{2e_i}$$

with $e\in\mathbb{N}_*$, $e_i \le e' \in \mathbb{N}_*$, *degree in* $w\subset v$ *bounded by* δ_w, *degree in* ℓ_i *bounded by an even number* δ_ℓ, *degree in* ℓ'_i *bounded by an even number* $\delta_{\ell'}$ *and degree in* (a_i,b_i) *bounded by* δ_z. *Then the final incompatibility has monoid part*

$$S^f\cdot \prod_{1\le i\le s} \mathrm{HMi}_{d_i}(P;Q)^{2f_i}$$

with $f \le 2^{3p}p^{4p+2}(q+3)^{3p}$,

$$f_i \le 2^{3p-1}p^{4p+2}(q+3)^{3p}(\delta_\ell + p^p(q+3)^p\delta_{\ell'} + 10p^{p+2}(q+3)^{p+1}e + 4pe)$$

and degree in w *bounded by*

$$2^{3p}p^{4p+2}(q+3)^{3p}\cdot$$
$$\cdot\Big(\delta_w + \Big(p^2(q+3)\delta_\ell + 3p^{p+1}(q+3)^{p+1}\delta_{\ell'} + 4p^2(q+3)\delta_z + 31p^{p+3}(q+3)^{p+2}e\Big)\max\{\deg_w P, \deg_w Q\}\Big).$$

Note that in the weak inference in Theorem 5.2.17, the elements $\ell_{i-1}^2 \cdot {\ell'_i}^2 \cdot \mathrm{HMi}_{d_{i-1}}(P;Q)^{2d'_i-1} \cdot \mathrm{HMi}_{d_i}(P;Q)$ for $1 \le i \le s$, d'_i odd, are, up to scalars, the only non-constant terms in the diagonal matrix $\mathrm{Di}^{\tau}_{P;Q}(\ell,\ell')$.

Proof. Consider the initial incompatibility

$$\downarrow \mathrm{Her}(P;Q) \equiv \mathrm{B}^{\tau}_{P;Q}(\ell,\ell',z)\cdot \mathrm{Di}^{\tau}_{P;Q}(\ell,\ell')\cdot {\mathrm{B}^{\tau}_{P;Q}}^{\mathrm{t}}(\ell,\ell',z),\ \det(\mathrm{B}^{\tau}_{P;Q}(\ell,\ell',z))\neq 0,$$
$$\bigwedge_{\substack{1\le i\le s,\\ d'_i \text{odd}}} \mathrm{sign}(\ell_{i-1}^2\cdot {\ell'_i}^2\cdot \mathrm{HMi}_{d_{i-1}}(P;Q)^{2d'_i-1}\cdot \mathrm{HMi}_{d_i}(P;Q)) = \tau(d_{i-1})\tau(d_i),\ \mathcal{H} \downarrow_{\mathbf{K}[v][\ell,\ell',a,b]} \tag{2}$$

where $\mathcal{H}$ is a system of sign conditions in $\mathbf{K}[v]$. By Proposition 5.2.5, for $0 \le j \le p$, $\mathrm{HMi}_j(P;Q) = \mathrm{sR}_j(C_0,\dots,C_{p-1},D_0,\dots,D_q)$.

Following Lemma 5.2.12, $\det(\mathrm{B}^{\tau}_{P;Q}(\ell,\ell',z))$ is equal to

$$\prod_{1\le i\le s} T_{d_{i-1}-1}^{d'_i}\cdot \prod_{\substack{1\le i\le s,\\ d'_i \text{odd}}} (-1)^{\frac12(d'_i-1)}2^{\frac12(d'_i+1)}(\ell_{i-1}\cdot\ell'_i)^{\frac12 d'_i(d'_i-1)}\cdot \prod_{\substack{1\le i\le s,\\ d'_i \text{even}}} (-2)^{\frac12 d'_i}(\ell_{i-1}\cdot\ell'_i)^{\frac12 {d'_i}^2}\cdot(a_i^2+b_i^2)^{\frac12 d'_i}.$$

Then we apply to (2) the weak inference

$$\bigwedge_{1\le i\le s} T_{d_{i-1}-1}\neq 0,\ \bigwedge_{1\le i\le s}\ell_i\neq 0,\ \bigwedge_{1\le i\le s}\ell'_i\neq 0,\ \bigwedge_{\substack{1\le i\le s,\\ d'_i \text{even}}} z_i\neq 0 \quad\vdash\quad \det(\mathrm{B}^{\tau}_{P;Q}(\ell,\ell',z))\neq 0.$$

By Lemma 2.1.2 (item 6) we obtain an incompatibility

$$\downarrow \mathrm{Her}(P;Q) \equiv \mathrm{B}^{\tau}_{P;Q}(\ell,\ell',z)\cdot \mathrm{Di}^{\tau}_{P;Q}(\ell,\ell')\cdot {\mathrm{B}^{\tau}_{P;Q}}^{\mathrm{t}}(\ell,\ell',z),$$
$$\bigwedge_{1\le i\le s} T_{d_{i-1}-1}\neq 0,\ \bigwedge_{1\le i\le s}\ell_i\neq 0,\ \bigwedge_{1\le i\le s}\ell'_i\neq 0,\ \bigwedge_{\substack{1\le i\le s,\\ d'_i \text{even}}} z_i\neq 0, \tag{3}$$
$$\bigwedge_{\substack{1\le i\le s,\\ d'_i \text{odd}}} \mathrm{sign}(\ell_{i-1}^2\cdot {\ell'_i}^2\cdot \mathrm{sR}_{d_{i-1}}^{2d'_i-1}\cdot \mathrm{sR}_{d_i}) = \tau(d_{i-1})\tau(d_i),\ \mathcal{H} \downarrow_{\mathbf{K}[v][\ell,\ell',a,b]}$$

with monoid part

$$S\cdot \prod_{1\le i\le s} T_{d_{i-1}-1}^{2d'_i e}\cdot \prod_{\substack{1\le i\le s,\\ d'_i \text{odd}}} (\ell_{i-1}\cdot\ell'_i)^{d'_i(d'_i-1)e+4e_i}\cdot(\mathrm{sR}_{d_{i-1}}^{2d'_i-1}\cdot \mathrm{sR}_{d_i})^{2e_i}\cdot \prod_{\substack{1\le i\le s,\\ d'_i \text{even}}} (\ell_{i-1}\cdot\ell'_i)^{{d'_i}^2 e}\cdot(a_i^2+b_i^2)^{d'_i e}$$

and the same degree bounds.

Let $\tilde e = 2^{2p}p^{4p}(q+3)^{3p}$. We pass in (3) all the terms in the ideal generated by $\{(\mathrm{Her}(P;Q) - \mathrm{B}^{\tau}_{P;Q}\cdot \mathrm{Di}^{\tau}_{P;Q}\cdot {\mathrm{B}^{\tau}_{P;Q}}^{\mathrm{t}})_{j_1,j_2} \mid 1\le j_1\le j_2\le p\}$ to the right hand side, we raise both sides to the $(\frac12 p(p+1)\tilde e)$-th power and we pass all the terms back to the left hand side. It is easy to see that what we obtain is an incompatibility

$$\downarrow \bigwedge_{1\le j_1\le j_2\le p} \Big(\mathrm{Her}(P;Q)_{j_1,j_2} - (\mathrm{B}^{\tau}_{P;Q}(\ell,\ell',z)\cdot \mathrm{Di}^{\tau}_{P;Q}(\ell,\ell')\cdot {\mathrm{B}^{\tau}_{P;Q}}^{\mathrm{t}}(\ell,\ell',z))_{j_1,j_2}\Big)^{\tilde e} = 0,$$
$$\bigwedge_{1\le i\le s} T_{d_{i-1}-1}\neq 0,\ \bigwedge_{1\le i\le s}\ell_i\neq 0,\ \bigwedge_{1\le i\le s}\ell'_i\neq 0,\ \bigwedge_{\substack{1\le i\le s,\\ d'_i\,\mathrm{even}}} z_i\neq 0,$$
$$\bigwedge_{\substack{1\le i\le s,\\ d'_i\,\mathrm{odd}}}\mathrm{sign}(\ell_{i-1}^2\cdot {\ell'_i}^2\cdot \mathrm{sR}_{d_{i-1}}^{2d'_i-1}\cdot \mathrm{sR}_{d_i}) = \tau(d_{i-1})\tau(d_i),\ \mathcal{H}\ \downarrow_{\mathbf{K}[v][\ell,\ell',a,b]}.$$

Following Lemma 5.2.16 and applying Lemma 2.1.8, we obtain an incompatibility

$$\downarrow \bigwedge_{1\le j\le p,\,\tau(j)=0}\mathrm{sR}_j = 0,\ \bigwedge_{1\le i\le s}\ell_i\cdot \mathrm{sR}_{d_i} = 1,\ \bigwedge_{1\le i\le s}\ell'_i\cdot T_{d_{i-1}-1} = 1,$$
$$\bigwedge_{\substack{1\le i\le s,\\ d'_i\,\mathrm{even}}} z_i^2 = (\mathrm{sR}_{d_{i-1}}\cdot T_{d_{i-1}-1})^{d'_i-1},\ \bigwedge_{1\le i\le s}T_{d_{i-1}-1}\neq 0,\ \bigwedge_{1\le i\le s}\ell_i\neq 0,\ \bigwedge_{1\le i\le s}\ell'_i\neq 0, \tag{4}$$
$$\bigwedge_{\substack{1\le i\le s,\\ d'_i\,\mathrm{even}}} z_i\neq 0,\ \bigwedge_{\substack{1\le i\le s,\\ d'_i\,\mathrm{odd}}}\mathrm{sign}(\ell_{i-1}^2\cdot {\ell'_i}^2\cdot \mathrm{sR}_{d_{i-1}}^{2d'_i-1}\cdot \mathrm{sR}_{d_i}) = \tau(d_{i-1})\tau(d_i),\ \mathcal{H}\ \downarrow_{\mathbf{K}[v][\ell,\ell',a,b]}$$

with monoid part

$$S^{\frac12 p(p+1)\tilde e}\cdot \prod_{1\le i\le s} T_{d_{i-1}-1}^{d'_ip(p+1)e\tilde e}\cdot \prod_{\substack{1\le i\le s,\\ d'_i\,\mathrm{odd}}}(\ell_{i-1}\cdot\ell'_i)^{\frac12 p(p+1)(d'_i(d'_i-1)e+4e_i)\tilde e}\cdot(\mathrm{sR}_{d_{i-1}}^{2d'_i-1}\cdot \mathrm{sR}_{d_i})^{p(p+1)e_i\tilde e}$$
$$\cdot\prod_{\substack{1\le i\le s,\\ d'_i\,\mathrm{even}}}(\ell_{i-1}\cdot\ell'_i)^{\frac12 p(p+1){d'_i}^2e\tilde e}\cdot\prod_{\substack{1\le i\le s,\\ d'_i\,\mathrm{even}}}(a_i^2+b_i^2)^{\frac12 p(p+1)d'_ie\tilde e} := S_1\cdot \prod_{\substack{1\le i\le s,\\ d'_i\,\mathrm{even}}}(a_i^2+b_i^2)^{\frac12 p(p+1)d'_ie\tilde e},$$

degree in w bounded by

$$\delta'_w := \tilde e\Big(\frac12 p(p+1)\delta_w + (4p^2(q+3)+p(q+3)+5)\max\{\deg_w P,\deg_w Q\}\Big),$$

degree in ℓ_i bounded by

$$\delta'_\ell := \tilde e\Big(\frac12 p(p+1)\delta_\ell + 4p^2(q+3)+p(q+3)+5\Big)$$

degree in ℓ'_i bounded by

$$\delta'_{\ell'} := \tilde e\Big(\frac12 p(p+1)\delta_{\ell'} + 4p^2(q+3)+p(q+3)+5\Big)$$

and degree in (a_i,b_i) bounded by

$$\delta'_z := \tilde e\Big(\frac12 p(p+1)\delta_z + 4p^2(q+3)+p(q+3)+5\Big).$$

Then we successively apply to (4) for $1\le i\le s$ with d'_i odd the weak inference

$$\mathrm{sign}(\mathrm{sR}_{d_i}) = \tau(i),\ \mathrm{sign}(\mathrm{sR}_{d_{i-1}}) = \tau(i-1),\ \ell_{i-1}^2>0,\ {\ell'_i}^2>0 \quad\vdash$$

$$\vdash \quad \mathrm{sign}(\ell_{i-1}^2 \cdot \ell_i'^2 \cdot \mathrm{sR}_{d_{i-1}}^{2d_i'-1} \cdot \mathrm{sR}_{d_{i-1}}) = \tau(i)\tau(i-1).$$

By Lemma 2.1.2 (item 8) we obtain an incompatibility with the same monoid part and degree bounds.

Then we successively apply for $1 \le i \le s$ with d_i' even the weak inferences

$$\begin{aligned} (\mathrm{sR}_{d_{i-1}} \cdot T_{d_{i-1}-1})^{d_i'-1} \neq 0 \quad &\vdash \quad \exists z_i \; [\; z_i \neq 0,\; z_i^2 = (\mathrm{sR}_{d_{i-1}} \cdot T_{d_{i-1}-1})^{d_i'-1} \;], \\ \mathrm{sR}_{d_{i-1}} \neq 0,\; T_{d_{i-1}-1} \neq 0 \quad &\vdash \quad (\mathrm{sR}_{d_{i-1}} \cdot T_{d_{i-1}-1})^{d_i'-1} \neq 0. \end{aligned}$$

Let $\{1 \le i \le s \mid d_i' \text{ even}\} = \{i_1 < \cdots < i_{s'}\}$ and $i_0 = 0$. Using Lemmas 2.3.2 and 2.1.2 (item 6), it can be proved by induction in r that, for $0 \le r \le s'$, after the application of the weak inferences corresponding to index r, we obtain an incompatibility with monoid part

$$S_1^{4^r} \cdot \prod_{r+1 \le j \le s'} (a_{i_j}^2 + b_{i_j}^2)^{\frac{1}{2}4^r p(p+1) d_{i_j}' e\tilde{e}} \cdot \prod_{1 \le j \le r} (\mathrm{sR}_{d_{i_j-1}} \cdot T_{d_{i_j-1}-1})^{4^{r-j+1}(\frac{1}{2}\cdot 4^{j-1} p(p+1) d_{i_j}' e\tilde{e}+1)(d_{i_j}'-1)},$$

degree in w bounded by

$$4^r \Big(\delta_w' + \big(10 + 3p^2(p+1)e\tilde{e} + 4\delta_z'\big) p(q+3)(p - d_{i_r}) \max\{\deg_w P, \deg_w Q\} \Big),$$

degree in ℓ_i bounded by $4^r \delta_\ell'$ and degree in ℓ_i' bounded by $4^r \delta_{\ell'}'$ and degree in (a_{i_j}, b_{i_j}) bounded by $4^r \delta_z'$ for $r+1 \le j \le s'$. At the end we obtain an incompatibility with monoid part

$$S^{\frac{1}{2}4^{s'} p(p+1)\tilde{e}} \cdot \prod_{1 \le i \le s} \ell_i^{2g_i} \cdot \ell_i'^{2g_i'} \cdot \mathrm{sR}_{d_i}^{2h_i} \cdot T_{d_{i-1}-1}^{2h_i'}$$

with

$$h_i \le \frac{1}{2} 4^{s'} \Big(2p^2(p+1)e' + \frac{1}{2} p^3 (p+1) e \Big) \tilde{e}, \qquad h_i' \le 4^{s'-1} p^2 (p+1)(p+2) e\tilde{e},$$

degree in w bounded by

$$\delta_w'' := 4^{s'} \Big(\delta_w' + \big(10 + 3p^2(p+1)e\tilde{e} + 4\delta_z'\big) p^2 (q+3) \max\{\deg_w P, \deg_w Q\} \Big),$$

degree in ℓ_i bounded by $4^{s'} \delta_\ell'$ and degree in ℓ_i' bounded by $4^{s'} \delta_{\ell'}'$. An explicit bound for g_i and g_i' will not be necessary.

Then we successively apply for $1 \le i \le s$ the weak inferences

$$\begin{aligned} \mathrm{sign}(\mathrm{sR}_{d_i}) = \tau(i) \quad &\vdash \quad \mathrm{sR}_{d_i} \neq 0, \\ \ell_i' \neq 0 \quad &\vdash \quad \ell_i'^2 > 0, \\ \ell_i \neq 0 \quad &\vdash \quad \ell_i^2 > 0, \\ T_{d_{i-1}-1} \neq 0 \quad &\vdash \quad \exists \ell_i' \; [\; \ell_i' \neq 0,\; \ell_i' \cdot T_{d_{i-1}-1} = 1 \;]. \end{aligned}$$

By Lemmas 2.1.2 (items 2 and 4) and 2.2.2 we obtain an incompatibility

$$\begin{aligned} \downarrow \; \textstyle\bigwedge_{0 \le i \le p-1} \mathrm{sign}(\mathrm{HMi}_i(P;Q)) = \tau(i),\; \bigwedge_{1 \le i \le s} \ell_i \cdot \mathrm{sR}_{d_i} = 1, \\ \textstyle\bigwedge_{1 \le i \le s} \ell_i \neq 0,\; \bigwedge_{1 \le i \le s} T_{d_{i-1}-1} \neq 0,\; \mathcal{H} \; \downarrow_{\mathbf{K}[v][\ell]} \end{aligned} \tag{5}$$

with monoid part

$$S^{\frac{1}{2}4^{s'}p(p+1)\tilde{e}} \cdot \prod_{1\le i\le s} \ell_i^{2g_i} \cdot \mathrm{sR}_{d_i}^{2h_i} \cdot T_{d_{i-1}-1}^{2h'_i+4^{s'}\delta'_{\ell'}-2g_i},$$

degree in w bounded by $\delta''_w + s4^{s'}p(q+3)\delta'_{\ell'}\max\{\deg_w P, \deg_w Q\}$ and degree in ℓ_i bounded by $4^{s'}\delta'_\ell$.

For $1 \le i \le s$, we successively multiply (5) by the polynomial $W(C,D)^{2h'_i+4^{s'}\delta'_{\ell'}-2g_i}$, where $W(C,D)$ is the polynomial from Lemma 5.2.15, and we substitute $T_{d_{i-1}-1}\cdot W$ in the monoid part of the result using the identity from this lemma. We obtain

$$\downarrow \bigwedge_{0\le i\le p-1} \mathrm{sign}(\mathrm{HMi}_i(P;Q)) = \tau(i) \ \bigwedge_{1\le i\le s} \ell_i\cdot \mathrm{sR}_{d_i} = 1,\ \bigwedge_{1\le i\le s} \ell_i \neq 0,\ \mathcal{H} \downarrow_{\mathbf{K}[v][\ell]} \tag{6}$$

with monoid part

$$S^{\frac{1}{2}4^{s'}p(p+1)\tilde{e}} \cdot \prod_{1\le i\le s} \ell_i^{2g_i} \cdot \mathrm{sR}_{d_i}^{2h''_i}$$

with

$$h''_i \le h_i + p^p(q+3)^p 4^{s'-1}(p^2(p+1)(p+2)e\tilde{e} + 2\delta'_{\ell'})$$

degree in w bounded by

$$\delta''_w + 4^{s'}\Big(sp(q+3)\delta'_{\ell'} + p^{p+1}(q+3)^{p+1}(p^2(p+1)(p+2)e\tilde{e} + 2\delta'_{\ell'})\Big)\max\{\deg_w P, \deg_w Q\}$$

and degree in ℓ_i bounded by $4^{s'}\delta'_\ell$.

Finally we successively apply to (6) for $1 \le i \le s$ the weak inferences

$$\mathrm{sR}_{d_i} \neq 0 \quad \vdash \quad \exists \ell_i\ [\ \ell_i \neq 0,\ \ell_i\cdot \mathrm{sR}_{d_i} = 1\ ],$$

$$\mathrm{sign}(\mathrm{sR}_{d_i}) = \tau(d_i) \quad \vdash \quad \mathrm{sR}_{d_i} \neq 0.$$

By Lemmas 2.2.2 and 2.1.2 (item 2) we obtain

$$\downarrow \bigwedge_{0\le i\le p-1} \mathrm{sign}(\mathrm{HMi}_i(P;Q)) = \tau(i),\ \mathcal{H} \downarrow_{\mathbf{K}[v]}$$

with monoid part

$$S^{\frac{1}{2}4^{s'}p(p+1)\tilde{e}} \cdot \prod_{1\le i\le s} \mathrm{sR}_{d_i}^{2h''_i+4^{s'}\delta'_\ell-2g_i}$$

and degree in w bounded by

$$\delta''_w + 4^{s'}\Big(sp(q+3)(\delta'_\ell + \delta'_{\ell'}) + p^{p+1}(q+3)^{p+1}(p^2(p+1)(p+2)e\tilde{e} + 2\delta'_{\ell'})\Big)\max\{\deg_w P, \deg_w Q\}$$

which serves as the final incompatibility, taking into account that $s' \le \frac{p}{2}$. □

5.3 Sylvester Inertia Law

Sylvester Inertia Law states that two diagonal reductions of a quadratic form in an ordered field have the same number of positive, negative and null coefficients. In order to obtain Sylvester Inertia Law as an incompatibility, we use linear algebra à la Gram. First, we introduce some definitions, notation and properties. We refer to [17] and [36] for further details and proofs.

Definition 5.3.1 *Let $\mathbf{A}$ be a commutative ring, $\boldsymbol{A} \in \mathbf{A}^{m\times n}$ and $k \in \mathbb{N}$.*

1. *The* Gram's coefficient $\mathrm{Gram}_k(\boldsymbol{A})$ *is the coefficient g_k of the polynomial*

$$\det(\mathrm{I}_m + y \cdot \boldsymbol{A} \cdot \boldsymbol{A}^{\mathrm{t}}) = g_0 + g_1 \cdot y + \cdots + g_m \cdot y^m,$$

   where y is an indeterminate over $\mathbf{A}$.

2. *The matrix $\boldsymbol{A}^{\ddagger_k} \in \mathbf{A}^{n\times m}$ is the matrix*

$$\boldsymbol{A}^{\ddagger_k} = \Big(\sum_{0\le i\le k-1} (-1)^i \mathrm{Gram}_{k-1-i}(\boldsymbol{A}) \cdot (\boldsymbol{A}^{\mathrm{t}} \cdot \boldsymbol{A})^i \Big) \cdot \boldsymbol{A}^{\mathrm{t}}.$$

Note that $\mathrm{Gram}_k(\boldsymbol{A})$ is an homogeneous polynomial of degree $2k$ in the entries of $\boldsymbol{A}$ and the entries of $\boldsymbol{A}^{\ddagger_k}$ are homogeneous polynomials of degree $2k-1$ in the entries of $\boldsymbol{A}$. Note also that $\mathrm{Gram}_0(\boldsymbol{A}) = 1$ and $\mathrm{Gram}_k(\boldsymbol{A}) = 0$ for $k > m$. For $1 \le k \le m$, $\mathrm{Gram}_k(\boldsymbol{A})$ is equal to the sum of the squares of all the k-minors of $\mathbf{A}$.

Notation 5.3.2 *Let $\mathbf{A}$ be a commutative ring, $\boldsymbol{A} \in \mathbf{A}^{m\times n}$ and $k \in \mathbb{N}$. We denote by $\mathcal{D}_k(\boldsymbol{A})$ the ideal generated by all the k-minors of the matrix $\boldsymbol{A}$.*

Proposition 5.3.3 *Let $\mathbf{A}$ be a commutative ring, $\boldsymbol{A} \in \mathbf{A}^{m\times n}$, $v \in \mathbf{A}^m$, $k \in \mathbb{N}$ and let $\boldsymbol{A}|\boldsymbol{v}$ be the matrix in $\mathbf{A}^{m\times(n+1)}$ obtained by adding $\boldsymbol{v}$ as a last column to $\boldsymbol{A}$. Then*

$$\mathrm{Gram}_k(\boldsymbol{A}) \cdot \boldsymbol{v} = \boldsymbol{A} \cdot \boldsymbol{A}^{\ddagger_k} \cdot \boldsymbol{v} \mod \mathcal{D}_{k+1}(\boldsymbol{A}|\boldsymbol{v}).$$

Moreover, this equation is given by homogeneous identities of degree $2k$ in the entries of $\boldsymbol{A}$ and of degree 1 in the entries of $\boldsymbol{v}$.

The following proposition plays a fundamental role to express Sylvester Inertia Law as an incompatibility.

Proposition 5.3.4 *Let $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s, \boldsymbol{w}_1, \ldots, \boldsymbol{w}_{t+1} \in \mathbf{K}[u]^p$ with $s \in \mathbb{N}_*, t \in \mathbb{N}, s+t = p$, $\boldsymbol{A} \in \mathbf{K}[u]^{p\times p}$ be a symmetric matrix, and let $\boldsymbol{V} \in \mathbf{K}[u]^{p\times s}$ be the matrix having $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s$ as columns. Then, there is an incompatibility*

$$\downarrow \mathrm{Gram}_s(\boldsymbol{V}) \neq 0, \ \bigwedge_{1\le i\le s} \boldsymbol{v}_i^{\mathrm{t}} \cdot \boldsymbol{A} \cdot \boldsymbol{v}_i \ge 0, \ \bigwedge_{1\le i<i'\le s} \boldsymbol{v}_i^{\mathrm{t}} \cdot \boldsymbol{A} \cdot \boldsymbol{v}_{i'} = 0,$$

$$\bigwedge_{1\le j\le t+1} \boldsymbol{w}_j^{\mathrm{t}} \cdot \boldsymbol{A} \cdot \boldsymbol{w}_j < 0, \ \bigwedge_{1\le j<j'\le t+1} \boldsymbol{w}_j^{\mathrm{t}} \cdot \boldsymbol{A} \cdot \boldsymbol{w}_{j'} = 0 \downarrow$$

with monoid part

$$\mathrm{Gram}_s(\boldsymbol{V})^{2^{2(t+1)}} \cdot \prod_{1\le j\le t+1} (\boldsymbol{w}_j^{\mathrm{t}} \cdot \boldsymbol{A} \cdot \boldsymbol{w}_j)^{2^{2(t-j)+3}}$$

and degree in $w \subset u$ *bounded by*

$$\frac{2}{3}(2^{2(t+1)}-1)\deg_w \boldsymbol{A}+\frac{4}{3}\Big(2^{2t+1}(3s+2)-1\Big)\max\{\deg_w \boldsymbol{v}_i \mid 1\le i\le s\}\cup\{\deg_w \boldsymbol{w}_i \mid 1\le j\le t+1\}.$$

Proof. Let $\mathcal{H}$ be the system of sign conditions whose incompatibility we want to obtain. Let $\delta_w = \deg_w \boldsymbol{A}$ and $\delta'_w = \max\{\deg_w \boldsymbol{v}_i \mid 1 \le i \le s\} \cup \{\deg_w \boldsymbol{w}_i \mid 1 \le j \le t+1\}$. For $0 \le j \le t+1$, we consider the matrix $\boldsymbol{V}_{s+j} \in \mathbf{A}^{p\times(s+j)}$ having the vectors $\boldsymbol{v}_1, \dots, \boldsymbol{v}_s, \boldsymbol{w}_1, \dots, \boldsymbol{w}_j$ as columns. We denote by G_{s+j} the Gram's coefficient $\mathrm{Gram}_{s+j}(\boldsymbol{V}_{s+j}) \in \mathbf{K}[u]$.

For $1 \le j \le t+1$, we apply Proposition 5.3.3 to the matrix $\boldsymbol{V}_{s+j-1}$, the vector $\boldsymbol{w}_j$ and the number $s+j-1$. If for $1 \le k \le s+j-1$ we denote $H_{s+j-1,k}$ the k-th coordinate of the vector $\boldsymbol{V}_{s+j-1}^{\ddagger_{s+j-1}} \cdot \boldsymbol{w}_j$, we obtain

$$G_{s+j-1}\cdot \boldsymbol{w}_j - \sum_{1\le k\le j-1} H_{s+j-1,s+k}\cdot \boldsymbol{w}_k = \sum_{1\le i\le s} H_{s+j-1,i}\cdot \boldsymbol{v}_i \mod \mathcal{D}_{s+j}(\boldsymbol{V}_{s+j}). \tag{7}$$

Next we apply to (7) the quadratic form associated to $\boldsymbol{A}$. After passing some terms to the left hand side, we obtain for $1 \le j \le t+1$,

$$G_{s+j-1}^2\cdot \boldsymbol{w}_j^{\mathrm{t}}\cdot \boldsymbol{A}\cdot \boldsymbol{w}_j + \sum_{1\le k\le j-1} H_{s+j-1,s+k}^2\cdot \boldsymbol{w}_k^{\mathrm{t}}\cdot \boldsymbol{A}\cdot \boldsymbol{w}_k - \sum_{1\le i\le s} H_{s+j-1,i}^2\cdot \boldsymbol{v}_i^{\mathrm{t}}\cdot \boldsymbol{A}\cdot \boldsymbol{v}_i + Z_j = D_{s+j} \tag{8}$$

with $Z_j \in \mathscr{Z}(\mathcal{H}_=)$ and $D_{s+j} \in \mathcal{D}_{s+j}(\boldsymbol{V}_{s+j})$. The degree in w of the first three terms of (8) and the components of Z_j and D_{s+j} is bounded by $\delta_w + (4(s+j)-2)\delta'_w$.

Raising (8) to the square, we obtain

$$G_{s+j-1}^4\cdot (\boldsymbol{w}_j^{\mathrm{t}}\cdot \boldsymbol{A}\cdot \boldsymbol{w}_j)^2 + N_j + Z'_j = D_{s+j}^2 \tag{9}$$

with $N_j \in \mathscr{N}(\mathcal{H}_\ge)$ and $Z'_j \in \mathscr{Z}(\mathcal{H}_=)$. Let $M_1, \dots, M_\ell \in \mathbf{K}[u]$ be all the $(s+j)$-minors of the matrix $\boldsymbol{V}_{s+j}$ and consider $Q_1, \dots, Q_\ell \in \mathbf{K}[u]$ such that $D_{s+j} = \sum_{1\le k\le \ell} M_k \cdot Q_k$. Note that for $1 \le k \le \ell$, $\deg_w M_k \le (s+j)\delta'_w$ and $\deg_w Q_k \le \delta_w + (3(s+j)-2)\delta'_w$. Adding to both sides of (9) the sum of squares $\mathrm{N}(M_1, \dots, M_\ell, Q_1, \dots, Q_\ell)$ defined in Remark 2.1.13, we obtain for $1 \le j \le t+1$,

$$G_{s+j-1}^4\cdot (\boldsymbol{w}_j^{\mathrm{t}}\cdot \boldsymbol{A}\cdot \boldsymbol{w}_j)^2 + N'_j + Z'_j = G_{s+j}\cdot R_{s+j} \tag{10}$$

with $N'_j \in \mathscr{N}(\mathcal{H}_\ge)$ and $R_{s+j} = 2^\ell \sum_{1\le k\le \ell} Q_k^2$. The degree in w of the first term of (10) and the components of N'_j and Z'_j is bounded by $2\delta_w + (8(s+j)-4)\delta'_w$.

