REAL EFFECTIVE NULLSTELLENSATZ IN ONE VARIABLE

WAROU Harouna, Rennes

Introduction

In this paper we deal with the algorithm of construction of an effective positivstellensatz given in [LOM1], for the particular case of a family of univariate polynomials with coefficients in real closed field.

We study in detail the mixed and generalized Taylor formulas which are essential tools for constructing algebraic identities for the real effective nullstellensatz. In particular we give more general and straightforward proof for mixed Taylor formulas, we prove that the coefficients which appear in both the mixed and generalized Taylor formulas are integers and we establish some related upper-bounds.

We also show that a good control on the "glueing" procedure leads to a bound on the degree by $8rd^2$ in the final algebraic identity, where d is a bound on the degrees of the input polynomials and r is a bound on the number of real roots of these polynomials and their successive derivatives.

1. Ground tools

1.1 Incompatible system and strong implication

A *strict sign condition* is one of the following two : $> 0, < 0$. We denote them by -1 and $+1$ respectively. A *generalized sign condition* is one of the elements of $\{< 0, \leq 0, = 0, \geq 0, \neq 0, > 0\}$. When we replace the strict sign condition < 0(respectively > 0) by the generalized sign condition ≤ 0 (respectively ≥ 0) we say that the sign condition is relaxed.

Given a polynomial $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ we recall that its *norm* is defined as $\left(\sum_{i=0}^{n} a_i^2\right)^{\frac{1}{2}}$ and its *size* $\| P \|$ is defined as the logarithm of its norm. The degree of P is denoted by $deg(P)$.

We consider an ordered field $\mathbf{K}$ and $\mathbf{R}$ a real closed extension of $\mathbf{K}$. We denote by $\mathbf{K[X]}$ the polynomial ring $\mathbf{K}[X_1, \ldots, X_n]$. Let F be a non empty finite subset of $\mathbf{K[X]}$. We denote by :

F^2 the set of squares of non zero elements of F.

$\mathcal{M}(F)$ the *multiplicative monoid* generated by $F \cup \{1\}$.

$\mathcal{C}_p(F)$ the *positive cone* generated by F (the additive monoid generated by the elements of type $p.P.Q^2$ where p is poistive in $\mathbf{K}$, P in $\mathcal{M}(F)$ and Q in $\mathbf{K[X]}$).

and $\mathcal{I}(F)$ the *ideal* generated by F.

Definition 1 : *Consider a system* $\mathbb{H} = [F_>, F_\geq, F_=, F_\neq]$ *of generalized sign conditions, consisting of four finite subsets of* $\mathbf{K[X]}$. *We say that the system* $\mathbb{H}$ *is strongly incompatible in* $\mathbf{R}$ *if we have in* $\mathbf{R[X]}$ *an equality of the following type* :

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

with $S \in \mathcal{M}(F_\geq^2 \cup F_\neq^2)$, $P \in \mathcal{C}_p(F_> \cup F_\geq)$, $Z \in \mathcal{I}(F_=)$

Notation 2 : The strong incompatibility of a system $\mathbb{H}$ of generalized sign conditions is denoted by

$$\downarrow \mathbb{H} \downarrow$$

Remark 3 : It is clear that a strong incompatibility is a very strong form of incompatibility. In particular, it implies that it is impossible to give the indicated signs to the polynomials, in any ordered extension of $\mathbf{K}$. The impossibility of system of generalized sign conditions is constructively equivalent to its formulation in form of various implications : for exemple the system $[P = 0, Q = 0]$ is strongly incompatible in $\mathbf{R}$ is equivalent to

$$\forall x_1, \ldots, x_n \in \mathbf{R} \;\; P(x_1, \ldots, x_n) = 0 \Longrightarrow Q(x_1, \ldots, x_n) \neq 0$$

We shall speak thus of *strong incompatibility, strong implication, or strong evidence*, meaning always implicitly a strong incompatibility.

Notation 4 :
1) Let τ be a generalized sign condition. We use the following notation for strong implication :
$^*([S_1 > 0, \ldots, S_i > 0, P_1 \geq 0, \ldots, P_j \geq 0, Z_1 = 0, \ldots, Z_k = 0, N_1 \neq 0, \ldots, N_h \neq 0] \Longrightarrow Q\ \tau)^*$
Note that if one takes $1 = 0$ in the right-hand