We will prove by induction on h that for $1 \le h \le t+1$ we have an identity

$$G_s^{4^h}\cdot \prod_{1\le j\le h} (\boldsymbol{w}_j^{\mathrm{t}}\cdot \boldsymbol{A}\cdot \boldsymbol{w}_j)^{2\cdot 4^{h-j}} + N''_h + Z''_h = G_{s+h}\cdot \prod_{1\le j\le h} R_{s+j}^{4^{h-j}} \tag{11}$$

with $N''_h \in \mathscr{N}(\mathcal{H}_\ge)$, $Z''_h \in \mathscr{Z}(\mathcal{H}_=)$ and degree in w of the first term of (11) and the components of N''_h and Z''_h bounded by

$$\frac{2}{3}(4^h-1)\delta_w + \frac{2}{3}\Big(4^h(3s+2)-2\Big)\delta'_w.$$

For $h = 1$, we take equation (10) for $j = 1$. Suppose now we have an equation like (11) for some $1 \leq h \leq t$. We raise it to the 4-th power and we multiply the result by $(\boldsymbol{w}_{h+1}^{\mathrm{t}} \cdot \boldsymbol{A} \cdot \boldsymbol{w}_{h+1})^2$. We obtain

$$G_s^{4^{h+1}} \cdot \prod_{1 \leq j \leq h+1} (\boldsymbol{w}_j^{\mathrm{t}} \cdot \boldsymbol{A} \cdot \boldsymbol{w}_j)^{2 \cdot 4^{h+1-j}} + N_h''' + Z_h''' = G_{s+h}^4 \cdot (\boldsymbol{w}_{h+1}^{\mathrm{t}} \cdot \boldsymbol{A} \cdot \boldsymbol{w}_{h+1})^2 \cdot \prod_{1 \leq j \leq h} R_{s+j}^{4^{h+1-j}} \quad (12)$$

with $N_h''' \in \mathscr{N}(\mathcal{H}_{\geq})$ and $Z_h''' \in \mathscr{Z}(\mathcal{H}_{=})$. On the other hand, we multiply equation (10) for $j = h+1$ by $\prod_{1 \leq j \leq h} R_{s+j}^{4^{h+1-j}}$ and we obtain

$$G_{s+h}^4 \cdot (\boldsymbol{w}_{h+1}^{\mathrm{t}} \cdot \boldsymbol{A} \cdot \boldsymbol{w}_{h+1})^2 \cdot \prod_{1 \leq j \leq h} R_{s+j}^{4^{h+1-j}} + N_{h+1}'''' + Z_{h+1}'''' = G_{s+h+1} \cdot \prod_{1 \leq j \leq h+1} R_{s+j}^{4^{h+1-j}} \quad (13)$$

with $N_h'''' \in \mathscr{N}(\mathcal{H}_{\geq})$ and $Z_h'''' \in \mathscr{Z}(\mathcal{H}_{=})$. Finally, by adding equations (12) and (13) and simplifying equal terms at both sides of the identity, we obtain an equation like (11) for $h+1$. The degree bound follows easily.

Taking into account that $G_s = \mathrm{Gram}_s(\boldsymbol{V})$ and $G_{s+t+1} = 0$ since $\boldsymbol{V}_{s+t+1}$ has only $p = s+t$ rows, the proposition follows by considering the incompatibility $\downarrow \mathcal{H} \downarrow$ obtained taking $h = t+1$ in equation (11). □

Lemma 5.3.5 *Let $\boldsymbol{C} \in \mathbf{K}[u]^{p \times p}$, $1 \leq s \leq p$, $1 \leq i_1 < \cdots < i_s \leq p$ and $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s \in \mathbf{K}[u]^p$ be the columns $i_1, \ldots, i_s$ of $\boldsymbol{C}$. Then*

$$\det(\boldsymbol{C}) \neq 0 \quad \vdash \quad \mathrm{Gram}_s([\boldsymbol{v}_1 | \ldots | \boldsymbol{v}_s]) \neq 0,$$

where $[\boldsymbol{v}_1 | \ldots | \boldsymbol{v}_s]$ is the matrix in $\mathbf{K}[u]^{p \times s}$ formed by the vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_s$ as columns. If we have an initial incompatibility in variables $v \supset u$ with monoid part $S \cdot \mathrm{Gram}_s([\boldsymbol{v}_1 | \ldots | \boldsymbol{v}_s])^{2e}$ and degree in $w \subset v$ bounded by δ_w, the final incompatibility has monoid part $S \cdot \det(\boldsymbol{C})^{4e}$ and degree in w bounded by $\delta_w + 4e(p-s)\deg_w \boldsymbol{C}$.

Proof. By the Generalized Laplace Expansion Theorem, $\det(\boldsymbol{C})$ is a linear combination of the s minors of $[\boldsymbol{v}_1 | \ldots | \boldsymbol{v}_s]$, where the coefficients are, up to sign, $p-s$ minors of the matrix formed with the remaining columns of $\boldsymbol{C}$. Then, the lemma follows from Lemma 2.1.15. □

We can prove now an incompatibility version of Sylvester Inertia Law.

Theorem 5.3.6 (Sylvester Inertia Law as an incompatibility) *Let $\boldsymbol{A} \in \mathbf{K}[u]^{p \times p}$ be a symmetric matrix, $\boldsymbol{B}, \boldsymbol{B}' \in \mathbf{K}[u]^{p \times p}$, $\boldsymbol{D}, \boldsymbol{D}' \in \mathbf{K}[u]^{p \times p}$ be diagonal matrices with $(\boldsymbol{D})_{ii} = D_i$ for $1 \leq i \leq p$ and $(\boldsymbol{D}')_{jj} = D_j'$ for $1 \leq j \leq p$ and $\eta, \eta' \in \{-1, 0, 1\}^p$. If the number of coordinates in η and η' equal to -1, 0 and 1 is not respectively the same, there is an incompatibility*

$$\downarrow \boldsymbol{A} \equiv \boldsymbol{B} \cdot \boldsymbol{D} \cdot \boldsymbol{B}^{\mathrm{t}},\ \boldsymbol{A} \equiv \boldsymbol{B}' \cdot \boldsymbol{D}' \cdot \boldsymbol{B}'^{\mathrm{t}},\ \det(\boldsymbol{B}) \neq 0,\ \det(\boldsymbol{B}') \neq 0,$$

$$\bigwedge_{1 \leq i \leq p} \mathrm{sign}(D_i) = \eta(i),\quad \bigwedge_{1 \leq j \leq p} \mathrm{sign}(D_j') = \eta'(j) \downarrow$$

with monoid part

$$\det(\boldsymbol{B})^{2e} \cdot \det(\boldsymbol{B})^{2e'} \cdot \prod_{\substack{1 \leq i \leq p, \\ \eta(i) \neq 0}} D_i^{2f_i} \cdot \prod_{\substack{1 \leq j \leq p, \\ \eta'(j) \neq 0}} D_j'^{2f_j'}$$

with $e, e' \leq p2^{2p}$, $f_i, f'_j \leq 2^{2(p-1)}$ *and degree in* $w \subset u$ *bounded by*

$$2^{2p}\deg_w \boldsymbol{A} + p^2 2^{2p+1}\max\{\deg_w \boldsymbol{B}, \deg_w \boldsymbol{B'}\} + 2^{2p+1}\max\{\deg_w \boldsymbol{D}, \deg_w \boldsymbol{D'}\}.$$

Proof. Let $\delta_w = \deg_w \boldsymbol{A}$, $\delta'_w = \max\{\deg_w \boldsymbol{B}, \deg_w \boldsymbol{B'}\}$ and $\delta''_w = \max\{\deg_w \boldsymbol{D}, \deg_w \boldsymbol{D'}\}$. Without loss of generality, we suppose that there are at least s coordinates $1 \leq k_1 < \cdots < k_s \leq p$ in η equal to 0 or 1 and at least $t+1$ coordinates $1 \leq k'_1 < \cdots < k'_{t+1} \leq p$ in η' equal to -1, with $s \in \mathbb{N}_*, t \in \mathbb{N}$ and $s + t = p$. We take $\boldsymbol{v}_1, \dots, \boldsymbol{v}_s$ as the columns $k_1, \dots, k_s$ of $\mathrm{Adj}(\boldsymbol{B})^{\mathrm{t}}$ and $\boldsymbol{w}_1, \dots, \boldsymbol{w}_{t+1}$ as the columns $k'_1, \dots, k'_{t+1}$ of $\mathrm{Adj}(\boldsymbol{B'})^{\mathrm{t}}$.

We successively apply to the incompatibility from Proposition 5.3.4 the weak inferences

$$\begin{aligned} \det(\mathrm{Adj}(\boldsymbol{B})^{\mathrm{t}}) \neq 0 \quad &\vdash \quad \mathrm{Gram}_s(\boldsymbol{V}) \neq 0, \\ \det(\boldsymbol{B}) \neq 0 \quad &\vdash \quad \det(\mathrm{Adj}(\boldsymbol{B})^{\mathrm{t}}) \neq 0. \end{aligned}$$

Since $\det(\mathrm{Adj}(\boldsymbol{B})^{\mathrm{t}}) = \det(\boldsymbol{B})^{p-1}$, by Lemmas 5.3.5 and 2.1.2 (item 6), we obtain an incompatibility with monoid part

$$\det(\boldsymbol{B})^{(p-1)2^{2t+3}} \cdot \prod_{1 \leq j \leq t+1} (\boldsymbol{w}_j^{\mathrm{t}} \cdot \boldsymbol{A} \cdot \boldsymbol{w}_j)^{2^{2(t-j)+3}}$$

and degree in w bounded by

$$\frac{2}{3}(2^{2(t+1)} - 1)\delta_w + (p-1)\Big(2^{2t+3}\Big(p + \frac{2}{3}\Big) - \frac{4}{3}\Big)\delta'_w.$$

Then we successively apply for $1 \leq i \leq s$ and for $1 \leq j \leq t+1$ the weak inferences

$$\begin{aligned} \boldsymbol{v}_i^{\mathrm{t}} \cdot \boldsymbol{A} \cdot \boldsymbol{v}_i = \det(\boldsymbol{B})^2 \cdot D_{k_i},\ \det(\boldsymbol{B})^2 \cdot D_{k_i} \geq 0 \quad &\vdash \quad \boldsymbol{v}_i^{\mathrm{t}} \cdot \boldsymbol{A} \cdot \boldsymbol{v}_i \geq 0, \\ \det(\boldsymbol{B})^2 \geq 0,\ D_{k_i} \geq 0 \quad &\vdash \quad \det(\boldsymbol{B})^2 \cdot D_{k_i} \geq 0, \\ &\vdash \quad \det(\boldsymbol{B})^2 \geq 0, \\ \boldsymbol{w}_j^{\mathrm{t}} \cdot \boldsymbol{A} \cdot \boldsymbol{w}_j = \det(\boldsymbol{B'})^2 \cdot D'_{k'_j},\ \det(\boldsymbol{B'})^2 \cdot D'_{k'_j} < 0 \quad &\vdash \quad \boldsymbol{w}_j^{\mathrm{t}} \cdot \boldsymbol{A} \cdot \boldsymbol{w}_j < 0, \\ \det(\boldsymbol{B'})^2 > 0,\ D'_{k'_j} < 0 \quad &\vdash \quad \det(\boldsymbol{B'})^2 \cdot D'_{k'_j} < 0, \\ \det(\boldsymbol{B'}) \neq 0 \quad &\vdash \quad \det(\boldsymbol{B'})^2 > 0. \end{aligned}$$

By Lemmas 2.1.2 (items 3, 4, 7 and 8) 2.1.5 (item 15), and 2.1.7, we obtain an incompatibility with monoid part

$$\det(\boldsymbol{B})^{(p-1)2^{2t+3}} \cdot \det(\boldsymbol{B'})^{\frac{4}{3}(2^{2(t+1)}-1)} \cdot \prod_{1 \leq j \leq t+1} {D'_{k'_j}}^{2^{2(t-j)+3}}$$

and degree in w bounded by

$$\frac{2}{3}(2^{2(t+1)} - 1)\delta_w + \Big(p^2 2^{2t+3} - \frac{1}{3}p2^{2t+3} - \frac{1}{3}2^{2t+4} + 2ps - \frac{8}{3}p + \frac{4}{3}\Big)\delta'_w + \Big(s + \frac{2}{3}(2^{2(t+1)} - 1)\Big)\delta''_w.$$

Finally, we successively apply the weak inferences

$$\begin{aligned} \boldsymbol{A} \equiv \boldsymbol{B} \cdot \boldsymbol{D} \cdot \boldsymbol{B}^{\mathrm{t}} \quad &\vdash \quad \mathrm{Adj}(\boldsymbol{B}) \cdot \boldsymbol{A} \cdot \mathrm{Adj}(\boldsymbol{B})^{\mathrm{t}} \equiv \det(\boldsymbol{B})^2 \cdot \boldsymbol{D}, \\ \boldsymbol{A} \equiv \boldsymbol{B}' \cdot \boldsymbol{D}' \cdot \boldsymbol{B}'^{\mathrm{t}} \quad &\vdash \quad \mathrm{Adj}(\boldsymbol{B}') \cdot \boldsymbol{A} \cdot \mathrm{Adj}(\boldsymbol{B}')^{\mathrm{t}} \equiv \det(\boldsymbol{B}')^2 \cdot \boldsymbol{D}'. \end{aligned}$$

By Lemma 2.5.3, we obtain an incompatibility with the same monoid part and degree in w bounded by

$$\frac{4}{3}(2^{2t+1}+1)\delta_w + \Big(p^2 2^{2t+3} - \frac{1}{3}p2^{2t+3} - \frac{1}{3}2^{2t+4} + 2ps + \frac{4}{3}p + \frac{4}{3}\Big)\delta'_w + \Big(s + \frac{4}{3}(2^{2t+1}+1)\Big)\delta''_w.$$

which is the incompatibility we wanted to obtain. □

5.4 Hermite's quadratic form and Sylvester Inertia Law

In order to obtain the main result of this section, we combine now Sylvester Inertia Law with the two methods we have considered to compute the signature of the Hermite's quadratic form.

Notation 5.4.1 *Let $p \in \mathbb{N}_*$.*

- *For $\tau \in \{-1,0,1\}^{\{0,\dots,p-1\}}$ and $d(\tau) = (d_0,\dots,d_s)$, we denote by*
  - $\mathrm{Rk}_{\mathrm{HMi}}(\tau) = p - d_s$,
  - $\mathrm{Si}_{\mathrm{HMi}}(\tau) = \sum_{\substack{1 \le i \le s, \\ d_{i-1}-d_i \text{ odd}}} \varepsilon_{d_{i-1}-d_i}\tau(d_{i-1})\tau(d_i)$.
- *For $m, n \in \mathbb{N}$ with $m + 2n = p$, $\boldsymbol{\eta} \in \{-1,0,1\}^m$ and $\boldsymbol{\kappa} \in \{0,1\}^n$, we denote by*
  - $\mathrm{Rk}_{\mathrm{Fact}}(\boldsymbol{\eta},\boldsymbol{\kappa})$ *the addition of the number of coordinates in $\boldsymbol{\eta}$ equal to -1 or 1 and twice the number of coordinates in $\boldsymbol{\kappa}$ equal to 1,*
  - $\mathrm{Si}_{\mathrm{Fact}}(\boldsymbol{\eta})$ *the number of coordinates in $\boldsymbol{\eta}$ equal to 1 minus the number of coordinates in $\boldsymbol{\eta}$ equal to -1.*

Note that $\mathrm{Rk}_{\mathrm{HMi}}(\tau)$ and $\mathrm{Si}_{\mathrm{HMi}}(\tau)$ are respectively the rank and signature of the matrix $\mathrm{Her}(P;Q)$ if τ is the sign condition satisfied by $\mathrm{HMi}(P;Q)$. Similarly, $\mathrm{Rk}_{\mathrm{Fact}}(\boldsymbol{\eta},\boldsymbol{\kappa})$ and $\mathrm{Si}_{\mathrm{Fact}}(\boldsymbol{\eta})$ are respectively the rank and signature of the matrix $\mathrm{Her}(P;Q)$ if in the decomposition into real irreducible factors of P, $\boldsymbol{\eta}$ is the sign condition satisfied by the real roots of P at Q and $\boldsymbol{\kappa}$ is the invertibility condition satisfied by the complex non-real roots of P at Q.

We define a new auxiliary function.

Definition 5.4.2 *Let $\mathrm{g}_H : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $\mathrm{g}_H\{p,q\} = 39 \cdot 2^{7p} p^{5p+6} (q+3)^{4p+2}$.*

In the following theorem, we combine Sylvester Inertia Law with Hermite's Theory as an incompatibility. To do so, we use many previously given definitions and notation, namely Notation 2.4.5, Notation 4.3.1, Definition 4.3.2, Definition 5.1.4, Definition 5.1.5, Notation 5.2.1 and Notation 5.4.1.

Theorem 5.4.3 (Hermite's Theory as an incompatibility) *Let* $P, Q \in \mathbf{K}[u][y]$ *with* $\deg_y P = p \geq 1$, $\deg_y Q = q$ *and* P *monic with respect to* y. *For* $\tau \in \{-1,0,1\}^{\{0,\dots,p-1\}}$, $d(\tau) = (d_0,\dots,d_s)$, $m+2n=p$, $(\boldsymbol{\mu},\boldsymbol{\nu}) \in \Lambda_m \times \Lambda_n$, $\boldsymbol{\eta} \in \{-1,0,1\}^{\#\boldsymbol{\mu}}$, $\boldsymbol{\kappa} \in \{0,1\}^{\#\boldsymbol{\nu}}$ *such that* $(\mathrm{Rk}_{\mathrm{HMi}}(\tau), \mathrm{Si}_{\mathrm{HMi}}(\tau)) \neq (\mathrm{Rk}_{\mathrm{Fact}}(\boldsymbol{\eta},\boldsymbol{\kappa}), \mathrm{Si}_{\mathrm{Fact}}(\boldsymbol{\eta}))$, $t = (t_1,\dots,t_{\#\boldsymbol{\mu}})$ *and* $z = (z_1,\dots,z_{\#\boldsymbol{\nu}})$, *we have*

$$\downarrow \bigwedge_{0\leq i\leq p-1} \mathrm{sign}(\mathrm{HMi}_i(P;Q)) = \tau(i),\ \mathrm{Fact}(P)^{\boldsymbol{\mu},\boldsymbol{\nu}}(t,z),$$

$$\bigwedge_{1\leq j\leq \#\boldsymbol{\mu}} \mathrm{sign}(Q(t_j)) = \eta_j,\ \bigwedge_{1\leq k\leq \#\boldsymbol{\nu}} \mathrm{inv}(Q(z_k)) = \kappa_k \downarrow_{\mathbf{K}[u][t,a,b]}$$

with monoid part

$$\prod_{1\leq i\leq s} \mathrm{HMi}_{d_i}(P;Q)^{2g_i} \cdot \prod_{1\leq j<j'\leq \#\boldsymbol{\mu}} (t_j - t_{j'})^{2e_{j,j'}} \cdot \prod_{1\leq k\leq \#\boldsymbol{\nu}} b_k^{2f_k} \cdot$$

$$\cdot \prod_{1\leq k<k'\leq \#\boldsymbol{\nu}} \mathrm{R}(z_k,z_{k'})^{2g_{k,k'}} \cdot \prod_{\substack{1\leq j\leq \#\boldsymbol{\mu},\\ \eta_j\neq 0}} Q(t_j)^{2e'_j} \cdot \prod_{\substack{1\leq k\leq \#\boldsymbol{\nu},\\ \kappa_k\neq 0}} (Q_{\mathrm{Re}}^2(z_k) + Q_{\mathrm{Im}}^2(z_k))^{2f'_k}$$

with $g_i, e_{j,j'}, f_k, g_{k,k'}, e'_j, f'_k \leq \mathrm{g}_H\{p,q\}$, *degree in* $w \subset u$ *bounded by* $\mathrm{g}_H\{p,q\}\max\{\deg_w P, \deg_w Q\}$ *and degree in* t_j *and degree in* (a_k,b_k) *bounded by* $\mathrm{g}_H\{p,q\}$.

Proof. We evaluate

$$\boldsymbol{A} = \mathrm{Her}(P;Q),\ \boldsymbol{B} = \mathrm{B}_{\boldsymbol{\kappa}}(t,z,z'),\ \boldsymbol{D} = \mathrm{Di}_Q^{\boldsymbol{\mu},\boldsymbol{\nu},\boldsymbol{\kappa}}(t), \boldsymbol{B'} = \mathrm{B}^{\tau}_{P;Q}(\ell,\ell',z''),\ \boldsymbol{D'} = \mathrm{Di}^{\tau}_{P;Q}(\ell,\ell')$$

in the incompatibility from Theorem 5.3.6 (Sylvester Inertia Law as an incompatibility), where $z' = (z'_k)_{\kappa_k=1}$, $\ell = (\ell_1,\dots,\ell_s)$, $\ell' = (\ell'_1,\dots,\ell'_s)$ and $z'' = (z''_i)_{d_{i-1}-d_i\,\mathrm{even}}$ and we obtain

$$\downarrow \mathrm{Her}(P;Q) \equiv \mathrm{B}_{\boldsymbol{\kappa}}(t,z,z') \cdot \mathrm{Di}_Q^{\boldsymbol{\mu},\boldsymbol{\nu},\boldsymbol{\kappa}}(t) \cdot \mathrm{B}^{\mathrm{t}}_{\boldsymbol{\kappa}}(t,z,z'),\ \det(\mathrm{B}_{\boldsymbol{\kappa}}(t,z,z')) \neq 0,$$

$$\mathrm{Her}(P;Q) \equiv \mathrm{B}^{\tau}_{P;Q}(\ell,\ell',z'') \cdot \mathrm{Di}^{\tau}_{P;Q}(\ell,\ell') \cdot {\mathrm{B}^{\tau}_{P;Q}}^{\mathrm{t}}(\ell,\ell',z''),\ \det(\mathrm{B}^{\tau}_{P;Q}(\ell,\ell',z'')) \neq 0,$$

$$\bigwedge_{1\leq j\leq \#\boldsymbol{\mu}} \mathrm{sign}(Q(t_j)) = \eta_j,$$

$$\bigwedge_{\substack{1\leq i\leq s,\\ d_{i-1}-d_i \mathrm{odd}}} \mathrm{sign}(\ell_{i-1}^2 \cdot {\ell'_i}^2 \cdot \mathrm{HMi}_{d_{i-1}}(P;Q)^{2(d_{i-1}-d_i)-1} \cdot \mathrm{HMi}_{d_i}(P;Q)) = \tau(d_{i-1})\tau(d_i) \downarrow_{\mathbf{K}[u][t,a,b,a',b',\ell,\ell',a'',b'']} \quad (14)$$

with monoid part

$$\det(\mathrm{B}_{\boldsymbol{\kappa}}(t,z,z'))^{2e_1} \cdot \det(\mathrm{B}^{\tau}_{P;Q}(\ell,\ell',z''))^{2e_2} \cdot \prod_{\substack{1\leq j\leq \#\boldsymbol{\mu},\\ \eta_j\neq 0}} Q(t_j)^{2f_{1,j}} \cdot$$

$$\prod_{\substack{1\leq i\leq s,\\ d_{i-1}-d_i \mathrm{odd}}} \left(\ell_{i-1}^2 \cdot {\ell'_i}^2 \cdot \mathrm{HMi}_{d_{i-1}}(P;Q)^{2(d_{i-1}-d_i)-1} \cdot \mathrm{HMi}_{d_i}(P;Q)\right)^{2f_{2,i}}$$

with $e_1, e_2 \leq p2^{2p}$, $f_{1,j} \leq 2^{2(p-1)}$ and $f_{2,i} \leq p2^{2(p-1)}$, degree in w bounded by $9p^4(q+3)2^{2p}\max\{\deg_w P, \deg_w Q\}$, degree in t_j and degree in (a_k, b_k) bounded by $p^3 2^{2p+1}$, degree in (a'_k, b'_k) bounded by $p^2 2^{2p+1}$, degree in ℓ_i and degree in ℓ'_i bounded by $5p^3 2^{2p}$ and degree in (a''_i, b''_i) bounded by $p^2 2^{2p+1}$.

Then we apply to (14) the weak inference from Theorem 5.1.11 (Hermite's Theory (1) as a weak existence) and we obtain

$$\downarrow \mathrm{Fact}(P)^{\boldsymbol{\mu},\boldsymbol{\nu}}(t,z), \bigwedge_{1\leq j\leq \#\boldsymbol{\mu}} \mathrm{sign}(Q(t_j)) = \eta_j, \bigwedge_{1\leq k\leq \#\boldsymbol{\nu}} \mathrm{inv}(Q(z_k)) = \kappa_k, \mathrm{B}^{\tau}_{P;Q}(\ell,\ell',z'')$$
$$\mathrm{Her}(P;Q) \equiv \cdot\mathrm{Di}^{\tau}_{P;Q}(\ell,\ell')\cdot {\mathrm{B}^{\tau}_{P;Q}}^{\mathrm{t}}(\ell,\ell',z''),\ \det(\mathrm{B}^{\tau}_{P;Q}(\ell,\ell',z''))\neq 0,$$
$$\bigwedge_{\substack{1\leq i\leq s,\\ d_{i-1}-d_i \mathrm{odd}}} \mathrm{sign}(\ell_{i-1}^2\cdot {\ell'_i}^2\cdot \mathrm{HMi}_{d_{i-1}}(P;Q)^{2(d_{i-1}-d_i)-1}\cdot \mathrm{HMi}_{d_i}(P;Q)) = \tau(d_{i-1})\tau(d_i) \downarrow_{\mathbf{K}[u][t,a,b,\ell,\ell',a'',b'']} \tag{15}$$

with monoid part

$$\det(\mathrm{B}^{\tau}_{P;Q}(\ell,\ell',z''))^{2^{2s(\boldsymbol{\kappa})+1}e_2}\cdot \prod_{\substack{1\leq i\leq s,\\ d_{i-1}-d_i \mathrm{odd}}} \Big(\ell_{i-1}^2\cdot{\ell'_i}^2\cdot\mathrm{HMi}_{d_{i-1}}(P;Q)^{2(d_{i-1}-d_i)-1}\cdot\mathrm{HMi}_{d_i}(P;Q)\Big)^{2^{2s(\boldsymbol{\kappa})+1}f_{2,i}}\cdot$$
$$\cdot \prod_{1\leq j<j'\leq \#\boldsymbol{\mu}} (t_{j'}-t_j)^{2^{2s(\boldsymbol{\kappa})+1}e_1}\cdot \prod_{1\leq k\leq \#\boldsymbol{\nu}} b_k^{2^{2s(\boldsymbol{\kappa})+1}(2\#\boldsymbol{\mu}+1)e_1}\cdot \prod_{1\leq k<k'\leq \#\boldsymbol{\nu}} \mathrm{R}(z_k,z_{k'})^{2^{2s(\boldsymbol{\kappa})+1}e_1}\cdot$$
$$\cdot \prod_{\substack{1\leq j\leq \#\boldsymbol{\mu},\\ \eta_j\neq 0}} Q(t_j)^{2^{2s(\boldsymbol{\kappa})+1}f_{1,j}}\cdot \prod_{\substack{1\leq k\leq \#\boldsymbol{\nu},\\ \kappa_k=1}} (Q^2_{\mathrm{Re}}(z_k)+Q^2_{\mathrm{Im}}(z_k))^{2f''_k}$$

with $f''_k \leq 2^{2s(\boldsymbol{\kappa})-2}(2e_1+1)$, degree in w bounded by

$$2^{2s(\boldsymbol{\kappa})}\Big(2^{2p}(9p^4(q+3)+2s(\boldsymbol{\kappa})(3p+2p^2))+q+2p+6\Big)\max\{\deg_w P, \deg_w Q\},$$

degree in t_j bounded by

$$2^{2s(\boldsymbol{\kappa})}(p^3 2^{2p+1}+q+2p-2),$$

degree in (a_k, b_k) bounded by

$$2^{2s(\boldsymbol{\kappa})}\Big(2^{2p+1}(p^3+(3p+2p^2)q)+6q+2p-2\Big),$$

degree in ℓ_i and degree in ℓ'_i bounded by $5\cdot 2^{2s(\boldsymbol{\kappa})}p^3 2^{2p}$, and degree in (a''_i, b''_i) bounded by $2^{2s(\boldsymbol{\kappa})}p^2 2^{2p+1}$; where $s(\boldsymbol{\kappa}) = \#\{k \mid 1\leq k\leq \#\boldsymbol{\nu}, \kappa_k = 1\}$.

Finally, we apply to (15) the weak inference from Theorem 5.2.17 (Hermite's Theory (2) as a weak existence) and we obtain

$$\downarrow \bigwedge_{0\leq i\leq p-1} \mathrm{sign}(\mathrm{HMi}_i(P;Q)) = \tau(i),\ \mathrm{Fact}(P)^{\boldsymbol{\mu},\boldsymbol{\nu}}(t,z),$$
$$\bigwedge_{1\leq j\leq \#\boldsymbol{\mu}} \mathrm{sign}(Q(t_j)) = \eta_j, \bigwedge_{1\leq k\leq \#\boldsymbol{\nu}} \mathrm{inv}(Q(z_k)) = \kappa_k \downarrow_{\mathbf{K}[u][t,a,b]}$$

with monoid part

$$\prod_{1\leq i\leq s} \mathrm{HMi}_{d_i}(P;Q)^{2g_i} \cdot \prod_{1\leq j<j'\leq \#\boldsymbol{\mu}} (t_{j'}-t_j)^{2^{2s(\boldsymbol{\kappa})+1}e_1 f} \cdot \prod_{1\leq k\leq \#\boldsymbol{\nu}} b_k^{2^{2s(\boldsymbol{\kappa})+1}(2\#\boldsymbol{\mu}+1)e_1 f}$$

$$\cdot \prod_{1\leq k<k'\leq \#\boldsymbol{\nu}} \mathrm{R}(z_k, z_{k'})^{2^{2s(\boldsymbol{\kappa})+1}e_1 f} \cdot \prod_{\substack{1\leq j\leq \#\boldsymbol{\mu},\\ \eta_j\neq 0}} Q(t_j)^{2^{2s(\boldsymbol{\kappa})+1}f_{1,j} f} \cdot \prod_{\substack{1\leq k\leq \#\boldsymbol{\nu},\\ \kappa_k=1}} (Q_{\mathrm{Re}}^2(z_k)+Q_{\mathrm{Im}}^2(z_k))^{2f_k'' f}$$

with

$$\begin{array}{rcl} g_i & \leq & 2^{5p+2s(\boldsymbol{\kappa})-1}p^{4p+4}(q+3)^{3p}(5p+5p^{p+1}(q+3)^p+10p^{p+1}(q+3)^{p+1}+1), \\ f & \leq & 2^{3p}p^{4p+2}(q+3)^{3p}, \end{array}$$

degree in w bounded by

$$2^{3p+2s(\boldsymbol{\kappa})}p^{4p+2}(q+3)^{3p}\Big(2^{2p}\Big(2s(\boldsymbol{\kappa})(3p+2p^2)+17p^4(q+3)+5p^5(q+3)+$$

$$+15p^{p+4}(q+3)^{p+1}+31p^{p+4}(q+3)^{p+2}\Big)+q+2p+6\Big)\max\{\deg_w P, \deg_w Q\},$$

degree in t_j bounded by

$$2^{3p+2s(\boldsymbol{\kappa})}p^{4p+2}(q+3)^{3p}(p^3 2^{2p+1}+q+2p-2),$$

and degree in (a_k, b_k) bounded by

$$2^{3p+2s(\boldsymbol{\kappa})}p^{4p+2}(q+3)^{3p}\Big(2^{2p+1}(p^3+(3p+2p^2)q)+6q+2p-2\Big).$$

It can be easily seen that this incompatibility satisfies the required bounds to be the final incompatibility. $\square$

6 Elimination of one variable

The main results of this section are as follows: given a family $\mathcal{Q}$ of univariate polynomials depending on parameters, first, to define an eliminating family $\mathrm{Elim}(\mathcal{Q})$ of polynomials in the parameters, such that the signs of the polynomials in the eliminating family $\mathrm{Elim}(\mathcal{Q})$ determine the realizable sign conditions on $\mathcal{Q}$ and second, to translate this statement under weak inference form.

Classical Cylindrical Algebraic Decomposition (CAD) is a well known method for constructing an eliminating family, containing subresultants of pairs of polynomials of $\mathcal{Q}$ (in the case where the polynomials are all monic with respect to the main variable). However in classical CAD the properties of the eliminating family are proved using properties of semi-algebraically connected components of realization of sign conditions. Since semi-algebraic connectivity is not available in our context, we cannot use CAD.

So we need to provide a new elimination method. This new elimination method uses the fact that each real root of a polynomial is uniquely determined by the signs it gives to the derivatives of the polynomial (Thom encoding). The eliminating family of $\mathcal{Q}$ will consist of principal minors of Hermite matrices of pairs of polynomials Q_1, Q_2 where Q_1 belongs to $\mathcal{Q}$ and Q_2 is the product of (a small number of) derivatives of Q_1 and at most one polynomial in $\mathcal{Q}$ or its square, according to sign determination. Since minors of Hermite matrices coincide with subresultants (see Proposition 5.2.5), the main difference between classical CAD and the new elimination method presented here is that in the new method it is not sufficient to consider subresultants of pairs of polynomials in $\mathcal{Q}$.

In order to design our new elimination method, we proceed in severeal steps. In Subsection 6.1 we first recall the Thom encodings, which characterize the real roots of a univariate polynomial by sign conditions on the derivatives and we prove some weak inferences related to them. In Subsection 6.2 we consider a univariate polynomial P depending on parameters and define a family of eliminating polynomials in the parameters whose signs determine the Thom encodings of the real roots of P (and the sign of another polynomial at these roots).

In Subsection 6.3, we consider a whole family $\mathcal{Q}$ of univariate polynomials depending on parameters and define the family $\mathrm{Elim}(\mathcal{Q})$ whose signs determine the ordered list of real roots of all the polynomials in $\mathcal{Q}$. Finally, in Subsection 6.4, we deduce that the signs of $\mathrm{Elim}(\mathcal{Q})$ determine the realizable sign conditions on the family $\mathcal{Q}$. All the results in this section are first explained in usual mathematical terms, then translated into weak inferences.

Apart from many results from Section 2, the only results from previous sections used in this section are Theorem 4.3.5 (Real Irreducible Factors with Multiplicities as a weak existence), which is used only once in the proof of Theorem 6.2.8 (Fixing the Thom encodings as a weak existence) and Theorem 5.4.3 (Hermite's Theory as an incompatibility), which is used once in the proof of Theorem 6.2.8 (Fixing the Thom encodings as a weak existence) and once in the proof of Theorem 6.2.9 (Fixing the Thom encodings with a Sign as a weak existence).

On the other hand, the main result of the section, Theorem 6.4.4 (Elimination of One Variable as a weak inference) which describes under weak inference form the fact that the signs of $\mathrm{Elim}(\mathcal{Q})$ determine the realizable sign conditions on $\mathcal{Q}$ will be the only result from the rest of the paper used in Section 7.

6.1 Thom encoding of real algebraic numbers

We start this section with a general definition.

Definition 6.1.1 *Let $\mathcal{Q} \subset \mathbf{K}[u]$ with $u = (u_1, \ldots, u_k)$. A* sign condition *on a set $\mathcal{Q}$ is an element of $\{-1, 0, 1\}^{\mathcal{Q}}$. The realization of a sign condition τ on $\mathcal{Q}$ is defined by*

$$\mathrm{Real}(\tau, \mathbf{R}) = \{\vartheta \in \mathbf{R}^k \mid \bigwedge_{Q \in \mathcal{Q}} \mathrm{sign}(Q(\vartheta)) = \tau(Q)\}.$$

We use

$$\mathrm{sign}(\mathcal{Q}) = \tau$$

to mean

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

It will be often convenient to use the following abuse of notation.

Notation 6.1.2 *If $\tau \in \{1, 0, -1\}^{\mathcal{Q}}$ is a sign condition on $\mathcal{Q}$ and $\mathcal{Q}' \subset \mathcal{Q}$, we denote again by τ the restriction $\tau \mid_{\mathcal{Q}'}$ of τ to $\mathcal{Q}'$.*

Now we recall the Thom encoding of real algebraic numbers [12] and explaining its main properties. We refer to [4] for proofs.

Definition 6.1.3 *Let $P = \sum_{0 \leq h \leq p} \gamma_h y^h \in \mathbf{K}[y]$ with $\gamma_p \neq 0$. We denote $\mathrm{Der}(P)$ the list formed by the first $p-1$ derivatives of P and $\mathrm{Der}_+(P)$ the list formed by P and $\mathrm{Der}(P)$. A real root θ of P is uniquely determined by the sign condition on $\mathrm{Der}(P)$ evaluated at θ, i.e. the list of signs of $\mathrm{Der}(P)(\theta)$, which is called the* Thom encoding *of θ with respect to P.*

By a slight abuse of notation, we identify sign conditions on $\mathrm{Der}(P)$ (resp. $\mathrm{Der}_+(P)$), i.e. elements of $\{1, 0, -1\}^{\mathrm{Der}(P)}$ (resp. $\{1, 0, -1\}^{\mathrm{Der}_+(P)}$) with $\{-1, 0, 1\}^{\{1, \ldots, p-1\}}$ (resp. $\{-1, 0, 1\}^{\{0, \ldots, p-1\}}$). For any sign condition η on $\mathrm{Der}(P)$ or $\mathrm{Der}_+(P)$, we extend its definition with $\eta(p) = \mathrm{sign}(\gamma_p)$ if needed.

Thom encoding not only characterizes the real roots of a polynomial, it can also be used to order real numbers as follows.

Notation 6.1.4 *Let $P = \sum_{0 \leq h \leq p} \gamma_h y^h \in \mathbf{K}[y]$. For η_1, η_2 sign conditions on $\mathrm{Der}_+(P)$, we use the notation $\eta_1 \prec_P \eta_2$ to indicate that $\eta_1 \neq \eta_2$ and, if q is the biggest value of k such that $\eta_1(k) \neq \eta_2(k)$, 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 $\eta_1 \prec_P \eta_2$.

Proposition 6.1.5 *Let $P = \sum_{0 \leq h \leq p} \gamma_h y^h \in \mathbf{K}[y]$ with $\gamma_p \neq 0$ 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 $\theta_1 < \theta_2$.*

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 6.1.4. Note that 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 $\eta_1 \neq \eta_2$.

Next we recall the mixed Taylor formulas, which play a central role in proving the weak inference version of these results.

Proposition 6.1.6 (Mixed Taylor Formulas) *Let $P = y^p + \sum_{0\le h\le p-1} \gamma_h y^h \in \mathbf{K}[y]$. For every $\varepsilon \in \{1,-1\}^{\{1,\dots,p\}}$ with $\varepsilon(1) = 1$, there exist $N_{\varepsilon,1}, \dots, N_{\varepsilon,p} \in \mathbb{N}_*$ such that*

$$P(t_2) = P(t_1) + \sum_{1\le k\le p} \varepsilon(k)\tfrac{N_{\varepsilon,k}}{k!} P^{(k)}(a_k)\cdot(t_2-t_1)^k \qquad (1)$$

where, for $1 \le k \le p-1$, $a_k = t_1$ if $\varepsilon(k) = \varepsilon(k+1)$ and $a_k = t_2$ otherwise.

Note that a_p is not defined in (1), but this is not important since $P^{(p)}$ is a constant. A proof of Proposition 6.1.6 can be found in [40] and also in [55].

We prove now the weak inference version of the main properties of Thom encoding.

Proposition 6.1.7 *Let $p \ge 1$, $P = y^p + \sum_{0\le h\le p-1} C_h \cdot y^h \in \mathbf{K}[u][y]$, η_1, η_2 be sign conditions on $\mathrm{Der}_+(P)$ such that exists q, $0 \le q \le p-1$, with $\eta_1(q) = \eta_2(q) = 0$ and $\eta_1(k) = \eta_2(k) \neq 0$ for $q+1 \le k \le p-1$. Then*

$$\mathrm{sign}(\mathrm{Der}_+(P)(t_1)) = \eta_1,\ \mathrm{sign}(\mathrm{Der}_+(P)(t_2)) = \eta_2 \quad \vdash \quad t_1 = t_2.$$

If we have an initial incompatibility in variables $v \supset (u, t_1, t_2)$ with monoid part S, degree in w bounded by δ_w for some subset of variables $w \subset v$ disjoint from (t_1, t_2), degree in t_1 and degree in t_2 bounded by δ_t, the final incompatibility has monoid part

$$S \cdot P^{(q+1)}(t_1)^2 \cdot P^{(q+1)}(t_2)^2,$$

degree in w bounded by $2\delta_w + 14\deg_w P$ and degree in t_1 and degree in t_2 bounded by $2\delta_t + 14(p-q) - 8$.

In order to prove Proposition 6.1.7, we will prove first an auxiliary lemma.

Lemma 6.1.8 *Let $p \ge 1$, $P = y^p + \sum_{0\le h\le p-1} C_h \cdot y^h \in \mathbf{K}[u][y]$, η_1, η_2 be sign conditions on $\mathrm{Der}_+(P)$ such that exists q, $0 \le q \le p-1$, with $\eta_1(q) = \eta_2(q) = 0$ and $\eta_1(k) = \eta_2(k) \neq 0$ for $q+1 \le k \le p-1$. Then*

$$\mathrm{sign}(\mathrm{Der}_+(P)(t_1)) = \eta_1,\ \mathrm{sign}(\mathrm{Der}_+(P)(t_2)) = \eta_2 \quad \vdash \quad t_1 \le t_2.$$

If we have an initial incompatibility in variables $v \supset (u, t_1, t_2)$ with monoid part S, degree in w bounded by δ_w for some subset of variables $w \subset v$ disjoint from (t_1, t_2), degree in t_1 and degree in t_2 bounded by δ_t, the final incompatibility has monoid part

$$S \cdot P^{(q+1)}(a_1)^2$$

where $a_1 = t_1$ if $q < p-1$ and $\eta_1(q+1)\eta_1(q+2) = -1$ and $a = t_2$ otherwise, degree in w bounded by $\delta_w + 7\deg_w P$, and degree in t_1 and degree in t_2 bounded by $\delta_t + 7(p-q) - 4$.

Proof. Consider the initial incompatibility

$$\downarrow t_1 \leq t_2,\ \mathcal{H} \downarrow \tag{2}$$

where $\mathcal{H}$ is a system of sign conditions in $\mathbf{K}[v]$. For $q \leq k \leq p$ we denote $\eta(k) = \eta_1(k) = \eta_2(k)$. If $\eta(q+1) = -1$, we change P by $-P$, η_1 by $-\eta_1$ and η_2 by $-\eta_2$; so without loss of generality we suppose $\eta(q+1) = 1$.

The mixed Taylor formula (Proposition 6.1.6) for $P^{(q)}$ and $\varepsilon = [\eta(q+1), -\eta(q+2)\ \ldots, (-1)^{p-q-1}\eta(p)]$ provides us the identity

$$P^{(q)}(t_2) - P^{(q)}(t_1) \quad = \quad (t_2 - t_1) \cdot S_o - S_e \tag{3}$$

where

$$\begin{aligned} S_o &= N_{\varepsilon,1} P^{(q+1)}(a_1) + \textstyle\sum_{\substack{3 \leq k \leq p-q, \\ k \text{ odd}}} \frac{N_{\varepsilon,k}}{k!} \eta(q+k) P^{(q+k)}(a_k) \cdot (t_2 - t_1)^{k-1}, \\ S_e &= \textstyle\sum_{\substack{2 \leq k \leq p-q, \\ k \text{ even}}} \frac{N_{\varepsilon,k}}{k!} \eta(q+k) P^{(q+k)}(a_k) \cdot (t_2 - t_1)^{k}. \end{aligned}$$

We successively apply to (2) the weak inferences

$$\begin{aligned} (t_2 - t_1) \cdot S_o \geq 0,\ S_o > 0 \quad &\vdash \quad t_1 \leq t_2, \\ (t_2 - t_1) \cdot S_o - S_e = 0,\ S_e \geq 0 \quad &\vdash \quad (t_2 - t_1) \cdot S_o \geq 0, \\ P^{(q)}(t_1) = 0,\ P^{(q)}(t_2) = 0 \quad &\vdash \quad (t_2 - t_1) \cdot S_o - S_e = 0. \end{aligned}$$

By Lemmas 2.1.9 and 2.1.5 (items 14 and 15) using (3), we obtain

$$\Big\downarrow\ S_o > 0,\ S_e \geq 0,\ P^{(q)}(t_1) = 0,\ P^{(q)}(t_2) = 0,\ \mathcal{H}\ \Big\downarrow \tag{4}$$

with monoid part $S \cdot S_o^2$, degree in w bounded by $\delta_w + 4 \deg_w P$ and degree in t_1 and degree in t_2 bounded by $\delta_t + 4(p-q) - 2$.

Then we successively apply to (4) the weak inferences

$$\begin{aligned} P^{(q+1)}(a_1) > 0,\ \bigwedge_{\substack{3 \leq k \leq p-q, \\ k \text{ odd}}} \eta(q+k) P^{(q+k)}(a_k) \cdot (t_2 - t_1)^{k-1} \geq 0 \quad &\vdash \quad S_o > 0, \\ \bigwedge_{\substack{2 \leq k \leq p-q, \\ k \text{ even}}} \eta(q+k) P^{(q+k)}(a_k) \cdot (t_2 - t_1)^{k} \geq 0 \quad &\vdash \quad S_e \geq 0. \end{aligned}$$

By Lemmas 2.1.7 and 2.1.5 (item 15) we obtain an incompatibility

$$\begin{aligned} &\Big\downarrow\ P^{(q+1)}(a_1) > 0,\ \bigwedge_{\substack{3 \leq k \leq p-q, \\ k \text{ odd}}} \eta(q+k) P^{(q+k)}(a_k) \cdot (t_2 - t_1)^{k-1} \geq 0, \\ &\bigwedge_{\substack{2 \leq k \leq p-q, \\ k \text{ even}}} \eta(q+k) P^{(q+k)}(a_k) \cdot (t_2 - t_1)^{k} \geq 0,\ P^{(q)}(t_1) = 0,\ P^{(q)}(t_2) = 0,\ \mathcal{H}\ \Big\downarrow \end{aligned} \tag{5}$$

with monoid part $S \cdot P^{(q+1)}(a_1)^2$, degree in w bounded by $\delta_w + 7 \deg_w P$ and degree in t_1 and degree in t_2 bounded by $\delta_t + 7(p-q) - 4$.

Then we successively apply to (5) for odd k, $3 \le k \le p-q$, the weak inferences

$$\begin{array}{rcl} \eta(q+k)P^{(q+k)}(a_k) \ge 0,\ (t_2-t_1)^{k-1} \ge 0 & \vdash & \eta(q+k)P^{(q+k)}(a_k)\cdot(t_2-t_1)^{k-1} \ge 0, \\ \operatorname{sign}(P^{(q+k)}(a_k)) = \eta(q+k) & \vdash & \eta(q+k)P^{(q+k)}(a_k) \ge 0, \\ & \vdash & (t_2-t_1)^{k-1} \ge 0, \end{array}$$

and for even k, $2 \le k \le p-q$, the weak inference

$$\begin{array}{rcl} \eta(q+k)P^{(q+k)}(a_k) \ge 0,\ (t_2-t_1)^{k} \ge 0 & \vdash & \eta(q+k)P^{(q+k)}(a_k)\cdot(t_2-t_1)^{k} \ge 0, \\ \operatorname{sign}(P^{(q+k)}(a_k)) = \eta(q+k) & \vdash & \eta(q+k)P^{(q+k)}(a_k) \ge 0, \\ & \vdash & (t_2-t_1)^{k} \ge 0. \end{array}$$

By Lemma 2.1.2 (items 1, 3 and 7) we obtain

$$\downarrow \operatorname{sign}(\operatorname{Der}_+(P)(t_1)) = \eta_1,\ \operatorname{sign}(\operatorname{Der}_+(P)(t_2)) = \eta_2,\ \mathcal{H} \downarrow$$

with the same monoid part and degree bounds. □

We can prove now Proposition 6.1.7.

Proof of Proposition 6.1.7. Consider the initial incompatibility

$$\downarrow t_1 = t_2,\ \mathcal{H} \downarrow \tag{6}$$

where $\mathcal{H}$ is a system of sign conditions in $\mathbf{K}[v]$.

We successively apply to (6) the weak inferences

$$\begin{array}{rcl} t_1 \ge t_2,\ t_1 \le t_2 & \vdash & t_1 = t_2, \\ \operatorname{sign}(\operatorname{Der}_+(P)(t_1)) = \eta_1,\ \operatorname{sign}(\operatorname{Der}_+(P)(t_2)) = \eta_2 & \vdash & t_1 \le t_2, \\ \operatorname{sign}(\operatorname{Der}_+(P)(t_2)) = \eta_2,\ \operatorname{sign}(\operatorname{Der}_+(P)(t_1)) = \eta_1 & \vdash & t_2 \le t_1. \end{array}$$

By Lemmas 2.1.4 and 6.1.8, we obtain

$$\downarrow \operatorname{sign}(\operatorname{Der}_+(P)(t_1)) = \eta_1,\ \operatorname{sign}(\operatorname{Der}_+(P)(t_2)) = \eta_2,\ \mathcal{H} \downarrow$$

with monoid part $S\cdot P^{(q+1)}(t_1)^2\cdot P^{(q+1)}(t_2)^2$, degree in w bounded by $2\delta_w + 14\deg_w P$ and degree in t_1 and degree in t_2 bounded by $2\delta_t + 14(p-q) - 8$, which serves as the final incompatibility. □

Proposition 6.1.9 *Let* $p \ge 1, P = y^p + \sum_{0\le h\le p-1} C_h\cdot y^h \in \mathbf{K}[u][y]$, η_1, η_2 *be sign conditions on* $\operatorname{Der}_+(P)$ *such that exists* q, $0 \le q \le p-1$, *with* $\eta_1(q) \ne \eta_2(q)$ *and* $\eta_1(k) = \eta_2(k) \ne 0$ *for* $q+1 \le k \le p-1$, *and* $\eta_1 \prec_P \eta_2$. *Then*

$$\operatorname{sign}(\operatorname{Der}_+(P)(t_1)) = \eta_1,\ \operatorname{sign}(\operatorname{Der}_+(P)(t_2)) = \eta_2 \quad \vdash \quad t_1 < t_2.$$

If we have an initial incompatibility in variables $v \supset (u, t_1, t_2)$ with monoid part $S \cdot (t_2 - t_1)^{2e}$ with $e \geq 1$, degree in w bounded by δ_w for some subset of variables $w \subset v$ disjoint from (t_1, t_2), degree in t_1 and degree in t_2 bounded by δ_t, the final incompatibility has monoid part

$$S \cdot P^{(q)}(b)^{2e}$$

with $b = t_2$ if $\eta_2(q) \neq 0$ and $b = t_1$ otherwise, degree in w bounded by $\delta_w + (6e+2)\deg_w P$ and degree in t_1 and degree in t_2 bounded by $\delta_t + (6e+2)p$.

Proof. The proof is an adaptation of the proof of Lemma 6.1.8. For $q+1 \leq k \leq p$ we denote $\eta(k) = \eta_1(k) = \eta_2(k)$. If $\eta(q+1) = -1$, we change P by $-P$, η_1 by $-\eta_1$ and η_2 by $-\eta_2$; so without loss of generality we suppose $\eta(q+1) = 1$. We replace the first three weak inferences in the proof of Lemma 6.1.8 by

$$\begin{array}{rcl} (t_2 - t_1)S_o > 0,\ S_o > 0 & \vdash & t_1 < t_2, \\ (t_2 - t_1)S_o - S_e > 0,\ S_e \geq 0 & \vdash & (t_2 - t_1)S_o > 0, \\ \operatorname{sign}(P^{(q)}(t_1)) = \eta_1(q),\ \operatorname{sign}(P^{(q)}(t_2)) = \eta_2(q) & \vdash & (t_2 - t_1)S_o - S_e > 0. \end{array}$$

In fact, just for the case $\eta_1(q) = -1$ and $\eta_2(q) = 1$, also the weak inference

$$P^{(q)}(t_1) < 0 \quad \vdash \quad P^{(q)}(t_1) \leq 0$$

from Lemma 2.1.2 (item 1) is also needed between the second and third weak inference above. By Lemmas 2.1.10, 2.1.7 and possibly 2.1.2 (item 1), we obtain

$$\downarrow S_o > 0,\ S_e \geq 0,\ \operatorname{sign}(P^{(q)}(t_1)) = \eta_1(q),\ \operatorname{sign}(P^{(q)}(t_2)) = \eta_2(q),\ \mathcal{H} \downarrow$$

with monoid part $S \cdot P^{(q)}(b)^{2e}$ with $b = t_2$ if $\eta_2(q) = 1$ and $b = t_1$ otherwise, degree in w bounded by $\delta_w + 6e \deg_w P$ and degree in t_1 and degree in t_2 bounded by $\delta_t + 2e(3(p-q)-1)$.

The rest of the proof is as in the proof of Lemma 6.1.8. □

6.2 Conditions on the parameters fixing the Thom encoding

Given $P, Q \in \mathbf{K}[u][y]$, with P monic in y and $u = (u_1, \ldots, u_k)$, our goal is to define a family of polynomials in $\mathbf{K}[u]$ whose signs fix the Thom encoding of the real roots of P and the signs of Q at these roots; the family composed by the principal minors of Hermite matrices of P and products of (a small number of) its derivatives with $1, Q$ or Q^2 has this property by sign determination (see [45, Theorem 27]).

We introduce some notation and definitions.

Notation 6.2.1 *Let $P \in \mathbf{K}[u][y]$ monic in y with $\deg_y P = p \geq 1$.*

For $\eta \in \{-1, 0, 1\}^{\mathrm{Der}(P)}$, we denote by $\eta_+ \in \{-1, 0, 1\}^{\mathrm{Der}_+(P)}$ the extension of η to $\mathrm{Der}_+(P)$ given by $\eta_+(0) = 0$.

For $\eta \in \{-1, 0, 1\}^{\mathrm{Der}_+(P)}$, the number $\mathrm{mu}(\eta, P)$ is the smallest index i, $0 \leq i \leq p$, such that $\eta(i) \neq 0$. Note that if the real root θ of P has Thom encoding η, the multiplicity of θ as a root of P is $\mathrm{mu}(\eta, P)$.

For $\eta \in \{-1,0,1\}^{\mathrm{Der}(P)}$*, the number* $\mathrm{mu}(\eta, P)$ *is* $\mathrm{mu}(\eta_+, P)$*.*

For a list of distinct sign conditions $\boldsymbol{\eta} = [\eta_1, \ldots, \eta_{\#\boldsymbol{\eta}}]$ *on* $\mathrm{Der}(P)$*, the vector* $\mathrm{vmu}(\boldsymbol{\eta})$ *is the list* $\mathrm{mu}(\eta_1, P), \ldots, \mathrm{mu}(\eta_{\#\boldsymbol{\eta}}, P)$ *in non-increasing order.*

We define the order $\prec_P^{\mathrm{mu}}$ *on* $\{-1,0,1\}^{\mathrm{Der}(P)}$*, given by* $\eta_1 \prec_P^{\mathrm{mu}} \eta_2$ *if* $\mathrm{mu}(\eta_1, P) > \mathrm{mu}(\eta_2, P)$ *or* $\mathrm{mu}(\eta_1, P) = \mathrm{mu}(\eta_2, P)$ *and* $\eta_{1,+} \prec_P \eta_{2,+}$*.*

Definition 6.2.2 *Let* $p \geq 1$*,* $P = y^p + \sum_{0 \leq h \leq p-1} C_h \cdot y^h \in \mathbf{K}[u][y]$*,* $(\boldsymbol{\mu}, \boldsymbol{\nu}) \in \Lambda_m \times \Lambda_n$ *with* $m + 2n = p$*,* $\boldsymbol{\eta} = [\eta_1, \ldots, \eta_{\#\boldsymbol{\eta}}]$ *be a list of distinct sign conditions on* $\mathrm{Der}(P)$ *with* $\#\boldsymbol{\mu} = \#\boldsymbol{\eta}$*,* $t = (t_1, \ldots, t_{\#\boldsymbol{\mu}})$ *and* $z = (z_1, \ldots, z_{\#\boldsymbol{\nu}})$*. We define the system of sign conditions*

$$\mathrm{Th}(P)^{\boldsymbol{\mu},\boldsymbol{\nu},\boldsymbol{\eta}}(t, z)$$

in $\mathbf{K}[u][t, a, b]$ *as*

$$\mathrm{Fact}(P)^{\boldsymbol{\mu},\boldsymbol{\nu}}(t, z), \quad \bigwedge_{1 \leq j \leq \#\boldsymbol{\mu}} \mathrm{sign}(\mathrm{Der}(P)(t_j)) = \eta_j.$$

Note that in Definition 6.2.2, since the multiplicity of the real roots of P can be read both from $\boldsymbol{\mu}$ and $\boldsymbol{\eta}$, there should be some restrictions on $\boldsymbol{\mu}$ and $\boldsymbol{\eta}$ in order that the system $\mathrm{Th}(P)^{\boldsymbol{\mu},\boldsymbol{\nu},\boldsymbol{\eta}}(t, z)$ admits a real solution. Nevertheless, we will still need the definition in the general case, with the only restriction on $\boldsymbol{\mu}$ and $\boldsymbol{\eta}$ given by $\#\boldsymbol{\mu} = \#\boldsymbol{\eta}$.

Definition 6.2.3 *Let* $p \geq 1$*,* $P = y^p + \sum_{0 \leq h \leq p-1} C_h \cdot y^h \in \mathbf{K}[u][y]$*,* $Q \in \mathbf{K}[u][y]$ *and* $i \in \mathbb{N}$*. We define*

$$\begin{aligned}
\mathrm{PDer}_i(P) &= \Big\{ \prod_{1 \leq h \leq p-1} (P^{(h)})^{\alpha_h} \mid \alpha \in \{0,1,2\}^{\{1,\ldots,p-1\}}, \#\{h \mid \alpha_h \neq 0\} \leq i \Big\} \subset \mathbf{K}[u][y], \\
\mathrm{PDer}_i(P; Q) &= \{AB \mid A \in \mathrm{PDer}_i(P), \, B \in \{Q, Q^2\}\} \subset \mathbf{K}[u][y], \\
\mathrm{ThElim}(P) &= \bigcup_{A \in \mathrm{PDer}_{\mathrm{bit}\{p\}}(P)} \mathrm{HMi}(P; A) \subset \mathbf{K}[u], \\
\mathrm{ThElim}(P; Q) &= \bigcup_{A \in \mathrm{PDer}_{\mathrm{bit}\{p\}-1}(P;Q)} \mathrm{HMi}(P; A) \subset \mathbf{K}[u].
\end{aligned}$$

The following two results show the connection between signs conditions on the sets $\mathrm{ThElim}(P)$ and $\mathrm{ThElim}(P; Q)$ and the Thom encodings of the real roots of P and the sign of Q at these roots.

Theorem 6.2.4 (Fixing the Thom encodings) *Let* $p \geq 1$*,* $P = y^p + \sum_{0 \leq h \leq p-1} C_h \cdot y^h \in \mathbf{K}[u][y]$*. For every realizable sign condition* τ *on* $\mathrm{ThElim}(P)$*, there exist unique* $(\boldsymbol{\mu}(\tau), \boldsymbol{\nu}(\tau)) \in \Lambda_m \times \Lambda_n$ *with* $m + 2n = p$*, and a unique list* $\boldsymbol{\eta}(\tau)$ *of distinct sign conditions on* $\mathrm{Der}(P)$ *ordered with respect to* $\prec_P^{\mathrm{mu}}$ *such that for every* $\vartheta \in \mathrm{Real}(\tau, \mathbf{R})$ *there exist* $\theta \in \mathbf{R}^{\#\boldsymbol{\mu}(\tau)}, \alpha \in \mathbf{R}^{\#\boldsymbol{\nu}(\tau)}, \beta \in \mathbf{R}^{\#\boldsymbol{\nu}(\tau)}$ *such that*

$$\mathrm{Th}(P(\vartheta))^{\boldsymbol{\mu}(\tau),\boldsymbol{\nu}(\tau),\boldsymbol{\eta}(\tau)}(\theta, \alpha + i\beta).$$

Proof. As said in Theorem 5.2.2 (Hermite's Theory (2)), a sign condition τ on $\mathrm{ThElim}(P)$ determines the rank and signature of $\mathrm{Her}(P; A)$ for every $A \in \mathrm{PDer}_{\mathrm{bit}\{p\}}(P)$. By sign determination [45, Theorem 27], this is enough to determine the decomposition of P into ireducible real factors and the Thom encodings of the real roots of P. □

Theorem 6.2.5 (Fixing the Thom encodings with a Sign) *Following the notation of Theorem 6.2.4, for every realizable sign condition* (τ, τ') *on* $\mathrm{ThElim}(P) \cup \mathrm{ThElim}(P; Q)$, *there exists a unique list* $\boldsymbol{\epsilon}(\tau, \tau') = [\epsilon_1(\tau, \tau'), \ldots, \epsilon_{\#\boldsymbol{\mu}(\tau)}(\tau, \tau')]$ *of signs such that for every* $\vartheta \in \mathrm{Real}((\tau, \tau'), \mathbf{R})$ *there exist* $\theta \in \mathbf{R}^{\#\boldsymbol{\mu}(\tau)}, \alpha \in \mathbf{R}^{\#\boldsymbol{\nu}(\tau)}, \beta \in \mathbf{R}^{\#\boldsymbol{\nu}(\tau)}$ *such that*

$$\mathrm{Th}(P(\vartheta))^{\boldsymbol{\mu}(\tau), \boldsymbol{\nu}(\tau), \boldsymbol{\eta}(\tau)}(\theta, \alpha + i\beta), \quad \bigwedge_{1 \le j \le \#\boldsymbol{\mu}(\tau)} \mathrm{sign}(Q(\theta_j)) = \epsilon_j(\tau, \tau').$$

Proof : The claim follows using Theorem 6.2.4 and the fact that a sign condition τ' on $\mathrm{ThElim}(P; Q)$ additionally determines the rank and signature of $\mathrm{Her}(P; A)$ for every $A \in \mathrm{PDer}_{\mathrm{bit}\{p\}-1}(P; Q)$, and therefore, by sign determination [45, Theorem 27], the signs of Q at the real roots of P. □

Before giving the weak inference versions of Theorems 6.2.4 and 6.2.5, we define new auxiliary functions (see Definitions 4.3.3 and 5.4.2).

Definition 6.2.6 *1. Let* $\mathrm{g}_{H,1} : \mathbb{N}_* \to \mathbb{N}$, $\mathrm{g}_{H,1}\{p\} = \mathrm{g}_H\{p, 2\mathrm{bit}\{p\}(p-1)\}$.

2. *Let* $\tilde{\mathrm{g}}_{H,1} : \mathbb{N}_* \to \mathbb{N}$, $\tilde{\mathrm{g}}_{H,1}\{p\} = \mathrm{bit}\{p\} 2^{2^{\frac{1}{2}(p-1)p+2}-2} \mathrm{g}_{H,1}\{p\}^{2^{\frac{1}{2}(p-1)p}-1} (\mathrm{g}_{H,1}\{p\} + 2)$.
3. *Let* $\mathrm{g}_{H,2} : \mathbb{N}_* \times \mathbb{N} \to \mathbb{N}$, $\mathrm{g}_{H,2}\{p, q\} = \mathrm{g}_H\{p, 2(\mathrm{bit}\{p\} - 1)(p-1) + 2q\}$.
4. *Let* $\tilde{\mathrm{g}}_{H,2} : \mathbb{N}_* \times \mathbb{N} \to \mathbb{R}$, $\tilde{\mathrm{g}}_{H,2}\{p, q\} = \mathrm{bit}\{p\} 2^{2^{\frac{1}{2}p^2+2}-2} \mathrm{g}_{H,2}\{p, q\}^{2^{\frac{1}{2}p^2}-1} (\mathrm{g}_{H,2}\{p, q\} + 2)$.
5. *Let* $\mathrm{g}_5 : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{R}$,

$$\mathrm{g}_5\{p, e, f, g, e'\} = \mathrm{g}_4\{p\} \max\{e', \tilde{\mathrm{g}}_{H,1}\{p\}\}^{2^{\frac{3}{2}p^2}} \max\{e, g, \tilde{\mathrm{g}}_{H,1}\{p\}\}^{2^{\frac{1}{2}p^2}} \max\{f, \tilde{\mathrm{g}}_{H,1}\{p\}\}^{2^{\frac{1}{2}p}}.$$

Technical Lemma 6.2.7 *For every* $(p, e, f, g, e') \in \mathbb{N}_* \times \mathbb{N} \times \mathbb{N} \times \mathbb{N} \times \mathbb{N}$,

$$2^{p+(((p-1)p+2)2^{(p-1)p}-2)(2^{\frac{1}{2}p^2}+2^{\frac{1}{2}p}+1)} \mathrm{g}_4\{p\} \max\{e', \tilde{\mathrm{g}}_{H,1}\{p\}\}^{(2^{(p-1)p}-1)(2^{\frac{1}{2}p^2}+2^{\frac{1}{2}p}+1)+1} \cdot$$
$$\cdot \max\{e, g, \tilde{\mathrm{g}}_{H,1}\{p\}\}^{2^{\frac{1}{2}p^2}} \max\{f, \tilde{\mathrm{g}}_{H,1}\{p\}\}^{2^{\frac{1}{2}p}} \le$$
$$\le \mathrm{g}_5\{p, e, f, g, e'\}.$$

Proof. See Section 8. □

Now, we first give weak inference versions of Theorems 6.2.4 and 6.2.5, and then the proofs of them.

Theorem 6.2.8 (Fixing the Thom encodings as a weak existence) *Let* $p \ge 1$, $P = y^p + \sum_{0 \le h \le p-1} C_h \cdot y^h \in \mathbf{K}[u][y]$ *and* τ *be a realizable sign condition on* $\mathrm{ThElim}(P)$. *Then, using the notation of Theorem 6.2.4,*

$$\mathrm{sign}(\mathrm{ThElim}(P)) = \tau \quad \vdash \quad \exists (t, z) \ [\ \mathrm{Th}(P)^{\boldsymbol{\mu}(\tau), \boldsymbol{\nu}(\tau), \boldsymbol{\eta}(\tau)}(t, z)\ ]$$

where $t = (t_1, \ldots, t_{\#\boldsymbol{\mu}(\tau)})$ *and* $z = (z_1, \ldots, z_{\#\boldsymbol{\nu}(\tau)})$.

Suppose we have an initial incompatibility in $\mathbf{K}[v][t,a,b]$*, where* $v \supset u$*, and* t,a,b *are disjoint from* v*, with monoid part*

$$S \cdot \prod_{1 \le j < j' \le \#\boldsymbol{\mu}(\tau)} (t_j - t_{j'})^{2e_{j,j'}} \cdot \prod_{1 \le k \le \#\boldsymbol{\nu}(\tau)} b_k^{2f_k} \cdot$$

$$\cdot \prod_{1 \le k < k' \le \#\boldsymbol{\nu}(\tau)} \mathrm{R}(z_k, z_{k'})^{2g_{k,k'}} \cdot \prod_{\substack{1 \le j \le \#\boldsymbol{\mu}(\tau),\, 1 \le h \le p-1, \\ \eta_j(\tau)(h) \neq 0}} P^{(h)}(t_j)^{2e'_{j,h}}$$

with $e_{j,j'} \le e$*,* $f_k \le f$*,* $g_{k,k'} \le g$*,* $e'_{j,h} \le e'$*, degree in* w *bounded by* δ_w *for some subset of variables* $w \subset v$*, degree in* t_j *bounded by* δ_t *and degree in* (a_k, b_k) *bounded by* δ_z*. Then the final incompatibility has monoid part*

$$S^h \cdot \prod_{\substack{H \in \mathrm{ThElim}(P), \\ \tau(H) \neq 0}} H^{2h'_H}$$

with $h, h'_H \le \mathrm{g}_5\{p,e,f,g,e'\}$*, and degree in* w *bounded by*

$$\mathrm{g}_5\{p,e,f,g,e'\}\Big(\max\{\delta_w, \tilde{\mathrm{g}}_{H,1}\{p\}\deg_w P\} + \max\{\delta_t, \delta_z, \tilde{\mathrm{g}}_{H,1}\{p\}\}\deg_w P\Big).$$

Theorem 6.2.9 (Fixing the Thom encodings with a Sign as a weak existence) *Let* $p \ge 1$*,* $P = y^p + \sum_{0 \le h \le p-1} C_h \cdot y^h \in \mathbf{K}[u][y]$*,* $Q \in \mathbf{K}[u][y]$ *with* $\deg_y Q = q$ *and* τ *and* τ' *be sign conditions on* $\mathrm{ThElim}(P)$ *and* $\mathrm{ThElim}(P;Q)$ *respectively such that* (τ, τ') *is a realizable sign condition on* $\mathrm{ThElim}(P) \cup \mathrm{ThElim}(P;Q)$*. Then using the notation of Theorem 6.2.5,*

$$\mathrm{sign}(\mathrm{ThElim}(P;Q)) = \tau',\ \mathrm{Th}(P)^{\boldsymbol{\mu}(\tau), \boldsymbol{\nu}(\tau), \boldsymbol{\eta}(\tau)}(t,z) \quad \vdash \quad \bigwedge_{1 \le j \le \#\boldsymbol{\mu}(\tau)} \mathrm{sign}(Q(t_j)) = \epsilon_j(\tau, \tau')$$

where $t = (t_1, \ldots, t_{\#\boldsymbol{\mu}(\tau)})$ *and* $z = (z_1, \ldots, z_{\#\boldsymbol{\nu}(\tau)})$*.*

Suppose we have an initial incompatibility in $\mathbf{K}[v]$*, where* $v \supset (u,t,a,b)$*, with monoid part*

$$S \cdot \prod_{\substack{1 \le j \le \#\boldsymbol{\mu}(\tau), \\ \epsilon_j(\tau,\tau') \neq 0}} Q(t_j)^{2h_j},$$

with $h_j \le h$*, degree in* w *bounded by* δ_w *for some subset of variables* $w \subset v$ *disjoint from* (t,a,b)*, degree in* t_j *bounded by* δ_t *and degree in* (a_k, b_k) *bounded by* δ_z*. Then, the final incompatibility has monoid part*

$$S^{h'} \cdot \prod_{\substack{H \in \mathrm{ThElim}(P;Q), \\ \tau'(H) \neq 0}} H^{2h'_H} \cdot \prod_{1 \le j < j' \le \#\boldsymbol{\mu}(\tau)} (t_j - t_{j'})^{2e_{j,j'}} \cdot \prod_{1 \le k \le \#\boldsymbol{\nu}(\tau)} b_k^{2f_k} \cdot$$

$$\cdot \prod_{1 \le k < k' \le \#\boldsymbol{\nu}(\tau)} \mathrm{R}(z_k, z_{k'})^{2g_{k,k'}} \cdot \prod_{\substack{1 \le j \le \#\boldsymbol{\mu}(\tau), 1 \le h \le p-1, \\ \eta_j(\tau)(h) \neq 0}} P^{(h)}(t_j)^{2e'_{h,j}}$$

with $h' \le 2^{(p+2)2^p - 2p - 2}\max\{h, \tilde{\mathrm{g}}_{H,2}\{p,q\}\}^{2^p - 1}$*,* $h'_H, e_{j,j'}, f_k, g_{k,k'}, \le 2^{(p+2)2^p - 2}\max\{h, \tilde{\mathrm{g}}_{H,2}\{p,q\}\}^{2^p - 1}\tilde{\mathrm{g}}_{H,2}\{p,q\}$*, degree in* w *bounded by*

$$2^{(p+2)2^p - 2}\max\{h, \tilde{\mathrm{g}}_{H,2}\{p,q\}\}^{2^p - 1}\max\{\delta_w, \tilde{\mathrm{g}}_{H,2}\{p,q\}\max\{\deg_w P, \deg_w Q\}\},$$

degree in t_j bounded by

$$2^{(p+2)2^p-2}\max\{h,\tilde{g}_{H,2}\{p,q\}\}^{2^p-1}\max\{\delta_t,\tilde{g}_{H,2}\{p,q\}\}$$

and degree in (a_k,b_k) bounded by

$$2^{(p+2)2^p-2}\max\{h,\tilde{g}_{H,2}\{p,q\}\}^{2^p-1}\max\{\delta_z,\tilde{g}_{H,2}\{p,q\}\}.$$

Proof of Theorem 6.2.8. Consider the initial incompatibility

$$\downarrow \mathrm{Th}(P)^{\boldsymbol{\mu}(\tau),\boldsymbol{\nu}(\tau),\boldsymbol{\eta}(\tau)}(t,z),\ \mathcal{H} \downarrow_{\mathbf{K}[v][t,a,b]} \tag{7}$$

where $\mathcal{H}$ is a system of sign conditions in $\mathbf{K}[v]$.

In order to proceed by case by case reasoning, our first aim is to obtain incompatibilities

$$\downarrow \mathrm{sign}(\mathrm{ThElim}(P))=\tau,\ \mathrm{Th}(P)^{\boldsymbol{\mu}(\tau),\boldsymbol{\nu}(\tau),\boldsymbol{\eta}},\ \mathcal{H} \downarrow_{\mathbf{K}[v][t,a,b]}$$

for every list of sign condition $\boldsymbol{\eta}=[\eta_1,\dots,\eta_{\#\boldsymbol{\mu}(\tau)}]$ on $\mathrm{Der}(P)$, including those $\boldsymbol{\eta}$ such that the system $\mathrm{Th}(P)^{\boldsymbol{\mu}(\tau),\boldsymbol{\nu}(\tau),\boldsymbol{\eta}}(t,z)$ has obviously no solution because of some real root of P having two different multiplicities according to $\boldsymbol{\mu}(\tau)$ and $\boldsymbol{\eta}$.

We consider first the case that $\boldsymbol{\eta}$ can be obtained from $\boldsymbol{\eta}(\tau)$ through permutations of elements corresponding to real roots with the same multiplicity. In this case, by simply renaming variables within the set of variables t in (7), we obtain

$$\downarrow \mathrm{Th}(P)^{\boldsymbol{\mu}(\tau),\boldsymbol{\nu}(\tau),\boldsymbol{\eta}}(t,z),\ \mathcal{H} \downarrow_{\mathbf{K}[v][t,a,b]} \tag{8}$$

with the same monoid part up to permutations within t and the same degree bounds.

We consider now the case that $\boldsymbol{\eta}$ cannot be obtained from $\boldsymbol{\eta}(\tau)$ through permutations as above. Let $\boldsymbol{\kappa}=[\kappa_1,\dots,\kappa_{\#\boldsymbol{\nu}(\tau)}]$ be a list of invertibility conditions on $\mathrm{Der}(P)$. By Theorem 6.2.4 (Fixing the Thom encodings) there exists $\alpha\in\{0,1,2\}^{1,\dots,p-1}$ with $\#\{h \mid \alpha_h\neq 0\}\leq \mathrm{bit}\{p\}$ such that $Q=\prod_{1\leq h\leq p-1}(P^{(h)})^{\alpha_h}\in \mathrm{PDer}_{\mathrm{bit}\{p\}}(P)$ verifies

$$(\mathrm{Rk}_{\mathrm{HMi}}(\tau),\mathrm{Si}_{\mathrm{HMi}}(\tau))\neq(\mathrm{Rk}_{\mathrm{Fact}}(\boldsymbol{\eta}^\alpha,\boldsymbol{\kappa}^\alpha),\mathrm{Si}_{\mathrm{Fact}}(\boldsymbol{\eta}^\alpha)),$$

where $\boldsymbol{\eta}^\alpha$ is the list of sign conditions satisfied by Q on t when $\boldsymbol{\eta}$ is the list of sign conditions satisfied by $\mathrm{Der}(P)$ on t and $\boldsymbol{\kappa}^\alpha$ is defined analogously. By Theorem 5.4.3 (Hermite's Theory as an incompatibility) there is an incompatibility

$$\begin{array}{c}\downarrow \mathrm{sign}(\mathrm{ThElim}(P))=\tau,\ \mathrm{Fact}(P)^{\boldsymbol{\mu}(\tau),\boldsymbol{\nu}(\tau)}(t,z),\\ \bigwedge_{1\leq j\leq\#\boldsymbol{\mu}(\tau)}\mathrm{sign}(Q(t_j))=\eta_j^\alpha,\quad \bigwedge_{1\leq k\leq\#\boldsymbol{\nu}(\tau)}\mathrm{inv}(Q(z_k))=\kappa_k^\alpha \downarrow_{\mathbf{K}[u][t,a,b]}\end{array} \tag{9}$$

with monoid part

$$\prod_{\substack{H\in\mathrm{HMi}(P;Q),\\ \tau(H)\neq 0}} H^{2\tilde{g}_H}\cdot\prod_{1\leq j<j'\leq\#\boldsymbol{\mu}(\tau)}(t_j-t_{j'})^{2\tilde{e}_{j,j'}}\cdot\prod_{1\leq k\leq\#\boldsymbol{\nu}(\tau)} b_k^{2\tilde{f}_k}.$$

$$\cdot \prod_{1\le k<k'\le \#\boldsymbol{\nu}(\tau)} \mathrm{R}(z_k,z_{k'})^{2\tilde g_{k,k'}} \cdot \prod_{\substack{1\le j\le \#\boldsymbol{\mu}(\tau),\\ \eta_j^{\alpha}\neq 0}} Q(t_j)^{2\tilde e'_j} \prod_{\substack{1\le k\le \#\boldsymbol{\nu}(\tau),\\ \kappa_k^{\alpha}\neq 0}} (Q^2_{\mathrm{Re}}(z_k)+Q^2_{\mathrm{Im}}(z_k))^{2\tilde f'_k}$$

with $\tilde g_H, \tilde e_{j,j'}, \tilde f_k, \tilde g_{k,k'}, \tilde e'_j, \tilde f'_k \le \mathrm{g}_{H,1}\{p\}$, degree in w bounded by $2\mathrm{bit}\{p\}\mathrm{g}_{H,1}\{p\}\deg_w P$ and degree in t_j and degree in (a_k,b_k) bounded by $\mathrm{g}_{H,1}\{p\}$.

Since the sign and invertibility of a product is determined by the sign and invertibility of each factor, by applying to (9) the weak inferences in Lemmas 2.1.2 (items 5, 6 and 8) and 2.1.8, we obtain

$$\Big\downarrow\ \mathrm{sign}(\mathrm{ThElim}(P))=\tau,\ \mathrm{Th}(P)^{\boldsymbol{\mu}(\tau),\boldsymbol{\nu}(\tau),\boldsymbol{\eta}}(t,z),\ \bigwedge_{1\le k\le \#\boldsymbol{\nu}(\tau)} \mathrm{inv}(\mathrm{Der}(P)(z_k))=\kappa_k\ \Big\downarrow_{\mathbf{K}[u][t,a,b]} \tag{10}$$

with monoid part

$$\prod_{\substack{H\in \mathrm{HMi}(P;Q),\\ \tau(H)\neq 0}} H^{2\tilde g_H} \cdot \prod_{1\le j<j'\le \#\boldsymbol{\mu}(\tau)} (t_j-t_{j'})^{2\tilde e_{j,j'}} \cdot \prod_{1\le k\le \#\boldsymbol{\nu}(\tau)} b_k^{2\tilde f_k} \cdot \prod_{1\le k<k'\le \#\boldsymbol{\nu}(\tau)} \mathrm{R}(z_k,z_{k'})^{2\tilde g_{k,k'}} \cdot$$

$$\cdot \prod_{\substack{1\le j\le \#\boldsymbol{\mu}(\tau),\,1\le h\le p-1,\\ \eta_j^{\alpha}\neq 0}} P^{(h)}(t_j)^{2\alpha_h \tilde e'_j} \cdot \prod_{\substack{1\le k\le \#\boldsymbol{\nu}(\tau),\,1\le h\le p-1,\\ \kappa_k^{\alpha}\neq 0}} (P^{(h)}_{\mathrm{Re}}(z_k)^2+P^{(h)}_{\mathrm{Im}}(z_k)^2)^{2\alpha_h \tilde f'_k},$$

degree in w bounded by $2\mathrm{bit}\{p\}(\mathrm{g}_{H,1}\{p\}+1)\deg_w P$, and degree in t_j and degree in (a_k,b_k) bounded by $\mathrm{g}_{H,1}\{p\}$. Note that Lemma 2.1.8 is used for the weak inference saying that, for $1\le k\le \#\boldsymbol{\nu}(\tau)$, $\mathrm{inv}(Q(z_k))=0$ when the invertibility of some factor of Q at z_k is 0.

Then we successively apply to (10) the weak inferences

$$\sum_{\substack{1\le k\le \#\boldsymbol{\nu}(\tau),1\le h\le p-1,\\ \kappa_k(h)=0}} (P^{(h)}_{\mathrm{Re}}(z_k)^2+P^{(h)}_{\mathrm{Im}}(z_k)^2)=0 \quad\vdash\quad \bigwedge_{\substack{1\le k\le \#\boldsymbol{\nu}(\tau),1\le h\le p-1,\\ \kappa_k(h)=0}} P^{(h)}_{\mathrm{Re}}(z_k)=0,\ P^{(h)}_{\mathrm{Im}}(z_k)=0$$

and

$$\bigwedge_{\substack{1\le k\le \#\boldsymbol{\nu}(\tau),1\le h\le p-1,\\ \kappa_k(h)=0}} P^{(h)}_{\mathrm{Re}}(z_k)^2+P^{(h)}_{\mathrm{Im}}(z_k)^2=0 \quad\vdash\quad \sum_{\substack{1\le k\le \#\boldsymbol{\nu}(\tau),1\le h\le p-1,\\ \kappa_k(h)=0}} (P^{(h)}_{\mathrm{Re}}(z_k)^2+P^{(h)}_{\mathrm{Im}}(z_k)^2)=0.$$

By Lemmas 2.1.14 and 2.1.5 (item 14) we obtain

$$\begin{aligned} &\Big\downarrow\ \mathrm{sign}(\mathrm{ThElim}(P))=\tau,\ \mathrm{Th}(P)^{\boldsymbol{\mu}(\tau),\boldsymbol{\nu}(\tau),\boldsymbol{\eta}}(t,z),\\ &\bigwedge_{\substack{1\le k\le \#\boldsymbol{\nu}(\tau),1\le h\le p-1,\\ \kappa_k(h)\neq 0}} P^{(h)}_{\mathrm{Re}}(z_k)^2+P^{(h)}_{\mathrm{Im}}(z_k)^2\neq 0,\\ &\bigwedge_{\substack{1\le k\le \#\boldsymbol{\nu}(\tau),1\le h\le p-1,\\ \kappa_k(h)=0}} P^{(h)}_{\mathrm{Re}}(z_k)^2+P^{(h)}_{\mathrm{Im}}(z_k)^2=0\ \Big\downarrow_{\mathbf{K}[u][t,a,b]} \end{aligned} \tag{11}$$

with monoid part

$$\prod_{\substack{H\in \mathrm{HMi}(P;Q),\\ \tau(H)\neq 0}} H^{4\tilde g_H} \cdot \prod_{1\le j<j'\le \#\boldsymbol{\mu}(\tau)} (t_j-t_{j'})^{4\tilde e_{j,j'}} \cdot \prod_{1\le k\le \#\boldsymbol{\nu}(\tau)} b_k^{4\tilde f_k} \cdot \prod_{1\le k<k'\le \#\boldsymbol{\nu}(\tau)} \mathrm{R}(z_k,z_{k'})^{4\tilde g_{k,k'}} \cdot$$

$$\cdot \prod_{\substack{1\le j\le \#\boldsymbol{\mu}(\tau), 1\le h\le p-1,\\ \eta_j^\alpha \neq 0}} P^{(h)}(t_j)^{4\alpha_h \tilde{e}'_j} \cdot \prod_{\substack{1\le k\le \#\boldsymbol{\nu}(\tau), 1\le h\le p-1,\\ \boldsymbol{\kappa}_k^\alpha \neq 0}} (P^{(h)}_{\mathrm{Re}}(z_k)^2 + P^{(h)}_{\mathrm{Im}}(z_k)^2)^{4\alpha_h \tilde{f}'_k},$$

degree in w bounded by $(4\mathrm{bit}\{p\}(\mathrm{g}_{H,1}\{p\}+1)+2)\deg_w P$, degree in t_j bounded by $2\mathrm{g}_{H,1}\{p\}$ and degree in (a_k, b_k) bounded by $2(\mathrm{g}_{H,1}\{p\}+p-1)$.

Then we fix $\boldsymbol{\eta}$ and we apply to incompatibilities (11) for $\boldsymbol{\eta}$ and every $\boldsymbol{\kappa}$, the weak inference,

$$\vdash \quad \bigvee_{K\in\mathcal{K}} \Big(\bigwedge_{(k,h)\notin K} P^{(h)}_{\mathrm{Re}}(z_k)^2 + P^{(h)}_{\mathrm{Im}}(z_k)^2 \neq 0, \bigwedge_{(k,h)\in K} P^{(h)}_{\mathrm{Re}}(z_k)^2 + P^{(h)}_{\mathrm{Im}}(z_k)^2 = 0 \Big)$$

where

$$\mathcal{K} = \{K \mid K \subset \{1\le k\le \#\boldsymbol{\nu}(\tau)\} \times \{1\le h\le p-1\}\}.$$

By Lemma 2.1.19 we obtain

$$\downarrow \mathrm{sign}(\mathrm{ThElim}(P)) = \tau,\ \mathrm{Th}(P)^{\boldsymbol{\mu}(\tau),\boldsymbol{\nu}(\tau),\boldsymbol{\eta}}(t,z) \downarrow_{\mathbf{K}[u][t,a,b]} \tag{12}$$

with monoid part

$$\prod_{\substack{H\in\mathrm{ThElim}(P),\\ \tau(H)\neq 0}} H^{2\hat{g}_H} \cdot \prod_{1\le j<j'\le \#\boldsymbol{\mu}(\tau)} (t_j - t_{j'})^{2\hat{e}_{j,j'}} \cdot \prod_{1\le k\le \#\boldsymbol{\nu}(\tau)} b_k^{2\hat{f}_k} \cdot$$

$$\cdot \prod_{1\le k<k'\le \#\boldsymbol{\nu}(\tau)} \mathrm{R}(z_k, z_{k'})^{2\hat{g}_{k,k'}} \cdot \prod_{\substack{1\le j\le \#\boldsymbol{\mu}(\tau), 1\le h\le p-1,\\ \eta_j(h)\neq 0}} P^{(h)}(t_j)^{2\hat{e}'_{j,h}}$$

with $\hat{g}_H, \hat{e}_{j,j'}, \hat{f}_k, \hat{g}_{k,k'}, \hat{e}'_{j,h} \le \tilde{\mathrm{g}}_{H,1}\{p\}$, degree in w bounded by $\tilde{\mathrm{g}}_{H,1}\{p\}\deg_w P$ and degree in t_j and degree in (a_k, b_k) bounded by $\tilde{\mathrm{g}}_{H,1}\{p\}$.

Now we have already obtained the necessary incompatibilities for every $\boldsymbol{\eta}$. Then we apply to incompatibilities (8) and (12) the weak inference

$$\vdash \quad \bigvee_{(J,J')\in\mathcal{J}} \Big(\bigwedge_{(j,h)\in J'} P^{(h)}(t_j) > 0, \bigwedge_{(j,h)\notin J\cup J'} P^{(h)}(t_j) < 0, \bigwedge_{(j,h)\in J} P^{(h)}(t_j) = 0 \Big)$$

where

$$\mathcal{J} = \{(J,J') \mid J \subset \{1\le j\le \#\boldsymbol{\mu}(\tau)\}\times\{1\le h\le p-1\}, J' \subset \{1\le j\le \#\boldsymbol{\mu}(\tau)\}\times\{1\le h\le p-1\}\setminus J\}.$$

By Lemma 2.1.21 we obtain

$$\downarrow \mathrm{sign}(\mathrm{ThElim}(P)) = \tau,\ \mathrm{Fact}(P)^{\boldsymbol{\mu}(\tau),\boldsymbol{\nu}(\tau)}(t,z),\ \mathcal{H} \downarrow_{\mathbf{K}[v][t,a,b]} \tag{13}$$

with monoid part

$$S^{\hat{h}'} \cdot \prod_{\substack{H\in\mathrm{ThElim}(P),\\ \tau(H)\neq 0}} H^{2\hat{g}'_H} \cdot \prod_{1\le j<j'\le \#\boldsymbol{\mu}(\tau)} (t_j - t_{j'})^{2\hat{e}'_{j,j'}} \cdot \prod_{1\le k\le \#\boldsymbol{\nu}(\tau)} b_k^{2\hat{f}'_k} \cdot \prod_{1\le k<k'\le \#\boldsymbol{\nu}(\tau)} \mathrm{R}(z_k, z_{k'})^{2\hat{g}'_{k,k'}}$$

with $\hat{h}' \leq f_0'$, $\hat{g}_H' \leq f_0'\tilde{g}_{H,1}\{p\}$, $\hat{e}_{j,j'}' \leq f_0' \max\{e, \tilde{g}_{H,1}\{p\}\}$, $\hat{f}_k' \leq f_0' \max\{f, \tilde{g}_{H,1}\{p\}\}$, $\hat{g}_{k,k'}' \leq f_0' \max\{g, \tilde{g}_{H,1}\{p\}\}$, degree in w bounded by $f_0' \max\{\delta_w, \tilde{g}_{H,1}\{p\} \deg_w P\}$, degree in t_j bounded by $f_0' \max\{\delta_t, \tilde{g}_{H,1}\{p\}\}$ and degree in (a_k, b_k) bounded by $f_0' \max\{\delta_z, \tilde{g}_{H,1}\{p\}\}$, where

$$f_0' = 2^{((p-1)p+2)2^{(p-1)p}-2} \max\{e', \tilde{g}_{H,1}\{p\}\}^{2^{(p-1)p}-1}.$$

We rename variables t and z in (13) as $t_{\boldsymbol{\mu}(\tau)}$ and $z_{\boldsymbol{\nu}(\tau)}$ respectively.

Our next aim is to obtain incompatibilities

$$\downarrow \operatorname{sign}(\operatorname{ThElim}(P)) = \tau,\ \operatorname{Fact}(P)^{\boldsymbol{\mu},\boldsymbol{\nu}}(t_{\boldsymbol{\mu}}, z_{\boldsymbol{\nu}}),\ \mathcal{H} \downarrow_{\mathbf{K}[v][t_{\boldsymbol{\mu}}, a_{\boldsymbol{\nu}}, b_{\boldsymbol{\nu}}]}$$

for every $(\boldsymbol{\mu}, \boldsymbol{\nu}) \in \cup_{m+2n=p} \Lambda_m \times \Lambda_n$, where $t_{\boldsymbol{\mu}} = (t_{\boldsymbol{\mu},1}, \dots, t_{\boldsymbol{\mu},\#\boldsymbol{\mu}})$ and $z_{\boldsymbol{\nu}} = (z_{\boldsymbol{\nu},1}, \dots, z_{\boldsymbol{\nu},\#\boldsymbol{\nu}})$, in order to be able to apply Theorem 4.3.5 (Real Irreducible Factors with Multiplicities as a weak existence). For $(\boldsymbol{\mu}(\tau), \boldsymbol{\nu}(\tau))$, we already have incompatibility (13), so now we suppose $(\boldsymbol{\mu}, \boldsymbol{\nu}) \neq (\boldsymbol{\mu}(\tau), \boldsymbol{\nu}(\tau))$.

By Theorem 6.2.4 (Fixing the Thom encodings) for every $\boldsymbol{\eta}$ list of sign conditions on $\operatorname{Der}(P)$ and $\boldsymbol{\kappa}$ list of invertibility conditions on $\operatorname{Der}(P)$, there exists $\alpha \in \{0, 1, 2\}^{1,\dots,p-1}$ with $\#\{h \mid \alpha_h \neq 0\} \leq \operatorname{bit}\{p\}$ such that $Q = \prod_{1 \leq h \leq p-1} (P^{(h)})^{\alpha_h} \in \operatorname{PDer}_{\operatorname{bit}\{p\}}(P)$ verifies

$$(\operatorname{Rk}_{\operatorname{HMi}}(\tau), \operatorname{Si}_{\operatorname{HMi}}(\tau)) \neq (\operatorname{Rk}_{\operatorname{Fact}}(\boldsymbol{\eta}^\alpha, \boldsymbol{\kappa}^\alpha), \operatorname{Si}_{\operatorname{Fact}}(\boldsymbol{\eta}^\alpha)).$$

Proceeding as before, we obtain

$$\downarrow \operatorname{sign}(\operatorname{ThElim}(P)) = \tau,\ \operatorname{Fact}(P)^{\boldsymbol{\mu},\boldsymbol{\nu}}(t_{\boldsymbol{\mu}}, z_{\boldsymbol{\nu}}) \downarrow_{\mathbf{K}[u][t_{\boldsymbol{\mu}}, a_{\boldsymbol{\nu}}, b_{\boldsymbol{\nu}}]} \tag{14}$$

with monoid part

$$\prod_{\substack{H \in \operatorname{ThElim}(P), \\ \tau(H) \neq 0}} H^{2\hat{g}_H''} \cdot \prod_{1 \leq j < j' \leq m} (t_{\boldsymbol{\mu},j} - t_{\boldsymbol{\mu},j'})^{2\hat{e}_{j,j'}''} \cdot \prod_{1 \leq k \leq n} b_{\boldsymbol{\nu},k}^{2\hat{f}_k''} \cdot \prod_{1 \leq k < k' \leq n} \operatorname{R}(z_k, z_{k'})^{2\hat{g}_{k,k'}''}$$

with $\hat{g}_H'', \hat{e}_{j,j'}'', \hat{f}_k'', \hat{g}_{k,k'}'' \leq f_0'\tilde{g}_{H,1}\{p\}$, degree in w bounded by $f_0'\tilde{g}_{H,1}\{p\} \deg_w P$, and degree in $t_{\boldsymbol{\mu},j}$ and degree in $(a_{\boldsymbol{\nu},k}, b_{\boldsymbol{\nu},k})$ bounded by $f_0'\tilde{g}_{H,1}\{p\}$.

Finally, we apply to incompatibility (13) and incompatibilities (14) for every $(\boldsymbol{\mu}, \boldsymbol{\nu}) \neq (\boldsymbol{\mu}(\tau), \boldsymbol{\nu}(\tau))$ the weak inference

$$\vdash \quad \bigvee_{\substack{m+2n=p \\ (\boldsymbol{\mu},\boldsymbol{\nu}) \in \Lambda_m \times \Lambda_n}} \exists (t_{\boldsymbol{\mu}}, z_{\boldsymbol{\nu}})\ [\ \operatorname{Fact}(P)^{\boldsymbol{\mu},\boldsymbol{\nu}}(t_{\boldsymbol{\mu}}, z_{\boldsymbol{\nu}})\ ].$$

By Theorem 4.3.5 (Real Irreducible Factors with Multiplicities as a weak existence), taking into account that $\# \cup_{m+2n=p} \Lambda_m \times \Lambda_n \leq 2^p$, and using Lemma 6.2.7, we obtain

$$\downarrow \operatorname{sign}(\operatorname{ThElim}(P)) = \tau,\ \mathcal{H} \downarrow_{\mathbf{K}[v]}$$

with monoid part

$$S^h \cdot \prod_{\substack{H \in \operatorname{ThElim}(P), \\ \tau(H) \neq 0}} H^{2h_H'}$$

with

$$\begin{aligned} h &\le \mathrm{g}_4\{p\} f_0'^{2^{2^{\frac{1}{2}p^2}}+2^{2^{\frac{1}{2}p}}+1} \max\{e, g, \tilde{\mathrm{g}}_{H,1}\{p\}\}^{2^{2^{\frac{1}{2}p^2}}} \max\{f, \tilde{\mathrm{g}}_{H,1}\{p\}\}^{2^{2^{\frac{1}{2}p}}} \le \\ &\le \mathrm{g}_5\{p, e, f, g, e'\}, \\ h'_H &\le 2^p \mathrm{g}_4\{p\} \tilde{\mathrm{g}}_{H,1}\{p\} f_0'^{2^{2^{\frac{1}{2}p^2}}+2^{2^{\frac{1}{2}p}}+1} \max\{e, g, \tilde{\mathrm{g}}_{H,1}\{p\}\}^{2^{2^{\frac{1}{2}p^2}}} \max\{f, \tilde{\mathrm{g}}_{H,1}\{p\}\}^{2^{2^{\frac{1}{2}p}}} \le \\ &\le \mathrm{g}_5\{p, e, f, g, e'\}, \end{aligned}$$

and degree in w bounded by

$$\begin{aligned} &\mathrm{g}_4\{p\} f_0'^{2^{2^{\frac{1}{2}p^2}}+2^{2^{\frac{1}{2}p}}+1} \max\{e, g, \tilde{\mathrm{g}}_{H,1}\{p\}\}^{2^{2^{\frac{1}{2}p^2}}} \max\{f, \tilde{\mathrm{g}}_{H,1}\{p\}\}^{2^{2^{\frac{1}{2}p}}} \cdot \\ &\cdot \Big(\max\{\delta_w, \tilde{\mathrm{g}}_{H,1}\{p\} \deg_w P\} + \max\{\delta_t, \delta_z, \tilde{\mathrm{g}}_{H,1}\{p\}\} \deg_w P \Big) \le \\ \le\ & \mathrm{g}_5\{p, e, f, g, e'\} \Big(\max\{\delta_w, \tilde{\mathrm{g}}_{H,1}\{p\} \deg_w P\} + \max\{\delta_t, \delta_z, \tilde{\mathrm{g}}_{H,1}\{p\}\} \deg_w P \Big), \end{aligned}$$

which serves as the final incompatibility. □

Proof of Theorem 6.2.9. We simplify the notation by renaming $\boldsymbol{\mu} = \boldsymbol{\mu}(\tau)$, $\boldsymbol{\nu} = \boldsymbol{\nu}(\tau)$ and $\boldsymbol{\eta} = \boldsymbol{\eta}(\tau)$. Consider the initial incompatibility

$$\downarrow \bigwedge_{1 \le j \le \#\boldsymbol{\mu}} \mathrm{sign}(Q(t_j)) = \epsilon_j(\tau, \tau'),\ \mathcal{H} \downarrow_{\mathbf{K}[v]} \tag{15}$$

where $\mathcal{H}$ is a system of sign conditions in $\mathbf{K}[v]$.

Once again, our aim is to proceed by case by case reasoning. Let $\boldsymbol{\epsilon} = [\epsilon_1, \dots, \epsilon_{\#\boldsymbol{\mu}}]$ be a list of sign conditions on Q with $\boldsymbol{\epsilon} \ne \boldsymbol{\epsilon}(\tau, \tau')$, $\boldsymbol{\kappa} = [\kappa_1, \dots, \kappa_{\#\boldsymbol{\nu}}]$ be a list of invertibility conditions on $\mathrm{Der}(P)$ and $\boldsymbol{\rho} = [\rho_1, \dots, \rho_{\#\boldsymbol{\nu}}]$ be a list of invertibility conditions on Q. By Theorem 6.2.5 (Fixing the Thom encodings with a Sign) there exist $\alpha \in \{0,1,2\}^{1,\dots,p-1}$ with $\#\{h \mid \alpha_h \ne 0\} \le \mathrm{bit}\{p\}-1$ and $\beta \in \{1,2\}$ such that $\tilde{Q} = (\prod_{1 \le h \le p-1} (P^{(h)})^{\alpha_h}) Q^\beta \in \mathrm{PDer}_{\mathrm{bit}\{p\}-1}(P; Q)$ verifies

$$(\mathrm{Rk}_{\mathrm{HMi}}(\tau), \mathrm{Si}_{\mathrm{HMi}}(\tau)) \ne (\mathrm{Rk}_{\mathrm{Fact}}(\boldsymbol{\eta}^\alpha \boldsymbol{\epsilon}^\beta, \boldsymbol{\kappa}^\alpha \boldsymbol{\rho}^\beta), \mathrm{Si}_{\mathrm{Fact}}(\boldsymbol{\eta}^\alpha \boldsymbol{\epsilon}^\beta)),$$

where $\boldsymbol{\eta}^\alpha \boldsymbol{\epsilon}^\beta$ is the list of sign conditions satisfied by $\tilde{Q}$ on t if $\mathrm{Th}(P)^{\boldsymbol{\mu},\boldsymbol{\nu},\boldsymbol{\eta}}(t,z)$ holds and $\boldsymbol{\epsilon}$ is the list of sign conditions satisfied by Q on t and $\boldsymbol{\kappa}^\alpha \boldsymbol{\rho}^\beta$ is defined analogously. By Theorem 5.4.3 (Hermite's Theory as an incompatibility) there is an incompatibility

$$\begin{aligned} &\downarrow \mathrm{sign}(\mathrm{ThElim}(P; Q)) = \tau',\ \mathrm{Fact}(P)^{\boldsymbol{\mu},\boldsymbol{\nu}}(t, z), \\ &\bigwedge_{1 \le j \le \#\boldsymbol{\mu}} \mathrm{sign}(\tilde{Q}(t_j)) = \eta_j^\alpha \epsilon_j^\beta,\ \bigwedge_{1 \le k \le \#\boldsymbol{\nu}} \mathrm{inv}(\tilde{Q}(z_k)) = \kappa_k^\alpha \rho_k^\beta \downarrow_{\mathbf{K}[u][t,a,b]} \end{aligned} \tag{16}$$

with monoid part

$$\prod_{\substack{H \in \mathrm{HMi}(P;\tilde{Q}), \\ \tau'(H) \ne 0}} H^{2\tilde{g}_H} \cdot \prod_{1 \le j < j' \le \#\boldsymbol{\mu}} (t_j - t_{j'})^{2\tilde{e}_{j,j'}} \cdot \prod_{1 \le k \le \#\boldsymbol{\nu}} b_k^{2\tilde{f}_k}.$$

$$\cdot \prod_{1\le k<k'\le \#\boldsymbol{\nu}} \mathrm{R}(z_k, z_{k'})^{2\tilde{g}_{k,k'}} \cdot \prod_{\substack{1\le j\le \#\boldsymbol{\mu},\\ \eta_j^{\alpha}\epsilon_j^{\beta}\neq 0}} \tilde{Q}(t_j)^{2\tilde{e}'_j} \cdot \prod_{\substack{1\le k\le \#\boldsymbol{\nu},\\ \kappa_j^{\alpha}\rho_k^{\beta}\neq 0}} (\tilde{Q}^2_{\mathrm{Re}}(z_k)+\tilde{Q}^2_{\mathrm{Im}}(z_k))^{2\tilde{f}'_k}$$

with $\tilde{g}_H, \tilde{e}_{j,j'}, \tilde{f}_k, \tilde{g}_{k,k'}, \tilde{e}'_j, \tilde{f}'_k \le \mathrm{g}_{H,2}\{p,q\}$, degree in w bounded by $2\mathrm{bit}\{p\}\mathrm{g}_{H,2}\{p,q\}\max\{\deg_w P, \deg_w Q\}$ and degree in t_j and degree in (a_k,b_k) bounded by $\mathrm{g}_{H,2}\{p,q\}$.

Since the sign and invertibility of a product is determined by the sign and invertibility of each factor, by applying to (16) the weak inferences in Lemmas 2.1.2 (items 5, 6 and 8) and 2.1.8 (used as in the proof of Theorem 6.2.8), we obtain

$$\begin{aligned}\Big\downarrow \mathrm{sign}(\mathrm{ThElim}(P;Q))=\tau',\ \mathrm{Th}^{\boldsymbol{\mu},\boldsymbol{\nu},\boldsymbol{\eta}}(t,z),\ \bigwedge_{1\le j\le \#\boldsymbol{\mu}} \mathrm{sign}(Q(t_j))=\epsilon_j,\\ \bigwedge_{1\le k\le \#\boldsymbol{\nu}} \mathrm{inv}(\mathrm{Der}(P)(z_k))=\kappa_k,\ \bigwedge_{1\le k\le \#\boldsymbol{\nu}} \mathrm{inv}(Q(z_k))=\rho_k \Big\downarrow_{\mathbf{K}[u][t,a,b]}\end{aligned} \tag{17}$$

with monoid part

$$\prod_{\substack{H\in \mathrm{HMi}(P;\tilde{Q}),\\ \tau'(H)\neq 0}} H^{2\tilde{g}_H} \cdot \prod_{1\le j<j'\le \#\boldsymbol{\mu}} (t_j-t_{j'})^{2\tilde{e}_{j,j'}} \cdot \prod_{1\le k\le \#\boldsymbol{\nu}} b_k^{2\tilde{f}_k} \cdot \prod_{1\le k<k'\le \#\boldsymbol{\nu}} \mathrm{R}(z_k,z_{k'})^{2\tilde{g}_{k,k'}} \cdot$$

$$\cdot \prod_{\substack{1\le j\le \#\boldsymbol{\mu},\\ \eta_j^{\alpha}\epsilon_j^{\beta}\neq 0}} \Big(\prod_{1\le h\le p-1} P^{(h)}(t_j)^{2\alpha_h \tilde{e}'_j}\Big)\cdot Q(t_j)^{2\beta\tilde{e}'_j}\cdot$$

$$\cdot \prod_{\substack{1\le k\le \#\boldsymbol{\nu},\\ \kappa_k^{\alpha}\rho_k^{\beta}\neq 0}} \Big(\prod_{1\le h\le p-1} (P^{(h)}_{\mathrm{Re}}(z_k)^2+P^{(h)}_{\mathrm{Im}}(z_k)^2)^{2\alpha_h\tilde{f}'_k}\Big)\cdot (Q^2_{\mathrm{Re}}(z_k)+Q^2_{\mathrm{Im}}(z_k))^{2\beta\tilde{f}'_k},$$

degree in w bounded by $2\mathrm{bit}\{p\}(\mathrm{g}_{H,2}\{p,q\}+1)\max\{\deg_w P, \deg_w Q\}$ and degree in t_j and degree in (a_k,b_k) bounded by $\mathrm{g}_{H,2}\{p,q\}$.

Then we successively apply to (17) the weak inferences

$$\sum_{\substack{1\le k\le \#\boldsymbol{\nu}, 1\le h\le p-1,\\ \kappa_k(h)=0}} (P^{(h)}_{\mathrm{Re}}(z_k)^2+P^{(h)}_{\mathrm{Im}}(z_k)^2) + \sum_{\substack{1\le k\le \#\boldsymbol{\nu},\\ \rho_k=0}} (Q^2_{\mathrm{Re}}(z_k)+Q^2_{\mathrm{Im}}(z_k))=0 \quad \vdash$$

$$\vdash \quad \bigwedge_{\substack{1\le k\le \#\boldsymbol{\nu}, 1\le h\le p-1,\\ \kappa_k(h)=0}} (P^{(h)}_{\mathrm{Re}}(z_k)=0,\ P^{(h)}_{\mathrm{Im}}(z_k)=0),\ \bigwedge_{\substack{1\le k\le \#\boldsymbol{\nu},\\ \rho_k=0}} (Q_{\mathrm{Re}}(z_k)=0,\ Q_{\mathrm{Im}}(z_k)=0)$$

and

$$\bigwedge_{\substack{1\le k\le \#\boldsymbol{\nu}, 1\le h\le p-1,\\ \kappa_k(h)=0}} P^{(h)}_{\mathrm{Re}}(z_k)^2+P^{(h)}_{\mathrm{Im}}(z_k)^2=0,\ \bigwedge_{\substack{1\le k\le \#\boldsymbol{\nu},\\ \rho_k=0}} Q^2_{\mathrm{Re}}(z_k)+Q^2_{\mathrm{Im}}(z_k)=0 \quad \vdash$$

$$\vdash \quad \sum_{\substack{1\le k\le \#\boldsymbol{\nu}, 1\le h\le p-1,\\ \kappa_k(h)=0}} (P^{(h)}_{\mathrm{Re}}(z_k)^2+P^{(h)}_{\mathrm{Im}}(z_k)^2) + \sum_{\substack{1\le k\le \#\boldsymbol{\nu},\\ \rho_k=0}} (Q^2_{\mathrm{Re}}(z_k)+Q^2_{\mathrm{Im}}(z_k))=0.$$

By Lemmas 2.1.14 and 2.1.5 (item 14) we obtain

$$\downarrow \operatorname{sign}(\operatorname{ThElim}(P;Q)) = \tau',\ \operatorname{Th}^{\boldsymbol{\mu},\boldsymbol{\nu},\boldsymbol{\eta}}(t,z),\ \bigwedge_{1\le j\le \#\boldsymbol{\mu}} \operatorname{sign}(Q(t_j)) = \epsilon_j,$$
$$\bigwedge_{\substack{1\le k\le \#\boldsymbol{\nu}, 1\le h\le p-1,\\ \kappa_k(h)\neq 0}} P^{(h)}_{\mathrm{Re}}(z_k)^2 + P^{(h)}_{\mathrm{Im}}(z_k)^2 \neq 0,\ \bigwedge_{\substack{1\le k\le \#\boldsymbol{\nu}, 1\le h\le p-1,\\ \kappa_k(h)= 0}} P^{(h)}_{\mathrm{Re}}(z_k)^2 + P^{(h)}_{\mathrm{Im}}(z_k)^2 = 0, \tag{18}$$
$$\bigwedge_{\substack{1\le k\le \#\boldsymbol{\nu},\\ \rho_k\neq 0}} Q^2_{\mathrm{Re}}(z_k) + Q^2_{\mathrm{Im}}(z_k) \neq 0,\ \bigwedge_{\substack{1\le k\le \#\boldsymbol{\nu},\\ \rho_k= 0}} Q^2_{\mathrm{Re}}(z_k) + Q^2_{\mathrm{Im}}(z_k) = 0 \downarrow_{\mathbf{K}[u][t,a,b]}$$

with monoid part

$$\prod_{\substack{H\in \operatorname{HMi}(P;\tilde{Q}),\\ \tau'(H)\neq 0}} H^{4\tilde{g}_H} \cdot \prod_{1\le j<j'\le \#\boldsymbol{\mu}} (t_j - t_{j'})^{4\tilde{e}_{j,j'}} \cdot \prod_{1\le k\le \#\boldsymbol{\nu}} b_k^{4\tilde{f}_k} \cdot \prod_{1\le k<k'\le \#\boldsymbol{\nu}} \mathrm{R}(z_k, z_{k'})^{4\tilde{g}_{k,k'}} \cdot$$
$$\cdot \prod_{\substack{1\le j\le \#\boldsymbol{\mu},\\ \eta_j^{\alpha}\epsilon_j^{\beta}\neq 0}} \Big(\prod_{1\le h\le p-1} P^{(h)}(t_j)^{4\alpha_h \tilde{e}'_j} \Big) \cdot Q(t_j)^{4\beta \tilde{e}'_j} \cdot$$
$$\cdot \prod_{\substack{1\le k\le \#\boldsymbol{\nu},\\ \kappa_k^{\alpha}\rho_k^{\beta}\neq 0}} \Big(\prod_{1\le h\le p-1} (P^{(h)}_{\mathrm{Re}}(z_k)^2 + P^{(h)}_{\mathrm{Im}}(z_k)^2)^{4\alpha_h \tilde{f}'_k} \Big) \cdot (Q^2_{\mathrm{Re}}(z_k) + Q^2_{\mathrm{Im}}(z_k))^{4\beta \tilde{f}'_k},$$

degree in w bounded by $(4\mathrm{bit}\{p\}(\mathrm{g}_{H,2}\{p,q\}+1)+2)\max\{\deg_w P, \deg_w Q\}$, degree in t_j bounded by $2\mathrm{g}_{H,2}\{p,q\}$ and degree in (a_k, b_k) bounded by $2(\mathrm{g}_{H,2}\{p,q\} + \max\{p-1, q\})$.

Then we fix $\boldsymbol{\epsilon}$ and we apply to incompatibilities (18) for $\boldsymbol{\epsilon}$ and every $\boldsymbol{\kappa}$ and $\boldsymbol{\rho}$, the weak inference

$$\vdash \bigvee_{\substack{K\in\mathcal{K},\\ K'\in\mathcal{K}'}} \Big(\bigwedge_{(k,h)\notin K'} P^{(h)}_{\mathrm{Re}}(z_k)^2 + P^{(h)}_{\mathrm{Im}}(z_k)^2 \neq 0,\ \bigwedge_{(k,h)\in K'} P^{(h)}_{\mathrm{Re}}(z_k)^2 + P^{(h)}_{\mathrm{Im}}(z_k)^2 = 0,$$
$$\bigwedge_{k\notin K} Q^2_{\mathrm{Re}}(z_k) + Q^2_{\mathrm{Im}}(z_k) \neq 0,\ \bigwedge_{k\in K} Q^2_{\mathrm{Re}}(z_k) + Q^2_{\mathrm{Im}}(z_k) = 0 \Big),$$

where

$$\mathcal{K} = \{K \mid K \subset \{1 \le k \le \#\boldsymbol{\nu}\}\} \quad \text{and} \quad \mathcal{K}' = \{K' \mid K' \subset \{1 \le k \le \#\boldsymbol{\nu}\} \times \{1,\dots,p-1\}\}.$$

By Lemma 2.1.19 we obtain

$$\downarrow \operatorname{sign}(\operatorname{ThElim}(P;Q)) = \tau',\ \operatorname{Th}^{\boldsymbol{\mu},\boldsymbol{\nu},\boldsymbol{\eta}}(t,z),\ \bigwedge_{1\le j\le \#\boldsymbol{\mu}} \operatorname{sign}(Q(t_j)) = \epsilon_j \downarrow_{\mathbf{K}[u][t,a,b]} \tag{19}$$

with monoid part

$$\prod_{\substack{H\in \operatorname{ThElim}(P;Q),\\ \tau'(H)\neq 0}} H^{2\hat{g}_H} \cdot \prod_{1\le j<j'\le \#\boldsymbol{\mu}} (t_j - t_{j'})^{2\hat{e}_{j,j'}} \cdot \prod_{1\le k\le \#\boldsymbol{\nu}} b_k^{2\hat{f}_k}.$$

$$\cdot \prod_{1\le k<k'\le \#\boldsymbol{\nu}} \mathrm{R}(z_k, z_{k'})^{2\hat{g}_{k,k'}} \cdot \prod_{\substack{1\le j\le \#\boldsymbol{\mu},\, 1\le h\le p-1,\\ \eta_j(h)\neq 0}} P^{(h)}(t_j)^{2\hat{e}'_{j,h}} \cdot \prod_{\substack{1\le j\le \#\boldsymbol{\mu},\\ \epsilon_j\neq 0}} Q(t_j)^{2\hat{e}'_j}$$

with $\hat{g}_H, \hat{e}_{j,j'}, \hat{f}_k, \hat{g}_{k,k'}, \hat{e}'_{j,h}, \hat{e}'_j \le \tilde{\mathrm{g}}_{H,2}\{p,q\}$, degree in w bounded by $\tilde{\mathrm{g}}_{H,2}\{p,q\}\max\{\deg_w P, \deg_w Q\}$ and degree in t_j and degree in (a_k, b_k) bounded by $\tilde{\mathrm{g}}_{H,2}\{p,q\}$.

Finally, we apply to incompatibilities (15) and (19) for every $\boldsymbol{\epsilon}\neq\boldsymbol{\epsilon}(\tau,\tau')$ the weak inference

$$\vdash \bigvee_{\substack{J\subset\{1,\dots,\#\boldsymbol{\mu}\}\\ J'\subset\{1,\dots,\boldsymbol{\mu}\}\setminus J}} \Big(\bigwedge_{j\in J'} Q(t_j)>0,\ \bigwedge_{j\notin J\cup J'} Q(t_j)<0,\ \bigwedge_{j\in J} Q(t_j)=0\Big).$$

By Lemma 2.1.21 we obtain

$$\downarrow \mathrm{sign}(\mathrm{ThElim}(P;Q))=\tau',\ \mathrm{Th}(P)^{\boldsymbol{\mu},\boldsymbol{\nu},\boldsymbol{\eta}},\ \mathcal{H} \downarrow_{\mathbf{K}[v]}$$

with monoid part

$$S^{h'} \cdot \prod_{\substack{H\in\mathrm{ThElim}(P;Q),\\ \tau'(H)\neq 0}} H^{2h'_H} \cdot \prod_{1\le j<j'\le \#\boldsymbol{\mu}} (t_j - t_{j'})^{2e_{j,j'}} \cdot \prod_{1\le k\le \#\boldsymbol{\nu}} b_k^{2f_k}$$

$$\cdot \prod_{1\le k<k'\le \#\boldsymbol{\nu}} \mathrm{R}(z_k, z_{k'})^{2g_{k,k'}} \cdot \prod_{\substack{1\le j\le \#\boldsymbol{\mu}, 1\le h\le p-1,\\ \eta_j(h)\neq 0}} P^{(h)}(t_j)^{2e'_{h,j}}$$

with

$$\begin{aligned} h' &\le 2^{(p+2)2^p-2p-2}\max\{h, \tilde{\mathrm{g}}_{H,2}\{p,q\}\}^{2^p-1},\\ h'_H, e_{j,j'}, f_k, g_{k,k'}, e'_{h,j} &\le 2^{(p+2)2^p-2}\max\{h, \tilde{\mathrm{g}}_{H,2}\{p,q\}\}^{2^p-1}\tilde{\mathrm{g}}_{H,2}\{p,q\}, \end{aligned}$$

and degree in w bounded by

$$2^{(p+2)2^p-2}\max\{h, \tilde{\mathrm{g}}_{H,2}\{p,q\}\}^{2^p-1}\max\{\delta_w, \tilde{\mathrm{g}}_{H,2}\{p,q\}\max\{\deg_w P, \deg_w Q\}\},$$

degree in t_j bounded by

$$2^{(p+2)2^p-2}\max\{h, \tilde{\mathrm{g}}_{H,2}\{p,q\}\}^{2^p-1}\max\{\delta_t, \tilde{\mathrm{g}}_{H,2}\{p,q\}\}$$

and degree in (a_k, b_k) bounded by

$$2^{(p+2)2^p-2}\max\{h, \tilde{\mathrm{g}}_{H,2}\{p,q\}\}^{2^p-1}\max\{\delta_z, \tilde{\mathrm{g}}_{H,2}\{p,q\}\},$$

which serves as the final incompatibility. □

We finish this subsection with the following remark, which will be used in Subsection 6.3.

Remark 6.2.10 *Following Definition 6.2.3, there are*

$$\sum_{0\le j\le i}\binom{p-1}{j}2^j \le 2p^i$$

elements in $\mathrm{PDer}_i(P)$*. Therefore, there are at most* $2p^{\mathrm{bit}\{p\}+1}$ *elements in* $\mathrm{ThElim}(P)$ *and, by Remark 5.2.14, their degrees in* u *are bounded by*

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

Similarly, there are at most $4p^{\mathrm{bit}\{p\}}$ *elements in* $\mathrm{ThElim}(P;Q)$ *and, again by Remark 5.2.14, their degrees in* u *are bounded by*

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

6.3 Conditions on the parameters fixing the real root order on a family

Consider now a finite family $\mathcal{Q}$ of polynomials in $\mathbf{K}[u][y]$ monic in the variable y, with $u = (u_1, \dots, u_k)$. Our aim is to define a family $\mathrm{Elim}(\mathcal{Q}) \subset \mathbf{K}[u]$ such that the list of realizable sign conditions on $\mathrm{Elim}(\mathcal{Q})$ fixes the factorization and relative order between the real roots of all polynomials in $\mathcal{Q}$.

Definition 6.3.1 *Let* $\mathcal{Q}$ *be a finite family of polynomials in* $\mathbf{K}[u][y]$ *monic in the variable* y*. We denote by*

$$\mathrm{Der}_+(\mathcal{Q}) = \bigcup_{P \in \mathcal{Q}} \mathrm{Der}_+(P) \subset \mathbf{K}[u][y].$$

We define

$$\mathrm{Elim}(\mathcal{Q}) = \bigcup_{P \in \mathcal{Q}} \Big(\mathrm{ThElim}(P) \bigcup \bigcup_{Q \in \mathrm{Der}_+(\mathcal{Q}) \setminus \mathrm{Der}_+(P)} \mathrm{ThElim}(P;Q)\Big) \subset \mathbf{K}[u].$$

In order to prove that the family $\mathrm{Elim}(\mathcal{Q})$ satisfies the required property, we introduce some notation and defintions.

Notation 6.3.2 *Let* $\mathcal{Q}$ *be a finite family of polynomials in* $\mathbf{K}[u][y]$ *monic in the variable* y*. We define the set* $\mathrm{H}(\mathcal{Q})$*, whose elements give a description of the total list of real roots of* $\mathcal{Q}$*. An element of* $\mathrm{H}(\mathcal{Q})$ *is a list* $\boldsymbol{\eta} = [\eta_1, \dots, \eta_r]$ *of distinct sign conditions on* $\mathrm{Der}_+(\mathcal{Q})$ *such that*

- *for every* $1 \le j \le r$*, there exists* $P \in \mathcal{Q}$ *such that* $\eta_j(P) = 0$*.*
- *for every* $1 \le j \le r$ *and every* $P \in \mathcal{Q}$ *such that* $\eta_j(P) = 0$*,* $\eta_{j'} \prec_P \eta_j$ *for* $1 \le j' < j$ *and* $\eta_j \prec_P \eta_{j'}$ *for* $j < j' \le r$*.*
- *for every* $1 \le j < j' \le r$ *and every* $P \in \mathcal{Q}$*,* $\eta_j \preceq_P \eta_{j'}$*.*

For $\boldsymbol{\eta} \in \mathrm{H}(\mathcal{Q})$ *and* $P \in \mathcal{Q}$ *we define* $\boldsymbol{\eta}(P)$ *as the (possibly empty) ordered sublist of* $\boldsymbol{\eta} \mid_{\mathrm{Der}(P)}$ *containing* $\eta_j \mid_{\mathrm{Der}(P)}$ *for those* $1 \le j \le r$ *such that* $\eta_j(P) = 0$*.*

Given $\boldsymbol{\eta} \in \mathrm{H}(\mathcal{Q})$*, we define the set* $\mathrm{N}(\mathcal{Q}, \boldsymbol{\eta})$*, whose elements give a description of the multiplicity of the complex roots of the polynomials in* $\mathcal{Q}$*, given the description* $\boldsymbol{\eta}$ *of their real roots, by*

$$\mathrm{N}(\mathcal{Q}, \boldsymbol{\eta}) = \prod_{P \in \mathcal{Q}} \Lambda_{\frac{1}{2}(\deg_y P - |\mathrm{vmu}(\boldsymbol{\eta}(P))|)}.$$

(cf Notation 6.2.1).

Note that every choice of $\vartheta \in \mathbf{R}^k$ defines an element $\boldsymbol{\eta}$ of $\mathrm{H}(\mathcal{Q})$ and an element $\boldsymbol{\nu}$ of $\mathrm{N}(\mathcal{Q}, \boldsymbol{\eta})$ by considering the list of signs of $\mathrm{Der}_+(\mathcal{Q}(\vartheta))$ at the roots $\theta_1, \ldots, \theta_r$ of the polynomials in $\mathcal{Q}(\vartheta) \subset \mathbf{K}[y]$ as well as the vectors of multiplicities of their complex roots.

Definition 6.3.3 *Let $\mathcal{Q}$ be a finite family of polynomials in $\mathbf{K}[u][y]$ monic in the variable y and $\boldsymbol{\eta} \in \mathrm{H}(\mathcal{Q}), \boldsymbol{\nu} \in \mathrm{N}(\mathcal{Q}, \boldsymbol{\eta})$ with $\boldsymbol{\eta} = [\eta_1, \ldots, \eta_r]$, $t = (t_1, \ldots, t_r)$, t_P be the vector formed by those t_j whose indices appear in $\boldsymbol{\eta}(P)$ in the order $\prec_P^{\mathrm{mu}}$, $z_P = (z_{P,1}, \ldots, z_{P,\#\boldsymbol{\nu}(P)})$ for $P \in \mathcal{Q}$ and $z = (z_P)_{P \in \mathcal{Q}}$. We define the system of sign conditions*

$$\mathrm{OFact}(\mathcal{Q})^{\boldsymbol{\eta}, \boldsymbol{\nu}}(t, z)$$

in $\mathbf{K}[u][t, a, b]$ describing the decompostion into irreducible real factors and the relative order between the real roots of all polynomials in $\mathcal{Q}$:

$$\bigwedge_{P \in \mathcal{Q}} \mathrm{Fact}(P)^{\mathrm{vmu}(\boldsymbol{\eta}(P)), \boldsymbol{\nu}(P)}(t_P, z_P), \quad \bigwedge_{1 \le j < j' \le r} t_j < t_{j'}.$$

The folowing result show the connection between a sign condition on the set $\mathrm{Elim}(\mathcal{Q})$ and the order between the real roots of the family $\mathcal{Q}$.

Theorem 6.3.4 (Fixing the Ordered List of the Roots) *For every realizable sign condition τ on $\mathrm{Elim}(\mathcal{Q})$, there exist $\boldsymbol{\eta}(\tau) \in \mathrm{H}(\mathcal{Q})$, $\boldsymbol{\nu}(\tau) \in \mathrm{N}(\mathcal{Q}, \boldsymbol{\eta}(\tau))$ such that for every $\vartheta \in \mathrm{Real}(\tau, \mathbf{R})$ there exist $\theta \in \mathbf{R}^{\#\boldsymbol{\eta}(\tau)}$, $\alpha \in \mathbf{R}^s, \beta \in \mathbf{R}^s$ with $s = \sum_{P \in \mathcal{Q}} \#\boldsymbol{\nu}(\tau)$ such that*

$$\mathrm{OFact}(\mathcal{Q}(\vartheta))^{\boldsymbol{\eta}(\tau), \boldsymbol{\nu}(\tau)}(\theta, \alpha + i\beta).$$

Proof. By usual properties of Thom encoding [4, Proposition 2.28] and sign determination [45, Theorem 27] a sign condition τ on $\mathrm{Elim}(\mathcal{Q})$ determines the decomposition into irreducible real factors and the relative order between the real roots of all polynomials in $\mathcal{Q}$. $\square$

Before giving a weak inference form of Theorem 6.3.4, we define new auxiliary functions (see Definitions 4.3.3 and 6.2.6).

Definition 6.3.5 *1. Let $\tilde{\mathrm{g}}_{H,3} : \mathbb{N}_* \to \mathbb{R}$, $\tilde{\mathrm{g}}_{H,3}\{p\} = \tilde{\mathrm{g}}_{H,2}\{p, p\}$.*

2. Let $\mathrm{g}_6 : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{R}$,

$$\begin{aligned} \mathrm{g}_6\{p, s, e, f, g\} \;=\; & \left(\mathrm{g}_4\{p\} g^{2^{\frac{1}{2}p^2}} f^{2^{\frac{1}{2}p}}\right)^{\frac{2^{s(\frac{3}{2}p^2+2)}-1}{2^{\frac{3}{2}p^2+2}-1}} 2^{(p+4)(2^{s(s-1)p^2}-1)2^{s(\frac{3}{2}p^2+2)}} \cdot \\ & \cdot \max\{(ps-1)e + s - 1, \tilde{\mathrm{g}}_{H,3}\{p\}\}^{2^{s(s-1)p^2 + s(\frac{3}{2}p^2+2)}-1}. \end{aligned}$$

We now give a weak inference form of Theorem 6.3.4.

Theorem 6.3.6 (Fixing the Ordered List of the Roots as a weak existence) *Let $p \ge 1$, $\mathcal{Q}$ be a family of s polynomials in $\mathbf{K}[u][y] \setminus \mathbf{K}$, monic in the variable y with $\deg_y P \le p$ for every $P \in \mathcal{Q}$, and τ be a realizable sign condition on $\mathrm{Elim}(\mathcal{Q})$. Then*

$$\mathrm{sign}(\mathrm{Elim}(\mathcal{Q})) = \tau \quad \vdash \quad \exists (t, z) \; [\; \mathrm{OFact}(\mathcal{Q})^{\boldsymbol{\eta}(\tau), \boldsymbol{\nu}(\tau)}(t, z) \;]$$

where $t = (t_1, \ldots, t_r)$ *with* $r = \#\boldsymbol{\eta}(\tau)$, $z_P = (z_{P,1}, \ldots, z_{P,\#\boldsymbol{\nu}(\tau)(P)})$ *for* $P \in \mathcal{Q}$ *and* $z = (z_P)_{P \in \mathcal{Q}}$.

Suppose we have an initial incompatibility in variables (v, t, a, b), *where* $v \supset u$, *and* t, a, b *are disjoint from* v, *with monoid part*

$$S \cdot \prod_{1 \le j < j' \le r} (t_j - t_{j'})^{2e_{j,j'}} \cdot \prod_{\substack{P \in \mathcal{Q}, \\ 1 \le k \le \#\boldsymbol{\nu}(\tau)(P)}} b_{P,k}^{2f_{P,k}} \cdot \prod_{\substack{P \in \mathcal{Q}, \\ 1 \le k < k' \le \#\boldsymbol{\nu}(\tau)(P)}} \mathrm{R}(z_{P,k}, z_{P,k'})^{2g_{P,k,k'}},$$

with $e_{j,j'} \le e \in \mathbb{N}_*$, $f_{P,k} \le f \in \mathbb{N}_*$, $g_{P,k,k'} \le g \in \mathbb{N}_*$, *degree in* w *bounded by* δ_w *for some subset of variables* $w \subset v$, *degree in* t_j *bounded by* δ_t *and degree in* $(a_{P,k}, b_{P,k})$ *bounded by* δ_z. *Then the final incompatibility has monoid part*

$$S^h \cdot \prod_{\substack{H \in \mathrm{Elim}(\mathcal{Q}), \\ \tau(H) \neq 0}} H^{2h'_H}$$

with $h, h'_H \le \mathrm{g}_6\{p, s, e, f, g\} \max\{(ps-1)e + s - 1, \tilde{\mathrm{g}}_{H,3}\{p\}\}$ *and degree in* w *bounded by*

$$\begin{aligned} & \mathrm{g}_6\{p, s, e, f, g\} \cdot \Big(\max\Big\{ 2^{ps(s-1)}(\delta_w + (ps(ps-1)(3e+1) + 14) \deg_w \mathcal{Q}), \tilde{\mathrm{g}}_{H,3}\{p\} \deg_w \mathcal{Q} \Big\} \\ + \ & \max\Big\{ 2^{ps(s-1)}(\delta_t + ((ps-1)(6e+2) + 15)p - 8) + p, 2^{ps(s-1)}\delta_z + p, \tilde{\mathrm{g}}_{H,3}\{p\} \Big\} \deg_w \mathcal{Q} \Big), \end{aligned}$$

where $\deg_w \mathcal{Q} = \max\{\deg_w P \mid P \in \mathcal{Q}\}$.

Proof. We simplify the notation by renaming $\boldsymbol{\eta}(\tau) = \boldsymbol{\eta}$, and $\boldsymbol{\nu}(\tau) = \boldsymbol{\nu}$. Consider the initial incompatibility

$$\downarrow \mathrm{OFact}(\mathcal{Q})^{\boldsymbol{\eta}, \boldsymbol{\nu}}(t, z), \ \mathcal{H} \downarrow_{\mathbf{K}[v][t,a,b]} \tag{20}$$

where $\mathcal{H}$ is a system of sign conditions in $\mathbf{K}[v]$.

For $1 \le j < j' \le r$ there exists a polynomial P in $\mathcal{Q}$ such that $\eta_j(P) = 0$ and $\eta_j \prec_P \eta_{j'}$. We successively apply to (20) for each such pair (j, j') the weak inference

$$t_j < t_{j'} \quad \vdash \quad t_j \neq t_{j'}$$

if it is the case that exists $Q \in \mathcal{Q}$ with $\mathrm{mu}(\eta_j, Q) > 0$ and $\mathrm{mu}(\eta_{j'}, Q) > 0$ and

$$\mathrm{sign}(\mathrm{Der}_+(P)(t_j)) = \eta_j, \ \mathrm{sign}(\mathrm{Der}_+(P)(t_{j'})) = \eta_{j'} \quad \vdash \quad t_j < t_{j'}$$

in every case. By Lemma 2.1.2 (item 2) and Proposition 6.1.9 we obtain

$$\begin{aligned} \Big\downarrow \bigwedge_{P \in \mathcal{Q}} P \equiv \mathrm{F}^{\mathrm{vmu}(\boldsymbol{\eta}(P)), \boldsymbol{\nu}(P)}(t_P, z_P), \quad \bigwedge_{\substack{P \in \mathcal{Q}, \\ 1 \le k \le \#\boldsymbol{\nu}(P)}} b_{P,k} \neq 0, \\ \bigwedge_{\substack{P \in \mathcal{Q}, \\ 1 \le k < k' \le \#\boldsymbol{\nu}(P)}} \mathrm{R}(z_k, z_{k'}) \neq 0, \ \bigwedge_{1 \le j \le r} \mathrm{sign}(\mathrm{Der}_+(\mathcal{Q})(t_j)) = \eta_j, \ \mathcal{H} \Big\downarrow_{\mathbf{K}[v][t,a,b]} \end{aligned} \tag{21}$$

with monoid part

$$S \cdot \prod_{\substack{1 \le j \le r, \, Q \in \mathrm{Der}_+(\mathcal{Q}), \\ \eta_j(Q) \neq 0}} Q(t_j)^{2e_{Q,j}} \cdot \prod_{\substack{P \in \mathcal{Q}, \\ 1 \le k \le \#\boldsymbol{\nu}(P)}} b_{P,k}^{2f_{P,k}} \cdot \prod_{\substack{P \in \mathcal{Q}, \\ 1 \le k < k' \le \#\boldsymbol{\nu}(P)}} \mathrm{R}(z_{P,k}, z_{P,k'})^{2g_{P,k,k'}}$$

with $e_{Q,j} \le (r-1)e$, degree in w bounded by $\delta_w + r(r-1)(3e+1)\deg_w \mathcal{Q}$, degree in t_j bounded by $\delta_t + (r-1)(6e+2)p$ and degree in $(a_{P,k}, b_{P,k})$ bounded by δ_z.

For each $1 \le j \le r$, suppose that $\mathcal{Q}_j$ is the list of polynomials P in $\mathcal{Q}$ such that $\mathrm{mu}(\eta_j, P) > 0$, t_j is the $\alpha(j,P)$-th element in t_P for $P \in \mathcal{Q}_j$ and $P_{\gamma(j)}$ the first element of $\mathcal{Q}_j$. Conversly, suppose that for $P \in \mathcal{Q}$ and $1 \le j' \le \#\boldsymbol{\eta}(P)$, the j'-th element in t_P is $t_{\beta(P,j')}$. We consider new variables $t'_P = (t'_{P,1}, \dots, t'_{P,\#\boldsymbol{\eta}(P)})$ for every $P \in \mathcal{Q}$ and we substitute t_j by $t'_{P_{\gamma(j)},\alpha(j,P_{\gamma(j)})}$ in (21) for $1 \le j \le r$. For each $P \in \mathcal{Q}$, let $\tilde{t}_P$ be the result obtained in each t_P after these substitutions. Then we apply the weak inference

$$\bigwedge_{\substack{1\le j\le r,\\ P\in\mathcal{Q}_j\setminus\{P_{\gamma(j)}\}}} t'_{P_{\gamma(j)},\alpha(j,P_{\gamma(j)})} = t'_{P,\alpha(j,P)},\ \bigwedge_{P\in\mathcal{Q}} P \equiv \mathrm{F}^{\mathrm{vmu}(\boldsymbol{\eta}(P)),\boldsymbol{\nu}(P)}(t'_P, z_P) \quad \vdash$$

$$\vdash \quad \bigwedge_{P\in\mathcal{Q}} P \equiv \mathrm{F}^{\mathrm{vmu}(\boldsymbol{\eta}(P)),\boldsymbol{\nu}(P)}(\tilde{t}_P, z_P).$$

By Lemma 2.1.8 we obtain

$$\begin{aligned}\downarrow \bigwedge_{\substack{1\le j\le r,\\ P\in\mathcal{Q}_j\setminus\{P_{\gamma(j)}\}}} t'_{P_{\gamma(j)},\alpha(j,P_{\gamma(j)})} = t'_{P,\alpha(j,P)},\ \bigwedge_{P\in\mathcal{Q}} P \equiv \mathrm{F}^{\mathrm{vmu}(\boldsymbol{\eta}(P)),\boldsymbol{\nu}(P)}(t'_P, z_P),\\ \bigwedge_{\substack{P\in\mathcal{Q},\\ 1\le k\le\#\boldsymbol{\nu}(P)}} b_{P,k} \ne 0,\ \bigwedge_{\substack{P\in\mathcal{Q},\\ 1\le k<k'\le\#\boldsymbol{\nu}(P)}} \mathrm{R}(z_{P,k}, z_{P,k'}) \ne 0,\\ \bigwedge_{\substack{P\in\mathcal{Q},\\ 1\le j\le\#\boldsymbol{\eta}(P)}} \mathrm{sign}(\mathrm{Der}_+(\mathcal{Q})(t'_{P,j})) = \eta_{\beta(P,j)},\ \mathcal{H}\big\downarrow_{\mathbf{K}[v][(t'_P)_{P\in Q},a,b]}\end{aligned} \tag{22}$$

with monoid part

$$S \cdot \prod_{\substack{P\in\mathcal{Q},\\ 1\le j\le\#\boldsymbol{\eta}(P)}} \prod_{\substack{Q\in\mathrm{Der}_+(\mathcal{Q}),\\ \eta_{\beta(P,j)}(Q)\ne 0}} Q(t'_{P,j})^{2e_{P,Q,j}} \cdot \prod_{\substack{P\in\mathcal{Q},\\ 1\le k\le\#\boldsymbol{\nu}(P)}} b_{P,k}^{2f_{P,k}} \cdot \prod_{\substack{P\in\mathcal{Q},\\ 1\le k<k'\le\#\boldsymbol{\nu}(P)}} \mathrm{R}(z_{P,k}, z_{P,k'})^{2g_{P,k,k'}}$$

with $e_{P,Q,j} \le (r-1)e$, degree in w bounded by $\delta_w + r(r-1)(3e+1)\deg_w \mathcal{Q}$, degree in $t'_{P,j}$ bounded by $\delta_t + ((r-1)(6e+2)+1)p$ and degree in $(a_{P,k}, b_{P,k})$ bounded by δ_z. For simplicity we rename t'_P as t_P for every $P \in \mathcal{Q}$ and $(t'_P)_{P\in Q}$ as t.

Then we successively apply to (22) for $1 \le j \le r$ and $P \in \mathcal{Q}_j \setminus \{P_{\gamma(j)}\}$ the weak inference

$$\mathrm{sign}(\mathrm{Der}_+(P_{\gamma(j)})(t_{P_{\gamma(j)},\alpha(j,P_{\gamma(j)})})) = \eta_j,\ \mathrm{sign}(\mathrm{Der}_+(P_{\gamma(j)})(t_{P,\alpha(j,P)})) = \eta_j \quad \vdash$$

$$\vdash \quad t_{P_{\gamma(j)},\alpha(j,P_{\gamma(j)})} = t_{P,\alpha(j,P)}.$$

By Proposition 6.1.7, we obtain

$$\begin{aligned}\downarrow \bigwedge_{P\in\mathcal{Q}} P \equiv \mathrm{F}^{\mathrm{vmu}(\boldsymbol{\eta}(P)),\boldsymbol{\nu}(P)}(t_P, z_P),\ \bigwedge_{\substack{P\in\mathcal{Q},\\ 1\le k\le\#\boldsymbol{\nu}(P)}} b_{P,k} \ne 0,\\ \bigwedge_{\substack{P\in\mathcal{Q},\\ 1\le k<k'\le\#\boldsymbol{\nu}(P)}} \mathrm{R}(z_{P,k}, z_{P,k'}) \ne 0,\ \bigwedge_{\substack{P\in\mathcal{Q},\\ 1\le j\le\#\boldsymbol{\eta}(P)}} \mathrm{sign}(\mathrm{Der}_+(\mathcal{Q})(t_{P,j})) = \eta_{\beta(P,j)},\ \mathcal{H}\big\downarrow_{\mathbf{K}[v][t,a,b]}\end{aligned} \tag{23}$$

with monoid part

$$S\cdot \prod_{\substack{P\in\mathcal{Q},\\ 1\le j\le \#\boldsymbol{\eta}(P)}} \prod_{\substack{Q\in \mathrm{Der}_+(\mathcal{Q}),\\ \eta_{\beta(P,j)}(Q)\neq 0}} Q(t_{P,j})^{2e'_{P,Q,j}} \cdot \prod_{\substack{P\in\mathcal{Q},\\ 1\le k\le \#\boldsymbol{\nu}(P)}} b_{P,k}^{2f_{P,k}} \cdot \prod_{\substack{P\in\mathcal{Q},\\ 1\le k<k'\le \#\boldsymbol{\nu}(P)}} \mathrm{R}(z_{P,k}, z_{P,k'})^{2g_{P,k,k'}}$$

with $e'_{P,Q,j} \le (r-1)e + s - 1 =: e'$, degree in w bounded by $2^{r(s-1)}(\delta_w + (r(r-1)(3e+1) + 14)\deg_w \mathcal{Q})$, degree in $t_{P,j}$ bounded by $2^{r(s-1)}(\delta_t + ((r-1)(6e+2)+15)p - 8)$ and degree in $(a_{P,k}, b_{P,k})$ bounded by $2^{r(s-1)}\delta_z$.

Then we apply to (23) the weak inference

$$\bigwedge_{P\in\mathcal{Q}} P \equiv \mathrm{F}^{\mathrm{vmu}(\boldsymbol{\eta}(P)),\boldsymbol{\nu}(P)}(t_P, z_P) \quad \vdash \quad \bigwedge_{\substack{P\in\mathcal{Q},\\ 1\le j\le \#\boldsymbol{\eta}(P)}} P(t_{P,j}) = 0.$$

By Lemma 2.1.8 we obtain

$$\begin{aligned} \downarrow \bigwedge_{P\in\mathcal{Q}} P \equiv \mathrm{F}^{\mathrm{vmu}(\boldsymbol{\eta}(P)),\boldsymbol{\nu}(P)}(t_P, z_P), \quad \bigwedge_{\substack{P\in\mathcal{Q},\\ 1\le k\le \#\boldsymbol{\nu}_P}} b_{P,k}\neq 0, \quad \bigwedge_{\substack{P\in\mathcal{Q},\\ 1\le k<k'\le \#\boldsymbol{\nu}(P)}} \mathrm{R}(z_{P,k}, z_{P,k'}) \neq 0, \\ \bigwedge_{\substack{P\in\mathcal{Q},\, Q\in\mathrm{Der}_+(\mathcal{Q})\setminus\{P\},\\ 1\le j\le\#\boldsymbol{\eta}(P)}} \mathrm{sign}(Q(t_{P,j})) = \eta_{\beta(P,j)}(Q),\ \mathcal{H}\downarrow_{\mathbf{K}[v][t,a,b]} \end{aligned} \tag{24}$$

with the same monoid part, degree in w bounded by $\delta'_w := 2^{r(s-1)}(\delta_w + (r(r-1)(3e+1) + 14)\deg_w \mathcal{Q})$, degree in $t_{P,j}$ bounded by $\delta'_t := 2^{r(s-1)}(\delta_t + ((r-1)(6e+2)+15)p - 8) + p$ and degree in $(a_{P,k}, b_{P,k})$ bounded by $\delta'_z := 2^{r(s-1)}\delta_z + p$.

Now we fix an arbitrary order $(P_1, Q_1), \dots, (P_m, Q_m)$ in the set $\{(P,Q)\in\mathcal{Q}\times\mathrm{Der}_+(\mathcal{Q}) \mid Q\notin \mathrm{Der}_+(P)\}$, note that $m \le s(s-1)p$. For $1\le i\le m$, we successively apply to (24) the weak inference

$$\mathrm{sign}(\mathrm{ThElim}(P_i,Q_i)) = \tau,\ \mathrm{Th}(P_i)^{\mathrm{vmu}(\boldsymbol{\eta}(P_i)),\boldsymbol{\nu}(P_i),\boldsymbol{\eta}(P_i)}(t_{P_i}, z_{P_i}) \quad \vdash$$

$$\vdash \quad \bigwedge_{1\le j\le \#\boldsymbol{\eta}(P_i)} \mathrm{sign}(Q_i(t_{P_i,j})) = \eta_{\beta(P_i,j)}.$$

Using Theorem 6.2.9 (Fixing the Thom encodings with a Sign as a weak existence), it can be proved by induction on i that for $1\le i\le m$, after the application of the i-th weak inference, we obtain an incompatibility in $\mathbf{K}[v][t,a,b]$ with monoid part

$$S^{\tilde h_i}\cdot \prod_{\substack{H\in\mathrm{Elim}(\mathcal{Q}),\\ \tau(H)\neq 0}} H^{2\tilde h'_{H,i}} \cdot \prod_{\substack{P\in\mathcal{Q},\\ 1\le j\le\#\boldsymbol{\eta}(P)}} \Bigg(\prod_{\substack{1\le h\le \deg_y P-1,\\ \eta_{\beta(P,j)}(P^{(h)})\neq 0}} P^{(h)}(t_{P,j})^{2\tilde e'_{P,j,h,i}} \cdot \prod_{\substack{Q\in\mathrm{Der}_+(\mathcal{Q})\setminus \mathrm{Der}_+(P),\\ \eta_{\beta(P,j)}(Q)\neq 0}} Q(t_{P,j})^{2\tilde e''_{P,Q,j,i}} \Bigg)\cdot$$

$$\cdot \prod_{\substack{P\in\mathcal{Q},\\ 1\le j<j'\le\#\boldsymbol{\eta}(P)}} (t_{P,j} - t_{P,j'})^{2\tilde e_{P,j,j',i}} \cdot \prod_{\substack{P\in\mathcal{Q},\\ 1\le k\le\#\boldsymbol{\nu}(P)}} b_{P,k}^{2\tilde f_{P,k,i}} \cdot \prod_{\substack{P\in\mathcal{Q},\\ 1\le k<k'\le\#\boldsymbol{\nu}(P)}} \mathrm{R}(z_{P,k}, z_{P,k'})^{2\tilde g_{P,k,k',i}}$$

with

$$\begin{array}{rcl}
\tilde{e}''_{P,Q,j,i} & \leq & 2^{((p+2)2^p-2p-2)\frac{2^{ip}-1}{2^p-1}} \max\{e', \tilde{\mathrm{g}}_{H,3}\{p\}\}^{2^{ip}}, \\
\tilde{h}_i & \leq & 2^{((p+2)2^p-2p-2)\frac{2^{ip}-1}{2^p-1}} \max\{e', \tilde{\mathrm{g}}_{H,3}\{p\}\}^{2^{ip}-1}, \\
\tilde{h}'_{H,i}, \tilde{e}_{P,j,j',i} & \leq & 2^{(p+2)2^p-2}(2^{(p+2)2^p-2p-2}+1)^{\frac{2^{ip}-1}{2^p-1}-1} \max\{e', \tilde{\mathrm{g}}_{H,3}\{p\}\}^{2^{ip}-1}\tilde{\mathrm{g}}_{H,3}\{p\}, \\
\tilde{e}'_{P,j,h,i} & \leq & 2^{(p+2)2^p-1}(2^{(p+2)2^p-2p-2}+1)^{\frac{2^{ip}-1}{2^p-1}-1} \max\{e', \tilde{\mathrm{g}}_{H,3}\{p\}\}^{2^{ip}}, \\
\tilde{f}_{P,k,i} & \leq & 2^{(p+2)2^p-1}(2^{(p+2)2^p-2p-2}+1)^{\frac{2^{ip}-1}{2^p-1}-1} \max\{e', \tilde{\mathrm{g}}_{H,3}\{p\}\}^{2^{ip}-1}\tilde{\mathrm{g}}_{H,3}\{p\}f, \\
\tilde{g}_{P,k,i} & \leq & 2^{(p+2)2^p-1}(2^{(p+2)2^p-2p-2}+1)^{\frac{2^{ip}-1}{2^p-1}-1} \max\{e', \tilde{\mathrm{g}}_{H,3}\{p\}\}^{2^{ip}-1}\tilde{\mathrm{g}}_{H,3}\{p\}g,
\end{array}$$

degree in w bounded by $2^{((p+2)2^p-2)\frac{2^{ip}-1}{2^p-1}} \max\{e', \tilde{\mathrm{g}}_{H,3}\{p\}\}^{2^{ip}-1} \max\{\delta'_w, \tilde{\mathrm{g}}_{H,3}\{p\} \deg_w \mathcal{Q}\}$, degree in $t_{P,j}$ bounded by $2^{((p+2)2^p-2)\frac{2^{ip}-1}{2^p-1}} \max\{e', \tilde{\mathrm{g}}_{H,3}\{p\}\}^{2^{ip}-1} \max\{\delta'_t, \tilde{\mathrm{g}}_{H,3}\{p\}\}$ and degree in $(a_{P,k}, b_{P,k})$ bounded by $2^{((p+2)2^p-2)\frac{2^{ip}-1}{2^p-1}} \max\{e', \tilde{\mathrm{g}}_{H,3}\{p\}\}^{2^{ip}-1} \max\{\delta'_z, \tilde{\mathrm{g}}_{H,3}\{p\}\}$. Therefore, at the end we obtain an incompatibility

$$\downarrow \mathrm{sign}(\mathrm{Elim}(\mathcal{Q})) = \tau, \ \bigwedge_{P \in \mathcal{Q}} \mathrm{Th}(P)^{\mathrm{vmu}(\boldsymbol{\eta}(P)), \boldsymbol{\nu}(P), \boldsymbol{\eta}(P)}(t_P, z_P), \ \mathcal{H} \downarrow_{\mathbf{K}[v][t,a,b]} \tag{25}$$

with monoid part

$$S^{\tilde{h}} \cdot \prod_{\substack{H \in \mathrm{Elim}(\mathcal{Q}), \\ \tau(H) \neq 0}} H^{2\tilde{h}'_H} \cdot \prod_{\substack{P \in \mathcal{Q}, \\ 1 \leq j < j' \leq \#\boldsymbol{\eta}(P)}} (t_{P,j} - t_{P,j'})^{2\tilde{e}_{P,j,j'}} \cdot \prod_{\substack{P \in \mathcal{Q}, \\ 1 \leq k \leq \#\boldsymbol{\nu}(P)}} b_{P,k}^{2\tilde{f}_{P,k}} \cdot$$

$$\cdot \prod_{\substack{P \in \mathcal{Q}, \\ 1 \leq k < k' \leq \#\boldsymbol{\nu}(P)}} \mathrm{R}(z_{P,k}, z_{P,k'})^{2\tilde{g}_{P,k,k'}} \cdot \prod_{\substack{P \in \mathcal{Q}, \\ 1 \leq j \leq \#\boldsymbol{\eta}(P)}} \prod_{\substack{1 \leq h \leq \deg_y P - 1, \\ \eta_{\beta(P,j)}(P^{(h)}) \neq 0}} P^{(h)}(t_{P,j})^{2\tilde{e}'_{P,j,h}}$$

with

$$\begin{array}{rcl}
\tilde{h}, \tilde{h}'_H, \tilde{e}_{P,j_1,j_2}, \tilde{e}'_{P,j,h} & \leq & 2^{(p+4)(2^{s(s-1)p^2}-1)} \max\{e', \tilde{\mathrm{g}}_{H,3}\{p\}\}^{2^{s(s-1)p^2}}, \\
\tilde{f}_{P,k} & \leq & 2^{(p+4)(2^{s(s-1)p^2}-1)} \max\{e', \tilde{\mathrm{g}}_{H,3}\{p\}\}^{2^{s(s-1)p^2}} f, \\
\tilde{g}_{P,k_1,k_2} & \leq & 2^{(p+4)(2^{s(s-1)p^2}-1)} \max\{e', \tilde{\mathrm{g}}_{H,3}\{p\}\}^{2^{s(s-1)p^2}} g,
\end{array}$$

degree in w bounded by $2^{(p+4)(2^{s(s-1)p^2}-1)} \max\{e', \tilde{\mathrm{g}}_{H,3}\{p\}\}^{2^{s(s-1)p^2}-1} \max\{\delta'_w, \tilde{\mathrm{g}}_{H,3}\{p\} \deg_w \mathcal{Q}\}$, degree in $t_{P,j}$ bounded by $2^{(p+4)(2^{s(s-1)p^2}-1)} \max\{e', \tilde{\mathrm{g}}_{H,3}\{p\}\}^{2^{s(s-1)p^2}-1} \max\{\delta'_t, \tilde{\mathrm{g}}_{H,3}\{p\}\}$, and degree in $(a_{P,k}, b_{P,k})$ bounded by $2^{(p+4)(2^{s(s-1)p^2}-1)} \max\{e', \tilde{\mathrm{g}}_{H,3}\{p\}\}^{2^{s(s-1)p^2}-1} \max\{\delta'_z, \tilde{\mathrm{g}}_{H,3}\{p\}\}$.

Finally we fix an arbitrary order $P_1, \dots, P_s$ in $\mathcal{Q}$ and for $1 \leq i \leq s$ we successively apply to (25) the weak inference

$$\mathrm{sign}(\mathrm{ThElim}(P_i)) = \tau \quad \vdash \quad \exists (t_{P_i}, z_{P_i}) \ [\ \mathrm{Thom}^{\mathrm{vmu}(\boldsymbol{\eta}(P_i)), \boldsymbol{\nu}(P_i), \boldsymbol{\eta}(P_i)}(t_{P_i}, z_{P_i}) \ ].$$

Using Theorem 6.2.8 (Fixing the Thom encodings as a weak existence), it can be proved by induction on i that for $1 \le i \le s$, after the application of the i-th weak inference, we obtain an incompatibility in $\mathbf{K}[v][t_{P_{i+1}}, \dots, t_{P_s}, a_{P_{i+1}}, b_{P_{i+1}}, \dots, a_{P_s}, b_{P_s}]$ with monoid part

$$S^{h_i} \cdot \prod_{\substack{H \in \mathrm{Elim}(\mathcal{Q}),\\ \tau(H)\neq 0}} H^{2h'_{H,i}} \cdot \prod_{\substack{i+1 \le i' \le s,\\ 1 \le j < j' \le \#\boldsymbol{\eta}(P_i)}} (t_{P_i,j} - t_{P_i,j'})^{2e_{P_i,j,j',i}} \cdot \prod_{\substack{i+1 \le i' \le s,\\ 1 \le k \le \#\boldsymbol{\eta}(P_{i'})}} b_{P_{i'},k}^{2f_{P_{i'},k,i}} \cdot$$

$$\cdot \prod_{\substack{i+1 \le i' \le s,\\ 1 \le k < k' \le \#\boldsymbol{\nu}(P_{i'})}} \mathrm{R}(z_{P,k}, z_{P,k'})^{2g_{P_{i'},k,k',i}} \cdot \prod_{\substack{i+1 \le i' \le s,\\ 1 \le j \le \#\boldsymbol{\eta}(P_{i'})}} \prod_{\substack{1 \le h \le \deg_y P_{i'} - 1,\\ \eta_{\beta(P_{i'},j)}(P^{(h)}) \neq 0}} P^{(h)}(t_{P_{i'},j})^{2e'_{P_{i'},j,h,i}}$$

with, denoting

$$G_i := \left(\mathrm{g}_4\{p\} g^{2^{\frac{1}{2}p^2}} f^{2^{\frac{1}{2}p}}\right)^{\frac{2^{i(\frac{3}{2}p^2+2)}-1}{2^{\frac{3}{2}p^2+2}-1}} 2^{(p+4)(2^{s(s-1)p^2}-1)2^{i(\frac{3}{2}p^2+2)}} \max\{e', \tilde{\mathrm{g}}_{H,3}\{p\}\}^{2^{s(s-1)p^2+i(\frac{3}{2}p^2+2)}-1},$$

$$\begin{aligned} h_i, h'_{H,i}, e_{P_{i'},j,j',i}, e'_{P_{i'},j,h,i} &\le G_i \max\{e', \tilde{\mathrm{g}}_{H,3}\{p\}\} \\ f_{P_{i'},k,i} &\le G_i \max\{e', \tilde{\mathrm{g}}_{H,3}\{p\}\} f, \\ g_{P_{i'},k,k',i} &\le G_i \max\{e', \tilde{\mathrm{g}}_{H,3}\{p\}\} g, \end{aligned}$$

degree in w bounded by $G_i\Big(\max\{\delta'_w, \tilde{\mathrm{g}}_{H,3}\{p\}\deg_w \mathcal{Q}\} + \max\{\delta'_t, \delta'_z, \tilde{\mathrm{g}}_{H,3}\{p\}\}\deg_w \mathcal{Q}\Big)$, degree in $t_{P_{i'},j}$ bounded by $G_i \max\{\delta'_t, \tilde{\mathrm{g}}_{H,3}\{p\}\}$ and degree in $(a_{P_{i'},k,P_{i'},k})$ bounded by $G_i \max\{\delta'_z, \tilde{\mathrm{g}}_{H,3}\{p\}\}$. Therefore, at the end we obtain

$$\downarrow \mathrm{sign}(\mathrm{Elim}(\mathcal{Q})) = \tau,\ \mathcal{H} \downarrow_{\mathbf{K}[v]}$$

with monoid part

$$S^h \cdot \prod_{\substack{H \in \mathrm{Elim}(\mathcal{Q}),\\ \tau(H)\neq 0}} H^{2h'_H}$$

with the respective bounds replacing i by s, which serves as the final incompatibility. □

We finish this subsection with the following remark, which will be used in Section 7.

Remark 6.3.7 *Let $\mathcal{Q} = \{P_1, \dots, P_s\} \subset \mathbf{K}[u][y]$ with P_i monic in the variable y and $\deg_y P_i \le p$ for $1 \le i \le s$. Following Definition 6.3.1, by Remark 6.2.10 there are at most*

$$4s^2 p^{\mathrm{bit}\{p\}+1}$$

elements in $\mathrm{Elim}(\mathcal{Q})$ and their degrees in u are bounded by

$$2p^2(\mathrm{bit}\{p\}+1)\max\{\deg_u P_i \mid 1 \le i \le s\} \le 4p^3 \max\{\deg_u P_i \mid 1 \le i \le s\}.$$

6.4 Realizable sign conditions on a family of polynomials

From the family $\mathrm{Elim}(\mathcal{Q}) \subset \mathbf{K}[u]$ defined in Subsection 6.3, we deduce now the list of realizable sign conditions on $\mathcal{Q}$.

Theorem 6.4.1 (Elimination of One Variable) *For every realizable sign condition τ on $\mathrm{Elim}(\mathcal{Q})$, there exists a list of sign conditions on $\mathcal{Q}$*

$$\mathrm{SIGN}(\mathcal{Q}\,|\tau)$$

such that for every $\vartheta = (\vartheta_1, \dots, \vartheta_k) \in \mathrm{Real}(\tau, \mathbf{R})$, the list of realizable sign conditions on $\mathcal{Q}(\vartheta)$ is $\mathrm{SIGN}(\mathcal{Q}\,|\tau)$.

Proof. The result is immediate from Theorem 6.3.4 (Fixing the Ordered List of the Roots), since once the factorization and relative order between the real roots of all the polynomial in $\mathcal{Q}$ is fixed, the list of all realizable sign conditions on $\mathcal{Q}$ can be determined by looking at the partition of the real line given by the set of real roots. □

Before stating the main result of Section 6, we introduce an auxiliary function.

Definition 6.4.2 *Let* $\mathrm{g}_7 : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{R}$, $\mathrm{g}_7\{p, s, e\} = 2^{2^{3(\frac{p}{2})^p + s^2(\frac{3}{2}p^2+3)+8}} e^{2^{6p^2s^2}}$.

Technical Lemma 6.4.3 *For every $p, s, e \in \mathbb{N}_*$,*

$$2^{ps(s-1)+2}e^2s^4p\,\mathrm{g}_6\{p, s, 2eps + 8(eps)^2, (ps+1)ep + 4e^2p^3s^2, 1\} \max\{8e^2p^3s^3, \tilde{\mathrm{g}}_{H,3}\{p\}\} \leq$$

$$\leq \mathrm{g}_7\{p, s, e\}.$$

Proof. See Section 8. □

The main result of Section 6 is the following weak inference form of Theorem 6.4.1.

Theorem 6.4.4 (Elimination of One Variable as a weak inference) *Let $p \geq 1$, $\mathcal{Q}$ be a family of s polynomials in $\mathbf{K}[u][y] \setminus \mathbf{K}$, monic in the variable y with $\deg_y P \leq p$ for every $P \in \mathcal{Q}$ and τ be a realizable sign condition on $\mathrm{Elim}(\mathcal{Q})$. Then*

$$\mathrm{sign}(\mathrm{Elim}(\mathcal{Q})) = \tau \quad \vdash \bigvee_{\sigma \in \mathrm{SIGN}(\mathcal{Q}\,|\tau)} \mathrm{sign}(\mathcal{Q}) = \sigma.$$

Suppose we have initial incompatibilities with monoid part

$$S_\sigma \cdot \prod_{\substack{P \in \mathcal{Q}, \\ \sigma(P) \neq 0}} P^{2e_{P,\sigma}}$$

with $e_{P,\sigma} \leq e \in \mathbb{N}_*$ and degree in $w \subset v$ bounded by δ_w. Then, the final incompatibility has monoid part

$$\prod_{\sigma \in \mathrm{SIGN}(\mathcal{Q}\,|\tau)} S_\sigma^{h_\sigma} \cdot \prod_{\substack{H \in \mathrm{Elim}(\mathcal{Q}), \\ \tau(H) \neq 0}} H^{2h'_H}$$

with $h_\sigma, h'_H \leq \mathrm{g}_7\{p, s, e\}$ and degree in w bounded by $\mathrm{g}_7\{p, s, e\} \max\{\delta_w, \deg_w \mathcal{Q}\}$.

As said before, once the factorization and relative order between the real roots of all polynomials in $\mathcal{Q}$ is fixed, the list of all realizable sign conditions on $\mathcal{Q}$ can be determined by looking at the partition of the real line given by the set of real roots. We prove now weak inference version of some auxiliary results in this direction.

Proposition 6.4.5

$$\vdash \quad y < t_1 \ \vee \ \ y = t_1 \ \vee (\ t_1 < y, \ y < t_2) \ \vee \ \ldots \ \vee \ (\ t_{r-1} < y, \ y < t_r) \ \vee \ y = t_r \ \vee \ t_r < y.$$

Suppose we have initial incompatibilities in variables $v \supset (t_1, \ldots, t_r, y)$ *with monoid part*

$$S'_1(y-t_1)^{2e_1}, \ S_1, \ S'_2(y-t_1)^{2f_1}(y-t_2)^{2e_2}, \ \ldots, \ S'_r(y-t_{r-1})^{2f_{r-1}}(y-t_r)^{2e_r}, \ S_r, \ \ S'_{r+1}(y-t_r)^{2f_r}$$

with $e_j \le e$ *and* $f_j \le e$ *and degree in* w *bounded by* $\delta'_{w,1}, \ \delta_{w,1}, \ \delta'_{w,2}, \ldots, \ \delta'_{w,r}, \ \delta_{w,r}, \ \delta'_{w,r+1}$ *for some subset of variables* $w \supset v$*. Then, the final incompatibility has monoid part*

$$\prod_{1 \le j \le r+1} S'_j \cdot \prod_{1 \le j \le r} S_j^{2(e_j+f_j)}$$

and degree in w *bounded by* $\sum_{1 \le j \le r+1} \delta'_{w,j} + 4e \cdot \sum_{1 \le j \le r} \delta_{w,j}$*.*

When $t_1, \ldots, t_r$ are not variables but elements in $\mathbf{K}$, similar degree estimations are due to Warou [55].

Proof. Consider the initial incompatibilities

$$\downarrow y < t_1, \ \mathcal{H} \downarrow, \ \ldots, \ \downarrow t_{r-1} < y, \ y < t_r, \ \mathcal{H} \downarrow, \ \downarrow y = t_r, \ \mathcal{H} \downarrow, \ \downarrow t_r < y, \ \mathcal{H} \downarrow_{\mathbf{K}[v]} \tag{26}$$

where $\mathcal{H}$ is a system of sign conditions in $\mathbf{K}[v]$.

We proceed by induction on r. If $r = 1$, the result follows from Lemma 2.1.18. Suppose now $r > 1$. We apply to the last three initial incompatibilities (26) the weak inference

$$\vdash \quad y < t_r \ \vee \ y = t_r \ \vee \ t_r < y.$$

By Lemma 2.1.18 we obtain an incompatibility

$$\downarrow t_{r-1} < y, \ \mathcal{H} \downarrow_{\mathbf{K}[v]} \tag{27}$$

with monoid part

$$S'_r \cdot S'_{r+1} \cdot S_r^{2(e_r+f_r)} \cdot (y - t_{r-1})^{2f_{r-1}}$$

and degree in w bounded by $\delta'_{w,r} + \delta'_{w,r+1} + 4e \cdot \delta_{w,r}$. The result follows by applying the inductive hypothesis to the remaining initial incompatibilities (26) and (27). □

Lemma 6.4.6 *Let* $p \ge 1$*,* $\mathcal{Q}$ *be a family of* s *polynomials in* $\mathbf{K}[u][y] \setminus \mathbf{K}$*, monic in the variable* y *with* $\deg_y P \le p$ *for every* $P \in \mathcal{Q}$*,* τ *be a realizable sign condition on* $\mathrm{Elim}(\mathcal{Q})$*,* $\boldsymbol{\eta}(\tau) = [\eta_1, \ldots, \eta_r]$ *with* $r \ge 1$ *and* $1 \le j_0 \le r$*. Then, defining* $\varepsilon_P = (-1)^{\sum_{j_0+1 \le j' \le r} \mathrm{mu}(\eta_{j'}, P)}$*,*

$$\exists (t,z) \ [\ \mathrm{OFact}(\mathcal{Q})^{\boldsymbol{\eta}(\tau), \boldsymbol{\nu}(\tau)}(t,z), \ y = t_{j_0} \ ] \quad \vdash \quad \bigwedge_{\substack{P \in \mathcal{Q}, \\ \mathrm{mu}(\eta_{j_0}, P) > 0}} P = 0, \quad \bigwedge_{\substack{P \in \mathcal{Q}, \\ \mathrm{mu}(\eta_{j_0}, P) = 0}} \mathrm{sign}(P) = \varepsilon_P$$

where $t = (t_1, \dots, t_r)$, $z = (z_P)_{P\in\mathcal{Q}}$ *and* $z_P = (z_{P,1}, \dots, z_{P,\#\boldsymbol{\nu}(\tau)(P)})$.

Suppose we have an initial incompatibility in variables $v \supset (u, y)$ *with monoid part*

$$S \cdot \prod_{\substack{P\in\mathcal{Q},\\ \mathrm{mu}(\eta_{j_0},P)=0}} P^{2e_P}$$

with $e_P \le e \in \mathbb{N}_*$ *and degree in* w *bounded by* δ_w *for some set of variables* $w \subset v$. *Then, the final incompatibility has monoid part*

$$S \cdot \prod_{\substack{1\le j'\le r\\ j'\ne j_0}} (t_{j_0} - t_{j'})^{2e_{j'}} \cdot \prod_{\substack{P\in\mathcal{Q}\\ 1\le k\le \#\boldsymbol{\nu}(\eta)(P)}} b_{P,k}^{2e_{P,k}}$$

with $e_{j'} \le eps$, $e_{P,k} \le ep$, *degree in* w *bounded by* δ_w, *degree in* t_j *bounded by* $2epsr$ *and degree in* $(a_{P,k}, b_{P,k})$ *bounded by* $2ep$.

Proof. We simplify the notation by renaming $\boldsymbol{\eta}(\tau) = \boldsymbol{\eta}$ and $\boldsymbol{\nu}(\tau) = \boldsymbol{\nu}$. Consider the initial incompatibility

$$\downarrow \bigwedge_{\substack{P\in\mathcal{Q},\\ \mathrm{mu}(\eta_{j_0},P)>0}} P = 0, \bigwedge_{\substack{P\in\mathcal{Q},\\ \mathrm{mu}(\eta_{j_0},P)=0}} \mathrm{sign}(P) = \varepsilon_P,\ \mathcal{H} \downarrow_{\mathbf{K}[v]} \tag{28}$$

where $\mathcal{H}$ is a system of sign conditions in $\mathbf{K}[v]$.

Following the notation from Definition 4.3.2 and Definition 6.3.3, we apply to (28) the weak inference

$$\bigwedge_{\substack{P\in\mathcal{Q},\\ \mathrm{mu}(\eta_{j_0},P)>0}} P \equiv \mathrm{F}^{\mathrm{vmu}(\boldsymbol{\eta}(P)),\boldsymbol{\nu}(P)}(t_P, z_P),\ y = t_{j_0} \quad \vdash \quad \bigwedge_{\substack{P\in\mathcal{Q},\\ \mathrm{mu}(\eta_{j_0},P)>0}} P = 0.$$

By Lemma 2.1.8, we obtain

$$\begin{aligned} \downarrow \bigwedge_{\substack{P\in\mathcal{Q},\\ \mathrm{mu}(\eta_{j_0},P)>0}} & P \equiv \mathrm{F}^{\mathrm{vmu}(\boldsymbol{\eta}(P)),\boldsymbol{\nu}(P)}(t_P, z_P),\ y = t_{j_0}, \\ & \bigwedge_{\substack{P\in\mathcal{Q},\\ \mathrm{mu}(\eta_{j_0},P)=0}} \mathrm{sign}(P) = \varepsilon_P,\ \mathcal{H} \downarrow_{\mathbf{K}[v][t,a,b]} \end{aligned} \tag{29}$$

with the same monoid part, degree in w bounded by δ_w, degree in t_j and degree in $(a_{P,k}, b_{P,k})$ bounded by p.

Then we successively apply to (29) for $P \in \mathcal{Q}$ with $\mathrm{mu}(\eta_{j_0}, P) = 0$ the weak inferences

$$P \equiv \mathrm{F}^{\mathrm{vmu}(\boldsymbol{\eta}(P)),\boldsymbol{\nu}(P)}(t_P, z_P),\ \mathrm{sign}(\mathrm{F}^{\mathrm{vmu}(\boldsymbol{\eta}(P)),\boldsymbol{\nu}(P)}(t_P, z_P)) = \varepsilon_P \ \vdash \ \mathrm{sign}(P) = \varepsilon_P$$

and

$$\bigwedge_{1\le j'\le j_0-1} t_{j'} < y,\ \bigwedge_{j_0+1\le j'\le r} y < t_{j'},\ \bigwedge_{1\le k\le \#\boldsymbol{\nu}(P)} (y - a_{P,k})^2 + b_{P,k}^2 > 0 \ \vdash$$

$$\vdash \ \mathrm{sign}(\mathrm{F}^{\mathrm{vmu}(\boldsymbol{\eta}(P)),\boldsymbol{\nu}(P)}(t_P, z_P)) = \varepsilon_P,$$

and for $P \in \mathcal{Q}$ with $\mathrm{mu}(\eta_j, P) = 0$ and $1 \leq k \leq \#\boldsymbol{\nu}(P)$ the weak inferences

$$\begin{aligned} (y - a_{P,k})^2 \geq 0,\ b_{P,k}^2 > 0 \quad &\vdash \quad (y - a_{P,k})^2 + b_{P,k}^2 > 0, \\ &\vdash \quad (y - a_{P,k})^2 \geq 0, \\ b_{P,k} \neq 0 \quad &\vdash \quad b_{P,k}^2 > 0. \end{aligned}$$

By Lemmas 2.4.2, 2.1.2 (items 8, 3 and 4) and 2.1.7 we obtain

$$\downarrow \bigwedge_{P \in \mathcal{Q}} P \equiv \mathrm{F}^{\mathrm{vmu}(\boldsymbol{\eta}(P)),\boldsymbol{\nu}(P)}(t_P, z_P)), \quad y = t_{j_0},\ \bigwedge_{1 \leq j' \leq j_0 - 1} t_{j'} < y,\ \bigwedge_{j_0+1 \leq j' \leq r} y < t_{j'},\ \bigwedge_{\substack{P \in \mathcal{Q} \\ 1 \leq k \leq \#\boldsymbol{\nu}(P)}} b_{P,k} \neq 0,\ \mathcal{H} \downarrow_{\mathbf{K}[v][t,a,b]} \tag{30}$$

with monoid part

$$S \cdot \prod_{\substack{1 \leq j' \leq r, \\ j' \neq j_0}} (y - t_{j'})^{2e_{j'}} \cdot \prod_{\substack{P \in \mathcal{Q} \\ 1 \leq k \leq \#\boldsymbol{\nu}(P)}} b_{P,k}^{2e_{P,k}}$$

with $e_{j'} \leq eps$, $e_{P,k} \leq ep$, degree in w bounded by δ_w, degree in t_j bounded by $2eps$ (taking into account that $\mathrm{mu}(\eta_{j_0}, P_0) > 0$ for at least one $P_0 \in \mathcal{Q}$) and degree in $(a_{P,k}, b_{P,k})$ bounded by $2ep$ (taking into account that for each $P \in \mathcal{Q}$, either $\mathrm{mu}(\eta_{j_0}, P) > 0$ or $\mathrm{mu}(\eta_{j_0}, P) = 0$).

Finally, we successively apply to (30) for $1 \leq j' \leq j_0 - 1$ the weak inference

$$t_{j'} < t_{j_0},\ t_{j_0} = y \quad \vdash \quad t_{j'} < y$$

and for $j + 1 \leq j' \leq r$ the weak inference

$$y = t_{j_0},\ t_{j_0} < t_{j'} \quad \vdash \quad y < t_{j'}.$$

By Lemma 2.1.7 we obtain

$$\downarrow \bigwedge_{P \in \mathcal{Q}} P \equiv \mathrm{F}^{\mathrm{vmu}(\boldsymbol{\eta}(P)),\boldsymbol{\nu}(P)}(t_P, z_P)), \quad y = t_{j_0},\ \bigwedge_{1 \leq j' \leq j_0 - 1} t_{j'} < t_{j_0},\ \bigwedge_{j_0+1 \leq j' \leq r} t_{j_0} < t_{j'},\ \bigwedge_{\substack{P \in \mathcal{Q} \\ 1 \leq k \leq \#\boldsymbol{\nu}(P)}} b_{P,k} \neq 0,\ \mathcal{H} \downarrow_{\mathbf{K}[v][t,a,b]}$$

with monoid part

$$S \cdot \prod_{\substack{1 \leq j' \leq r, \\ j' \neq j_0}} (t_{j_0} - t_{j'})^{2e_{j'}} \cdot \prod_{\substack{P \in \mathcal{Q} \\ 1 \leq k \leq \#\boldsymbol{\nu}(P)}} b_{P,k}^{2e_{P,k}}$$

with degree in w bounded by δ_w, degree in t_j bounded by $2epsr$ and degree in $(a_{P,k}, b_{P,k})$ bounded by $2ep$, which serves as the final incompatibility. □

Lemma 6.4.7 *Let $p \geq 1$, $\mathcal{Q}$ be a family of s polynomials in $\mathbf{K}[u][y] \setminus \mathbf{K}$, monic in the variable y with $\deg_y P \leq p$ for every $P \in \mathcal{Q}$, τ be a realizable sign condition on $\mathrm{Elim}(\mathcal{Q})$, $\boldsymbol{\eta}(\tau) = [\eta_1, \dots, \eta_r]$ with $r > 1$ and $1 \leq j_0 \leq r - 1$. Then, defining $\varepsilon_P = (-1)^{\sum_{j_0+1 \leq j' \leq r} \mathrm{mu}(\eta_{j'}, P)}$,*

$$\exists (t, z)\ [\ \mathrm{OFact}(\mathcal{Q})^{\boldsymbol{\eta}(\tau),\boldsymbol{\nu}(\tau)}(t, z),\ t_{j_0} < y,\ y < t_{j_0+1}\ ] \quad \vdash \quad \bigwedge_{P \in \mathcal{Q}} \mathrm{sign}(P) = \varepsilon_P$$

where $t = (t_1, \ldots, t_r)$, $z = (z_P)_{P \in \mathcal{Q}}$ and $z_P = (z_{P,1}, \ldots, z_{P,\#\boldsymbol{\nu}(\tau)(P)})$.

Suppose we have an initial incompatibility in variables $v \supset (u, y)$ with monoid part

$$S \cdot \prod_{P \in \mathcal{Q}} P^{2e_P}$$

with $e_P \leq e \in \mathbb{N}_*$ and degree in w bounded by δ_w for some set of variables $w \subset v$. Then, the final incompatibility has monoid part

$$S \cdot (y - t_{j_0})^{2e_{j_0}} \cdot (y - t_{j_0+1})^{2e_{j_0+1}} \cdot \prod_{1 \leq j' \leq j_0 - 1} (t_{j_0} - t_{j'})^{2e_{j'}} \cdot \prod_{j_0+2 \leq j' \leq r} (t_{j_0+1} - t_{j'})^{2e_{j'}} \cdot \prod_{\substack{P \in \mathcal{Q} \\ 1 \leq k \leq \#\boldsymbol{\nu}(P)}} b_{P,k}^{2e_{P,k}},$$

with $e_j \leq eps$, $e_{P,k} \leq ep$, degree in w bounded by δ_w, degree in t_j bounded by $2epsr$ and degree in $(a_{P,k}, b_{P,k})$ bounded by $2ep$.

Proof. We simplify the notation by renaming $\boldsymbol{\eta}(\tau) = \boldsymbol{\eta}$ and $\boldsymbol{\nu}(\tau) = \boldsymbol{\nu}$. Consider the initial incompatibility

$$\downarrow \bigwedge_{P \in \mathcal{Q}} \operatorname{sign}(P) = \varepsilon_P,\ \mathcal{H} \downarrow_{\mathbf{K}[v]} \tag{31}$$

where $\mathcal{H}$ is a system of sign conditions in $\mathbf{K}[v]$.

We successively apply to (31) for $P \in \mathcal{Q}$ the weak inferences

$$P \equiv \mathrm{F}^{\mathrm{vmu}(\boldsymbol{\eta}(P)), \boldsymbol{\nu}(P)}(t_P, z_P)),\ \operatorname{sign}\Big(\mathrm{F}^{\mathrm{vmu}(\boldsymbol{\eta}(P)), \boldsymbol{\nu}(P)}(t_P, z_P))\Big) = \varepsilon_P \ \vdash \ \operatorname{sign}(P) = \varepsilon_P$$

and

$$\bigwedge_{1 \leq j' \leq j_0} t_{j'} < y, \quad \bigwedge_{j_0+1 \leq j' \leq r} y < t_{j'}, \quad \bigwedge_{1 \leq k \leq \#\boldsymbol{\nu}(P)} (y - a_{P,k})^2 + b_{P,k}^2 > 0 \ \vdash$$
$$\vdash \ \operatorname{sign}(\mathrm{F}^{\mathrm{vmu}(\boldsymbol{\eta}(P)), \boldsymbol{\nu}(P)}(t_P, z_P))) = \varepsilon_P,$$

and for $P \in \mathcal{Q}$ and $1 \leq k \leq \#\boldsymbol{\nu}(P)$ the weak inferences

$$\begin{aligned} (y - a_{P,k})^2 \geq 0,\ b_{P,k}^2 > 0 \quad &\vdash \quad (y - a_{P,k})^2 + b_{P,k}^2 > 0, \\ &\vdash \quad (y - a_{P,k})^2 \geq 0, \\ b_{P,k} \neq 0 \quad &\vdash \quad b_{P,k}^2 > 0. \end{aligned}$$

By Lemmas 2.4.2, 2.1.2 (items 8, 3 and 4) and 2.1.7 we obtain

$$\begin{aligned} &\downarrow \bigwedge_{P \in \mathcal{Q}} P \equiv \mathrm{F}^{\mathrm{vmu}(\boldsymbol{\eta}(P)), \boldsymbol{\nu}(P)}(t_P, z_P), \\ \bigwedge_{1 \leq j' \leq j_0} t_{j'} < y, \quad &\bigwedge_{j_0+1 \leq j' \leq r} y < t_{j'}, \quad \bigwedge_{\substack{P \in \mathcal{Q} \\ 1 \leq k \leq \#\boldsymbol{\nu}(P)}} b_{P,k} \neq 0,\ \mathcal{H} \downarrow_{\mathbf{K}[v][t,a,b]} \end{aligned} \tag{32}$$

with monoid part

$$S \cdot \prod_{1 \leq j \leq r} (y - t_j)^{2e_j} \cdot \prod_{\substack{P \in \mathcal{Q} \\ 1 \leq k \leq \#\boldsymbol{\nu}(P)}} b_{P,k}^{2e_{P,k}}$$

with $e_j \leq eps$, $e_{P,k} \leq ep$, degree in w bounded by δ_w, degree in t_j bounded by $2eps$ and degree in $(a_{P,k}, b_{P,k})$ bounded by $2ep$.

Finally, we successively apply to (32) for $1 \leq j' \leq j_0 - 1$ the weak inferences

$$t_{j'} < t_{j_0},\ t_{j_0} \leq y \quad \vdash \quad t_{j'} < y,$$

$$t_{j_0} < y \quad \vdash \quad t_{j_0} \leq y$$

and for $j_0 + 2 \leq j' \leq r$ the weak inferences

$$y \leq t_{j_0+1},\ t_{j_0+1} < t_{j'} \quad \vdash \quad y < t_{j'},$$

$$y < t_{j_0+1} \quad \vdash \quad y \leq t_{j_0+1}.$$

By Lemmas 2.1.7 and 2.1.2 (item 1) we obtain

$$\downarrow \bigwedge_{P \in \mathcal{Q}} P \equiv \mathrm{F}^{\mathrm{vmu}(\boldsymbol{\eta}(P)),\boldsymbol{\nu}(P)}(t_P, z_P),$$
$$t_{j_0} < y,\ y < t_{j_0+1},\ \bigwedge_{1 \leq j' \leq j_0 - 1} t_{j'} < t_{j_0},\ \bigwedge_{j_0+2 \leq j' \leq r} t_{j_0+1} < t_{j'},\ \bigwedge_{\substack{P \in \mathcal{Q} \\ 1 \leq k \leq \#\boldsymbol{\nu}(P)}} b_{P,k} \neq 0,\ \mathcal{H}\downarrow_{\mathbf{K}[v][t,a,b]}$$

with monoid part

$$S \cdot (y - t_{j_0})^{2e_{j_0}} \cdot (y - t_{j_0+1})^{2e_{j_0+1}} \cdot \prod_{1 \leq j' \leq j_0 - 1} (t_{j_0} - t_{j'})^{2e_{j'}} \cdot \prod_{j_0+2 \leq j' \leq r} (t_{j_0+1} - t_{j'})^{2e_{j'}} \cdot \prod_{\substack{P \in \mathcal{Q} \\ 1 \leq k \leq \#\boldsymbol{\nu}(P)}} b_{P,k}^{2e_{P,k}},$$

degree in w bounded by δ_w, degree in t_j bounded by $2epsr$ and degree in $(a_{P,k}, b_{P,k})$ bounded by $2ep$, which serves as the final incompatibility. □

We state below two more lemmas corresponding to the other cases needed to analyze the whole partition of the real line given by the set of roots. We omit their proofs since they are very similar to the proof of Lemma 6.4.7.

Lemma 6.4.8 *Let $p \geq 1$, $\mathcal{Q}$ be a family of s polynomials in $\mathbf{K}[u][y] \setminus \mathbf{K}$, monic in the variable y with $\deg_y P \leq p$ for every $P \in \mathcal{Q}$, τ be a realizable sign condition on* Elim($\mathcal{Q}$) *and $\boldsymbol{\eta}(\tau) = [\eta_1, \dots, \eta_r]$ with $r \geq 1$. Then*

$$\exists (t, z)\ [\ \mathrm{OFact}(\mathcal{Q})^{\boldsymbol{\eta}(\tau),\boldsymbol{\nu}(\tau)}(t, z),\ t_r < y\ ] \quad \vdash \quad \bigwedge_{P \in \mathcal{Q}} P > 0$$

where $t = (t_1, \dots, t_r)$, $z = (z_P)_{P \in \mathcal{Q}}$ and $z_P = (z_{P,1}, \dots, z_{P,\#\boldsymbol{\nu}(\tau)(P)})$.

Suppose we have an initial incompatibility in variables $v \supset (u, y)$ with monoid part

$$S \cdot \prod_{P \in \mathcal{Q}} P^{2e_P}$$

with $e_P \leq e \in \mathbb{N}_*$ and degree in w bounded by δ_w for some set of variables $w \subset v$. Then, the final incompatibility has monoid part

$$S \cdot (y - t_r)^{2e_r} \cdot \prod_{1 \leq j \leq r-1} (t_r - t_j)^{2e_j} \cdot \prod_{\substack{P \in \mathcal{Q} \\ 1 \leq k \leq \#\boldsymbol{\nu}(P)}} b_{P,k}^{2e_{P,k}},$$

with $e_j \leq eps$, $e_{P,k} \leq ep$, degree in w bounded by δ_w, degree in t_j bounded by $2epsr$ and degree in $(a_{P,k}, b_{P,k})$ bounded by $2ep$.

Lemma 6.4.9 *Let $p \geq 1$, $\mathcal{Q}$ be a family of s polynomials in $\mathbf{K}[u][y] \setminus \mathbf{K}$, monic in the variable y with $\deg_y P \leq p$ for every $P \in \mathcal{Q}$, be τ a realizable sign condition on $\mathrm{Elim}(\mathcal{Q})$ and $\boldsymbol{\eta}(\tau) = [\eta_1, \dots, \eta_r]$ with $r \geq 1$. Then*

$$\exists (t, z) \ [\ \mathrm{OFact}(\mathcal{Q})^{\boldsymbol{\eta}(\tau), \boldsymbol{\nu}(\tau)}(t, z),\ y < t_1\ ] \quad \vdash \quad \bigwedge_{P \in \mathcal{Q}} \mathrm{sign}(P) = (-1)^{\sum_{1 \leq j \leq r} \mathrm{mu}(\eta_j, P)}$$

where $t = (t_1, \dots, t_r)$, $z = (z_P)_{P \in \mathcal{Q}}$ and $z_P = (z_{P,1}, \dots, z_{P, \#\boldsymbol{\nu}(\tau)(P)})$.

Suppose we have an initial incompatibility in variables $v \supset (u, y)$ with monoid part

$$S \cdot \prod_{P \in \mathcal{Q}} P^{2e_P}$$

with $e_P \leq e \in \mathbb{N}_*$ and degree in w bounded by δ_w for some set of variables $w \subset v$. Then, the final incompatibility has monoid part

$$S \cdot (y - t_1)^{2e_1} \cdot \prod_{2 \leq j \leq r} (t_1 - t_j)^{2e_j} \prod_{\substack{P \in \mathcal{Q} \\ 1 \leq k \leq \#\boldsymbol{\nu}(P)}} b_{P,k}^{2e_{P,k}},$$

with $e_j \leq eps$, $e_{P,k} \leq ep$, degree in w bounded by δ_w, degree in t_j bounded by $2epsr$ and degree in $(a_{P,k}, b_{P,k})$ bounded by $2ep$.

We introduce an auxiliary definition.

Definition 6.4.10 *Let τ be a relizable sign condition on $\mathrm{Elim}(\mathcal{Q})$ and $\boldsymbol{\eta}(\tau) = [\eta_1, \dots, \eta_r]$. If $\vartheta \in \mathbf{R}^k$, $\theta \in \mathbf{R}^r, \alpha \in \mathbf{R}^s, \beta \in \mathbf{R}^s$ with $s = \sum_{P \in \mathcal{Q}} \#\boldsymbol{\nu}(\tau)(P)$ verifies $\mathrm{sign}(\mathrm{Elim}(\mathcal{Q})(\vartheta)) = \tau$ and $\mathrm{OFact}(\mathcal{Q}(\vartheta))^{\boldsymbol{\eta}(\tau), \boldsymbol{\nu}(\tau)}(\theta, \alpha + i\beta)$, we denote σ_j the sign condition $\mathrm{sign}(\mathcal{Q}(\vartheta, \theta_j))$ for $1 \leq j \leq r$ and $\sigma_{(j-1,j)}$ the sign condition $\mathrm{sign}(\mathcal{Q})(\iota)$ for any $\iota \in (\theta_{j-1}, \theta_j)$ for $1 \leq j \leq r+1$, where $\theta_0 = -\infty$ and $\theta_{r+1} = +\infty$.*

Proposition 6.4.11 *Let $p \geq 1$, $\mathcal{Q}$ be a family of s polynomials in $\mathbf{K}[u][y] \setminus \mathbf{K}$, monic in the variable y with $\deg_y P \leq p$ for every $P \in \mathcal{Q}$, τ be a realizable sign condition on $\mathrm{Elim}(\mathcal{Q})$, $\boldsymbol{\eta}(\tau) = [\eta_1, \dots, \eta_r]$, $t = (t_1, \dots, t_r)$ and $z = (z_P)_{P \in \mathcal{Q}}$ where $z_P = (z_{P,1}, \dots, z_{P, \#\boldsymbol{\nu}(\tau)(P)})$. Then*

$$\exists\, (t, z) \ [\ \mathrm{OFact}(\mathcal{Q})^{\boldsymbol{\eta}(\tau), \boldsymbol{\nu}(\tau)}(t, z)\,] \quad \vdash \quad \bigvee_{\sigma \in \mathrm{SIGN}(\mathcal{Q}\,|\tau)} \mathrm{sign}(\mathcal{Q}) = \sigma.$$

Suppose we have for $\sigma = \sigma_{(0,1)}, \sigma_1, \dots, \sigma_{(r,r+1)}$ an initial incompatibility in variables $v \supset (u, y)$ with monoid part

$$S_\sigma \cdot \prod_{\substack{P \in \mathcal{Q}, \\ \sigma(P) \neq 0}} P^{2e_{P,\sigma}}$$

with $e_{P,\sigma} \leq e \in \mathbb{N}_*$ and degree in w bounded by δ_w for some subset of variables $w \subset v$. Then the final incompatibility has monoid part

$$\prod_{1 \leq j \leq r+1} S_{\sigma_{(j-1,j)}} \cdot \prod_{1 \leq j \leq r} S_{\sigma_j}^{e_j} \cdot \prod_{1 \leq j < j' \leq r} (t_{j'} - t_j)^{2e_{j,j'}} \cdot \prod_{\substack{P \in \mathcal{Q} \\ 1 \leq k \leq \#\boldsymbol{\nu}(\tau)(P)}} b_{P,k}^{2e_{P,k}}$$

with $e_j \leq 4eps$, $e_{j,j'} \leq 2eps + 8(eps)^2$, $e_{P,k} \leq (ps+1)ep + 4e^2p^3s^2$, degree in w bounded by $(ps + 1 + 4ep^2s^2)\delta_w$, degree in t_j bounded by $2(ps + 1 + 4ep^2s^2)ep^2s^2$ and degree in $(a_{P,k}, b_{P,k})$ bounded by $2(ps + 1 + 4ep^2s^2)ep$.

Proof. We consider first the case that at least one polynomial in $\mathcal{Q}$ has a real root, this is to say, $r > 0$. In this case, the proof is done by applying to the initial incompatibilities the weak inferences in Lemmas 6.4.6, 6.4.7, 6.4.8 and 6.4.9 and Proposition 6.4.5.

In the case that every polynomial in $\mathcal{Q}$ has no real root, this is to say, $r = 0$, the set of variables $t = (t_1, \dots, t_r)$ is actually empty. Moreover, it is clear that $\mathrm{SIGN}(\mathcal{Q}\,|\tau)$ has only the element $1^{\mathcal{Q}}$, since every P is monic and without real roots. We omit the proof since it is very easy. □

We are finally ready for the proof of the main result of the section.

Proof of Theorem 6.4.4. Consider the initial incompatibilities

$$\downarrow \mathrm{sign}(\mathcal{Q}) = \sigma,\ \mathcal{H} \downarrow \tag{33}$$

where $\mathcal{H}$ is a system of sign conditions in $\mathbf{K}[v]$.

We apply to (33) the weak inference

$$\exists\,(t,z)\ [\ \mathrm{OFact}(\mathcal{Q})^{\boldsymbol{\eta}(\tau),\boldsymbol{\nu}(\tau)}(t,z)\,] \quad \vdash \quad \bigvee_{\sigma \in \mathrm{SIGN}(\mathcal{Q}\,|\tau)} \mathrm{sign}(\mathcal{Q}) = \sigma.$$

By Proposition 6.4.11 we obtain

$$\Big\downarrow \mathrm{OFact}(\mathcal{Q})^{\boldsymbol{\eta}(\tau),\boldsymbol{\nu}(\tau)}(t,z),\ \mathcal{H} \Big\downarrow_{\mathbf{K}[v][t,a,b]}, \tag{34}$$

where $\boldsymbol{\eta}(\tau) = [\eta_1, \dots, \eta_r]$, $t = (t_1, \dots, t_r)$, $z = (z_P)_{P \in \mathcal{Q}}$ with $z_P = (z_{P,1}, \dots, z_{P,\#\boldsymbol{\nu}(\tau)(P)})$, with monoid part

$$\prod_{1 \le j \le r+1} S_{\sigma_{(j-1,j)}} \cdot \prod_{1 \le j \le r} S_{\sigma_j}^{e_j} \cdot \prod_{1 \le j < j' \le r} (t_{j'} - t_j)^{2e_{j,j'}} \cdot \prod_{\substack{P \in \mathcal{Q} \\ 1 \le k \le \#\boldsymbol{\nu}(\tau)(P)}} b_{P,k}^{2e_{P,k}}$$

with $e_j \le 4eps$, $e_{j,j'} \le 2eps + 8(eps)^2$, $e_{P,k} \le (ps+1)ep + 4e^2p^3s^2$, degree in w bounded by $(ps + 1 + 4ep^2s^2)\delta_w$, degree in t_j bounded by $2(ps + 1 + 4ep^2s^2)ep^2s^2$ and degree in $(a_{P,k}, b_{P,k})$ bounded by $2(ps + 1 + 4ep^2s^2)ep$.

Finally we apply to (34) the weak inference

$$\mathrm{sign}(\mathrm{Elim}(\mathcal{Q})) = \tau \quad \vdash \quad \exists(t,z)\ [\ \mathrm{OFact}(\mathcal{Q})^{\boldsymbol{\eta}(\tau),\boldsymbol{\nu}(\tau)}(t,z)\ ].$$

By Theorem 6.3.6 (Fixing the Ordered List of the Roots as a weak existence), we obtain

$$\downarrow \mathrm{sign}(\mathrm{Elim}(\mathcal{Q})) = \tau,\ \mathcal{H} \downarrow$$

with monoid part

$$\prod_{\sigma \in \mathrm{SIGN}(\mathcal{Q}\,|\tau)} S_\sigma^{h_\sigma} \cdot \prod_{\substack{H \in \mathrm{Elim}(\mathcal{Q}), \\ \tau(H) \ne 0}} H^{2h'_H}$$

with

$$h_\sigma, h'_H \le 4eps\mathrm{g}_6\{p, s, 2eps + 8(eps)^2, (ps+1)ep + 4e^2p^3s^2, 1\} \max\{8e^2p^3s^3, \tilde{\mathrm{g}}_{H,3}\{p\}\},$$

and degree in w bounded by

$$\begin{aligned}
& \mathrm{g}_6\{p, s, 2eps + 8(eps)^2, (ps+1)ep + 4e^2p^3s^2, 1\}\cdot \\
\cdot \quad & \Big(\max\{2^{ps(s-1)}(6ep^2s^2\delta_w + 24e^2p^4s^4 \deg_w \mathcal{Q}), \tilde{\mathrm{g}}_{H,3}\{p\} \deg_w \mathcal{Q}\} + \\
& \max\{2^{ps(s-1)}56e^2p^4s^4, \tilde{\mathrm{g}}_{H,3}\{p\}\} \deg_w \mathcal{Q}\Big) \leq \\
\leq \quad & 2^{ps(s-1)+1}e^2s^4\tilde{\mathrm{g}}_{H,3}\{p\}\mathrm{g}_6\{p, s, 2eps + 8(eps)^2, (ps+1)ep + 4e^2p^3s^2, 1\} \max\{\delta_w, \deg_w \mathcal{Q}\},
\end{aligned}$$

which serves as the final incompatibility, using Lemma 6.4.3. □

7 Proof of the main theorems

In this section we prove Theorem 1.4.2 (Positivstellensatz with elementary recursive degree estimates) and Theorem 1.4.4 (Hilbert 17-th problem with elementary recursive degree estimates), which are the main results of this paper. The proof proceeds by successive elimination of the variables, using at each stage Theorem 6.4.4 (Elimination of One Variable as a weak inference). This is the only result from previous sections which is used in this section.

First, we introduce some notation, new auxiliary functions and a final auxiliary lemma.

Notation 7.0.1 *For* $\mathcal{Q} \subset \mathbf{K}[x_1, \ldots, x_k]$, $\mathrm{SIGN}(\mathcal{Q})$ *is the set of realizable sign conditions on* $\mathcal{Q}$ *in* $\mathbf{R}^k$.

Note that by Theorem 6.4.1 (Elimination of One Variable),

$$\mathrm{SIGN}(\mathcal{Q}) = \bigcup_{\tau \in \mathrm{SIGN}(\mathrm{Elim}(\mathcal{Q}))} \mathrm{SIGN}(\mathcal{Q}\,|\tau).$$

Definition 7.0.2

- *Let* $\mathrm{g}_8 : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{R}$,

$$\mathrm{g}_8\{d, s, k, i\} =$$

$$= \mathrm{g}_7 \left\{ 4^{\frac{4^{k-i}-1}{3}} d^{4^{k-i}}, s^{2^{k-i}} \max\{2,d\}^{(16^{k-i}-1)\mathrm{bit}\{d\}}, 2^{2^{\left(2^{\max\{2,d\}^{4^{k-i}}}+s^{2^{k-i}}\max\{2,d\}^{16^{k-i}\mathrm{bit}(d)}\right)}} \right\}.$$

- *Let* $\mathrm{g}_9 : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{R}$,

$$\mathrm{g}_9\{d, k, i\} = \mathrm{g}_7 \left\{ 4^{\frac{4^{k-i}-1}{3}} d^{4^{k-i}}, d^{(16^{k-i}-1)\mathrm{bit}\{d\}}, 2^{\left(2^{2^{d^{4^{k-i}}}}-2\right)} \right\}.$$

Technical Lemma 7.0.3

1. *For every* $d, s, k, i \in \mathbb{N}_*$ *with* $1 \leq i \leq k$,

$$\mathrm{g}_8\{d, s, k, i\} \cdot 2^{2^{\left(2^{\max\{2,d\}^{4^{k-i}}}+s^{2^{k-i}}\max\{2,d\}^{16^{k-i}\mathrm{bit}(d)}\right)}} \leq$$

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

2. *For every* $d, k, i \in \mathbb{N}_*$ *with* $1 \leq i \leq k$ *and* $d \geq 2$,

$$\mathrm{g}_9\{d, k, i\} \cdot 2^{\left(2^{2^{d^{4^{k-i}}}}-2\right)} \leq 2^{\left(2^{2^{d^{4^{k-i+1}}}}-2\right)}.$$

Proof. See Section 8. □

Given a set of polynomials $\mathcal{P}$ and a polynomial ℓ, we denote by $\mathcal{P} \circ \ell$ the set of compositions $\{P \circ \ell \mid P \in \mathcal{P}\}$. Similarly, if $\mathcal{F} = [\mathcal{F}_{\neq}, \mathcal{F}_{\geq}, \mathcal{F}_{=}]$ is a system of sign conditions, we denote by $\mathcal{F} \circ \ell$ the system $[\mathcal{F}_{\neq} \circ \ell, \mathcal{F}_{\geq} \circ \ell, \mathcal{F}_{=} \circ \ell]$.

We are ready now to prove our main theorems.

Proof of Theorem 1.4.2. We define $\mathcal{P}_k$ as $|\mathcal{F}|$ (see Notation 1.3.1), note that without loss of generality we can assume $\mathcal{F} \subset \mathbf{K}[x] \setminus \mathbf{K}$. For $i = k, \ldots, 1$, we define inductively finite families $\mathcal{Q}_i \subset \mathbf{K}[x_1, \ldots, x_i]$ and $\mathcal{P}_{i-1} \subset \mathbf{K}[x_1, \ldots, x_{i-1}]$. Let $\ell_i : \mathbf{K}[x_1, \ldots, x_i] \to \mathbf{K}[x_1, \ldots, x_i]$ be a linear change of variables such that for every polynomial $P \in \mathcal{P}_i$, $P \circ \ell_i(x_1, \ldots, x_i)$ is quasimonic in the variable x_i; we define

- $\mathcal{Q}_i$ as the family obtained by dividing each polynomial $P \circ \ell_i(x_1, \ldots, x_i)$ in $\mathcal{P}_i \circ \ell_i$ by its leading coefficient in the variable x_i,
- $\mathcal{P}_{i-1} = \mathrm{Elim}(\mathcal{Q}_i) \setminus \mathbf{K}$, considering $(x_1, \ldots, x_{i-1})$ as parameters and x_i as the main variable.

Following Remark 6.3.7, it can be easily proved by induction that for $i = k, \ldots, 1$,

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

Also using Remark 6.3.7, we will prove that

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

Indeed, $\#\mathcal{P}_k = s$ and for $i = k, \ldots, 2$,

$$\begin{aligned}
\#\mathcal{P}_{i-1} &\leq 4s^{2^{k-i+1}} \max\{2, d\}^{2(16^{k-i}-1)\mathrm{bit}\{d\}} (4^{\frac{4^{k-i}-1}{3}} d^{4^{k-i}})^{\mathrm{bit}\{4^{\frac{4^{k-i}-1}{3}} d^{4^{k-i}}\}+1} \leq \\
&\leq s^{2^{k-i+1}} \max\{2, d\}^{2+2(16^{k-i}-1)\mathrm{bit}\{d\}+(2\frac{4^{k-i}-1}{3}+4^{k-i})(2\frac{4^{k-i}-1}{3}+4^{k-i}\mathrm{bit}\{d\}+1)} \leq \\
&\leq s^{2^{k-(i-1)}} \max\{2, d\}^{(16^{k-(i-1)}-1)\mathrm{bit}\{d\}}.
\end{aligned}$$

For $1 \leq i \leq k$, we denote by $\ell_{[k,i]}$ the polynomial $\ell_k \circ \cdots \circ \ell_i$. Let us show by induction in $i = k, \ldots, 0$, that for every realizable sign condition σ on $\mathcal{P}_i$ we have an incompatibility

$$\downarrow \mathrm{sign}(\mathcal{P}_i) = \sigma, \ \mathcal{F} \circ \ell_{[k,i+1]} \downarrow \tag{1}$$

with monoid part

$$\prod_{H \in \mathcal{P}_i,\, \sigma(H) \neq 0} H^{2e_H}$$

with e_H bounded by

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

for $H \in \mathrm{Elim}(\mathcal{P}_i)$ with $\sigma(H) \neq 0$ and degree bounded by

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

For $i = k$, $|\mathcal{F}|$ and $\mathcal{P}_i$ are the same sets of polynomials. Moreover, for every strict sign condition σ which is realizable for $|\mathcal{F}|$, there must be a polynomial $P \in |\mathcal{F}|$ such that $\sigma(P)$ is incompatible with the system of sign conditions $\mathcal{F}$. It is easy to check that, in all possible cases, the algebraic identity

$$P^2 - P^2 = 0$$

serves as the corresponding incompatibility (see Example 1.2.5). So $e_H \leq 1$ for $H \in \mathcal{P}_i$ with $\sigma(H) \neq 0$ and the degree of the incompatibility (1) is bounded by $2d$.

Suppose now that the induction hypothesis holds for some value of $i > 0$ and let τ be a realizable strict sign condition on $\mathcal{P}_{i-1}$. For every realizable strict sign condition σ on $\mathcal{P}_i$ we compose the incompatibility we have already by induction hypothesis with ℓ_i to obtain an incompatibility for

$$\downarrow \operatorname{sign}(\mathcal{P}_i \circ \ell_i) = \sigma,\ \mathcal{F} \circ \ell_{[k,i]} \downarrow$$

with the same bounds for the degree and the exponents in the monoid part as (1). We denote σ' the strict sign condition on $\mathcal{Q}_i$ obtained from a strict σ on $\mathcal{P}_i \circ \ell_i$ by replacing $>$ for $<$ and vice versa when the leading coefficient of the corresponding polynomial in $\mathcal{P}_i \circ \ell_i$ is negative. It is clear that

$$\operatorname{SIGN}(\mathcal{Q}_i) = \{\sigma' \mid \sigma \in \operatorname{SIGN}(\mathcal{P}_i \circ \ell_i)\}.$$

So, we have for every realizable strict sign condition σ' on $\mathcal{Q}_i$ an incompatibility

$$\downarrow \operatorname{sign}(\mathcal{Q}_i) = \sigma',\ \mathcal{F} \circ \ell_{[k,i]} \downarrow \tag{2}$$

with the same bounds as (1). We apply to (2) for every $\sigma' \in \operatorname{SIGN}(\mathcal{Q}_i \,|\tau)$ the weak inference

$$\operatorname{sign}(\mathcal{P}_{i-1}) = \tau \quad \vdash \bigvee_{\sigma' \in \operatorname{SIGN}(\mathcal{Q}_i \,|\tau)} \operatorname{sign}(\mathcal{Q}_i) = \sigma'$$

of Theorem 6.4.4 (Elimination of One Variable as a weak inference). We obtain in this way an incompatibility

$$\downarrow \operatorname{sign}(\mathcal{P}_{i-1}) = \tau,\ \mathcal{F} \circ \ell_{[k,i]} \downarrow$$

with monoid part

$$\prod_{H \in \mathcal{P}_{i-1},\, \sigma(H) \neq 0} H^{2e'_H}$$

with e'_H bounded by $\mathrm{g}_8\{d, s, k, i\}$ and degree bounded by

$$\mathrm{g}_8\{d, s, k, i\} \cdot 2^{2^{\left(2^{\max\{2,d\}^{4^{k-i}}} + s^{2^{k-i}} \max\{2,d\}^{16^{k-i}\operatorname{bit}(d)}\right)}}.$$

The claim follows then by Lemma 7.0.3 (item 1).

Since $\mathcal{P}_0 \subset \mathbf{K}$, after the inductive procedure described above is finished, we obtain a single incompatibility

$$\downarrow \mathcal{F} \circ \ell_{[k,1]} \downarrow$$

with degree bounded by

$$2^{2^{\left(2^{\max\{2,d\}^{4^{k}}} + s^{2^{k}} \max\{2,d\}^{16^{k}\operatorname{bit}(d)}\right)}}.$$

Our result follows then by composing this incompatibility with $\ell_{[k,1]}^{-1}$ which does not change the degree bound. $\square$

Proof of Theorem 1.4.4. The sketch of the proof is the following: first we proceed as in the proof of Theorem 1.4.2 (Positivstellensatz with elementary recursive degree estimates) but obtaining a slightly better bound which holds for the particular case when the original system has only one polynomial. Then we proceed as in the proof of Theorem 1.2.11 (Improved Hilbert 17-th problem).

The initial system $\mathcal{F}$ we consider is

$$P \neq 0, -P \geq 0$$

and the initial incompatibility between $\mathcal{F}$ and $P \geq 0$ is

$$P^2 - P^2 = 0.$$

Note that since P is nonnegative in $\mathbf{R}^k$, d is even and therefore $d \geq 2$.

Proceeding as in the proof of Theorem 1.4.2 and using Lemma 7.0.3 (item 2) (instead of Lemma 7.0.3 (item 1)), we prove that for $i = k, \dots, 0$, for every realizable strict sign condition σ on $\mathcal{P}_i$ we have an incompatibility

$$\downarrow \operatorname{sign}(\mathcal{P}_i) = \sigma, \ \mathcal{F} \circ \ell_{[k,i+1]} \downarrow$$

with monoid part

$$\prod_{H \in \mathcal{P}_i,\, \sigma(H) \neq 0} H^{2e_H}$$

with e_H bounded by

$$2^{\left(2^{2^{d^{4^{k-i}}}} - 2\right)}$$

for $H \in \operatorname{Elim}(\mathcal{P}_i)$ with $\sigma(H) \neq 0$ and degree bounded by

$$2^{\left(2^{2^{d^{4^{k-i}}}} - 2\right)}.$$

After finishing the inductive procedure and composing with $\ell_{[k,1]}^{-1}$ as before, we obtain a final incompatibility of $\mathcal{F}$,

$$\downarrow P \neq 0, -P \geq 0 \downarrow,$$

of type

$$P^{2e} + N_1 - N_2 P = 0$$

with $e \in \mathbb{N}$, $N_1, N_2 \in \mathscr{N}(\emptyset)$ and degree bounded by

$$2^{\left(2^{2^{d^{4^{k}}}} - 2\right)}.$$

From this we deduce, as in the proof of Theorem 1.2.11 (Improved Hilbert 17-th problem),

$$P = \frac{N_2 P^2}{P^{2e} + N_1} = \frac{N_2 P^2 (P^{2e} + N_1)}{(P^{2e} + N_1)^2}. \tag{3}$$

After expanding the numerator in (3) we obtain an expression

$$P = \sum_i \omega_i \frac{P_i^2}{Q^2}$$

with $\omega_i \in \mathbf{K}, \omega_i > 0, P_i \in \mathbf{K}[x], Q = P^{2e} + N_1 \in \mathbf{K}[x]$ and

$$\deg P_i^2 \leq 2^{\left(2^{2^{d^{4^k}}}-1\right)} + d \leq 2^{2^{2^{d^{4^k}}}}$$

for every i and

$$\deg Q^2 \leq 2^{\left(2^{2^{d^{4^k}}}-1\right)} \leq 2^{2^{2^{d^{4^k}}}}.$$

$\square$

8 Annex

Here we include the proof of technical lemmas from the previous sections.

Proof of Technical Lemma 4.1.7. We first prove item 1.

$$3\mathrm{g}_1\{p-1,p\} = 3\cdot 2^{3\cdot 2^{p-1}}p^p \le 2^{3\cdot 2^{p-1}+p^2} \le 2^{2^{3\frac{p}{2}}} = \mathrm{g}_2\{p\}.$$

Now we prove item 2. We check separately that the inequality holds for $p=4$ and $p=6$ and we suppose that $p\ge 8$. Then we have

$$\frac{3}{16}p^9\mathrm{n}\{p\}^{\mathrm{n}\{p\}+1}2^{4\binom{\mathrm{n}\{p\}+1}{2}}\mathrm{g}_2^{\mathrm{n}\{p\}+1}\{\mathrm{n}\{p\}\} \le 2^{\frac{1}{2}p^4+\frac{1}{2}p^2 2^{3(\frac{p^2-p}{4})2^{\mathrm{r}\{p\}-1}}}.$$

The lemma follows since

$$\frac{1}{2}p^4+\frac{1}{2}p^2 2^{3(\frac{p^2-p}{4})2^{\mathrm{r}\{p\}-1}} \le p^2 2^{3(\frac{p^2-p}{4})2^{\mathrm{r}\{p\}-1}} \le 2^{3(\frac{p}{2})2^{\mathrm{r}\{p\}}}.$$

$\square$

Proof of Technical Lemma 4.2.3. We first prove item 1.

$$3(2p+1)\mathrm{g}_1\{p-1,p\}\mathrm{g}_3\{p-1\} \le 2^{1+p^2+3\cdot 2^{p-1}+2^{3(\frac{p-1}{2})^{p-1}+1}} \le 2^{2^{3(\frac{p-1}{2})^{p-1}+3}} \le \mathrm{g}_3\{p\}.$$

Now we prove item 2.

$$6p^3\mathrm{g}_1\{p-2,p-1\}\mathrm{g}_2\{p\}\mathrm{g}_3^2\{p-2\} \le 2^{p^2+3\cdot 2^{p-2}+2^{3(\frac{p}{2})^p}+2^{3(\frac{p-2}{2})^{p-2}+2}} \le \mathrm{g}_3\{p\}.$$

$\square$

Proof of Technical Lemma 6.2.7. It is easy to see that it is enough to prove that

$$2^{p+(((p-1)p+2)2^{(p-1)p}-2)(2^{\frac{1}{2}p^2}+2^{\frac{1}{2}p}+1)} \le \tilde{\mathrm{g}}_{H,1}\{p\}^{2^{\frac{3}{2}p^2}-(2^{(p-1)p}-1)(2^{\frac{1}{2}p^2}+2^{\frac{1}{2}p}+1)-1}.$$

Indeed, since $2^{(2^{\frac{1}{2}(p-1)p+2}-2)} \le \tilde{\mathrm{g}}_{H,1}\{p\}$ and $2^{\frac{3}{2}p^2}-(2^{(p-1)p}-1)(2^{\frac{1}{2}p^2}+2^{\frac{1}{2}p}+1)-1 \ge 0$, the lemma follows from

$$p+(((p-1)p+2)2^{(p-1)p}-2)(2^{\frac{1}{2}p^2}+2^{\frac{1}{2}p}+1) \le ((p-1)p+2)2^{\frac{3}{2}p^2-1} \le$$

$$\le (2^{\frac{1}{2}(p-1)p+2}-2)2^{\frac{3}{2}p^2-1} \le (2^{\frac{1}{2}(p-1)p+2}-2)(2^{\frac{3}{2}p^2}-(2^{(p-1)p}-1)(2^{\frac{1}{2}p^2}+2^{\frac{1}{2}p}+1)-1).$$

$\square$

Proof of Technical Lemma 6.4.3. First, it is easy to prove that for every $p\in\mathbb{N}_*$ we have that $\tilde{\mathrm{g}}_{H,3}\{p\} \le 2^{(9p^2+14p+3)2^{\frac{1}{2}p^2+2}-2}$. Then,

$$2^{ps(s-1)+2}e^2s^4p\,\mathrm{g}_6\{p,s,2eps+8(eps)^2,(ps+1)ep+4e^2p^3s^2,1\}\max\{8e^2p^3s^3,\tilde{\mathrm{g}}_{H,3}\{p\}\} \le$$

$$\leq 2^{ps(s-1)+2}e^2s^4p\Big(\mathrm{g}_4\{p\}(6e^2p^3s^2)^{2^{\frac{1}{2}p}}\Big)^{\frac{2^{s(\frac{3}{2}p^2+2)}-1}{2^{\frac{3}{2}p^2+2}-1}}2^{(p+4)(2^{s(s-1)p^2}-1)2^{s(\frac{3}{2}p^2+2)}}\cdot$$

$$\cdot\max\{8e^2p^3s^3, \tilde{\mathrm{g}}_{H,3}\{p\}\}^{2^{s(s-1)p^2+s(\frac{3}{2}p^2+2)}}\leq$$

$$\leq\Big((6p^3)^{2^{\frac{1}{2}p}}2^{2^{3(\frac{p}{2})^p+2}}\Big)^{\frac{2^{s(\frac{3}{2}p^2+2)}-1}{2^{\frac{3}{2}p^2+2}-1}}2^{\alpha_1\{p,s\}}s^{\beta_1\{p,s\}}e^{\gamma_1\{p,s\}},$$

where

$$\alpha_1\{p,s\}=(p+4)2^{s(s-1)p^2+s(\frac{3}{2}p^2+2)}+((9p^2+14p+3)2^{\frac{1}{2}p^2+2}-2)2^{s(s-1)p^2+s(\frac{3}{2}p^2+2)},$$

$$\beta_1\{p,s\}=4+2^{\frac{1}{2}p+1}\frac{2^{s(\frac{3}{2}p^2+2)}-1}{2^{\frac{3}{2}p^2+2}-1}+3\cdot 2^{s(s-1)p^2+s(\frac{3}{2}p^2+2)},$$

and

$$\gamma_1\{p,s\}=2+2^{\frac{1}{2}p+1}\frac{2^{s(\frac{3}{2}p^2+2)}-1}{2^{\frac{3}{2}p^2+2}-1}+2^{s(s-1)p^2+s(\frac{3}{2}p^2+2)+1}.$$

Then we have

$$\Big((6p^3)^{2^{\frac{1}{2}p}}2^{2^{3(\frac{p}{2})^p+2}}\Big)^{\frac{2^{s(\frac{3}{2}p^2+2)}-1}{2^{\frac{3}{2}p^2+2}-1}}2^{\alpha_1\{p,s\}}\leq 2^{\alpha_2\{p,s\}}$$

and

$$s^{\beta_1\{p,s\}}\leq 2^{\alpha_2'\{p,s\}}$$

where

$$\alpha_2\{p,s\}=2^{s(\frac{3}{2}p^2+2)}+2^{3(\frac{p}{2})^p+2+s(\frac{3}{2}p^2+2)}+$$

$$+(p+4)2^{s(s-1)p^2+s(\frac{3}{2}p^2+2)}+((9p^2+14p+3)2^{\frac{1}{2}p^2+2}-2)2^{s(s-1)p^2+s(\frac{3}{2}p^2+2)}$$

and

$$\alpha_2'\{p,s\}=(s-1)(2^{s(\frac{3}{2}p^2+2)}+3\cdot 2^{s(s-1)p^2+s(\frac{3}{2}p^2+2)}).$$

But then,

$$\alpha_2\{p,s\}+\alpha_2'\{p,s\}\leq 2^{3(\frac{p}{2})^p+2+s(\frac{3}{2}p^2+2)}+2^{\frac{1}{2}p^2+p+7+s(s-1)p^2+s(\frac{3}{2}p^2+2)}+2^{s(s-1)p^2+s(\frac{3}{2}p^2+3)}\leq$$

$$\leq 2^{3(\frac{p}{2})^p+s^2(\frac{3}{2}p^2+3)+8}.$$

On the other hand,

$$\gamma_1\{p,s\}\leq 2^{s(\frac{3}{2}p^2+2)}+2^{s(s-1)p^2+s(\frac{3}{2}p^2+2)+1}\leq 2^{6s^2p^2}$$

and the lemma follows. □

Proof of Technical Lemma 7.0.3. We prove item 1 and the proof of item 2 can be done in a similar way.

$$\mathrm{g}_8\{d,s,k,i\}\cdot 2^{2^{\left(2^{\max\{2,d\}^{4^{k-i}}}+s^{2^{k-i}}\max\{2,d\}^{16^{k-i}}\mathrm{bit}(d)\right)}}=2^{2^{\alpha\{d,s,k\}}}2^{2^{\beta\{d,s,k\}}}2^{2^{\gamma\{d,s,k\}}}$$

where

$$\alpha\{d,s,k\} = 3\left(2^{2^{\frac{4^{k-i}-1}{3}}-1}d^{4^{k-i}}\right)^{2^{2^{\frac{4^{k-i}-1}{3}}}d^{4^{k-i}}} +$$

$$+s^{2^{k-i+1}}\max\{2,d\}^{2(16^{k-i}-1)\mathrm{bit}\{d\}}\left(\frac{3}{2}2^{4^{\frac{4^{k-i}-1}{3}}}d^{2\cdot 4^{k-i}}+3\right)+8,$$

$$\beta\{d,s,k\} = 2^{\max\{2,d\}^{4^{k-i}}} +$$

$$+s^{2^{k-i}}\max\{2,d\}^{16^{k-i}\mathrm{bit}(d)} + 6\cdot 2^{4^{\frac{4^{k-i}-1}{3}}}d^{2\cdot 4^{k-i}}s^{2^{k-i+1}}\max\{2,d\}^{2(16^{k-i}-1)\mathrm{bit}\{d\}},$$

and

$$\gamma\{d,s,k\} = 2^{\max\{2,d\}^{4^{k-i}}} + s^{2^{k-i}}\max\{2,d\}^{16^{k-i}\mathrm{bit}(d)}.$$

The inequality holds since

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

$$\begin{aligned}\beta\{d,s,k\} &\leq 2^{\max\{2,d\}^{4^{k-i+1}}} + 7s^{2^{k-i+1}}\max\{2,d\}^{4\frac{4^{k-i}-1}{3}+2\cdot 4^{k-i}+2(16^{k-i}-1)\mathrm{bit}(d)}\\ &\leq 2^{\max\{2,d\}^{4^{k-i+1}}} + s^{2^{k-i+1}}\max\{2,d\}^{16^{k-i+1}\mathrm{bit}(d)} - 2,\end{aligned}$$

and

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

□

References

[1] Artin E. *Uber die Zerlegung definiter Funktionen in Quadrate.* Abh. Math. Sem. Hamburg, 5, 100–115 (1927). The collected papers of Emil Artin, 273–288. Reading, Addison-Wesley, 1965.

[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, first edition. Springer-Verlag, Berlin, 2003.

[4] 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.

[5] Blekherman G., Gouveia J. and Pfeiffer J. *Sums of Squares on the Hypercube* Manuscript. arXiv:1402.4199.

[6] Bochnak J., Coste M. and Roy M.-F. *Géométrie algébrique réelle* (Second edition in english: Real Algebraic Geometry), volume 12 (36) of Ergebnisse der Mathematik und ihrer Grenzgebiete [Results in Mathematics and Related Areas]. Springer-Verlag, Berlin, 1987 (1998).

[7] Brownawell W. D. *Local diophantine nullstellen identities.* Journal of AMS, 1, 311–322, 1988.

[8] Caniglia L., Galligo A. and Heintz J. *Borne simplement exponentielle pour les degrés dans le théorème des zéros sur un corps de caractéristique quelconque.* C. R. Acad. Sci. Paris, 307, 255–258, 1988.

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

[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., Lombardi H. and Roy M.-F. *Dynamical method in algebra: Effective Nullstellensätze* Annals of Pure and Applied Logic 111, 203–256 (2001).

[12] 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).

[13] 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.

[14] Daykin D. E. *Hilbert's 17th problem.* Ph.D. Thesis, Univ. of Reading, (1961) unpublished.

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

[16] Delzell C.N. *Kreisel's unwinding of Artin's proof*, 113–245 in Kreiseliana: About and Around Georg Kreisel, ed. P. Odifreddi, A K Peters, Ltd.(1996).

[17] Díaz-Toca G., Gonzalez-Vega G. and Lombardi H. *Generalizing Cramer's Rule: Solving uniformly linear systems of equations.* SIAM Journal on Matrix Analysis and Applications. 27, 621–637 (2005).

[18] Dubois D. *A nullstellensatz for ordered fields,* Arkiv for Mat., Stockholm, 8, 111–114 (1969).

[19] Efroymson G. *Local reality on algebraic varieties*, J. of Algebra, 29, 113–142 (1974).

[20] Gantmacher F. R. *The theory of matrices.* Chelsea 1959. (english translation)

[21] Gonzalez L., Lombardi H., Recio T. and Roy M.-F. *Spécialisation of la suite of Sturm et sous-résultants. I.* RAIRO Informatique theorique et Applications 24, 561–588 (1990). Detailed version: CALSYF journées du GRECO of Calcul Formel 1989.

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

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

[24] Grigoriev D. and Vorobjov N. *Complexity of Null- and Positivstellensatz proofs.* Ann. Pure Appl. Logic 113, 153–160 (2002).

[25] Hermann G. *Die frage der endlich vielen schritte in der theorie der polynomialideale.* Math. Annalen 95, 736–788, (1926).

[26] Hermite C. *Remarques sur le théorème de sturm.* C. R. Acad. Sci. Paris, 36, 52–54, (1853).

[27] Hilbert D. *Sur les problèmes futurs des mathématiques.* Compte Rendu du Deuxième Congrès International des Mathématiciens, pp. 58–114, Gauthier-Villars, Paris, 1902.

[28] Hilbert D. *Mathematische Probleme.* Göttinger Nachrichten, (1900), 253–297, and in Archiv der Mathematik und Physik, (3) 1 (1901), 44–63 and 213–237.

[29] Hilbert D. *Mathematical problems.* Bull. Amer. Math. Soc. 8 (1902), no. 10, 437–479.

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

[31] Jelonek Z., *On the effective Nullstellensatz.* Invent. Math. 162 (2005), no. 1, 117.

[32] Kollár J. *Effective nullstellensatz for arbitrary ideals.* J. Eur. Math. Soc. 1, 313–337, (1999).

[33] Kreisel G. *Hilbert's 17-th problem.* in Summaries of talks presented at the Summer Inst. of Symbolic Logic at Cornell Univ (1957)

[34] Kreisel G. *Sums of squares.* Summaries of Talks Presented at the Summer Institute in Symbolic Logic in 1957 at Cornell Univ., Princeton, Institute for Defense Analysis, (1960) 313–320.

[35] Krivine J.-L. *Anneaux préordonnés.* Journal d'analyse mathématique 12, 307–326 (1964).

[36] Lancaster P. and Tismenetsky, M. *The Theory of Matrices.* 2nd edition. Academic Press, 1985.

[37] Laplace P.-S. *Leçons de mathématiques données à l'École normale en 1795.* Document (Gallica) Œuvres complètes, tome 14, 10–177.

[38] Lojasiewicz S. *Ensembles semi-analytiques.* Institut des Hautes Etudes Scientifiques, 1965 - 153 pages.

[39] Lombardi H. *Théorème effectif des zéros réel et variantes.* Publications Mathématiques of l'Universite de Besançon. 1988-89. Fascicule 1.

[40] Lombardi H. *Effective real nullstellensatz and variants*, in: Effective Methods in Algebraic Geometry. Eds. Mora T., Traverso C.. Birkhaüser (1991). Progress in Math. 94 (MEGA 90), 263–288. (abridged english version of [39])

[41] Lombardi H. *Nullstellensatz réel effectif et variantes.* C.R.A.S. Paris, t. 310, Serie I, 635–640, (1990).

[42] Lombardi H. *Théorème effectif des zéros réel et variantes, avec une majoration explicite des degrés.* 1990. Mémoire d'habilitation.

[43] Lombardi H. *Une borne sur les degrés pour le Théorème des zéros réel effectif.* 323–345. In: Real Algebraic Geometry. Proccedings, Rennes 1991, Lecture Notes in Mathematics no 1524. Eds.: Coste, Mahe, Roy. (Springer-Verlag, 1992).

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

[45] Perrucci D. and Roy M.-F. *Zero-nonzero and real-nonreal sign determination*, Linear Algebra and Its Applications 439 (2013), no. 10, pp. 3016-3030.

[46] Perrucci D. and Roy M.-F. *Elementary recursive quantifier elimination based on Thom encoding and sign determination*, to appear in Annals of Pure and Applied Logic.

[47] 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).

[48] Risler J.-J. *Une caractérisation des idéaux des variétés algébriques réelles,* C.R.A.S. Paris, t. 271, 1970, serie A, 1171–1173.

[49] Rose H. *Subrecursion: functions and hierarchies.* Oxford Logic Guides, 9. The Clarendon Press, Oxford University Press, New York, 1984.

[50] Schmid J. *On the degree complexity of Hilbert's 17th problem and the Real Nullstellensatz*, Habilitation, University of Dortmund, n ř 70, Seminar of logic, Paris 7, (2000).

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

[52] Stengle G. *A Nullstellensatz and a Positivstellensatz in semialgebraic geometry.* Math. Ann. 207, 87–97 (1974)

[53] Tarski A. *A decision method for elementary algebra and geometry.* University of California Press, Berkeley and Los Angeles, Calif., 1951. 2nd ed.

[54] van der Waerden B. L. *Modern Algebra, Volume II.* F. Ungar Publishing Co., 1950.

[55] Warou H. *An algorithm and bounds for the real effective Nullstellensatz in one variable*, Progress in Mathematics, no 143, 373–387. Birkhäuser. Basel. 1996.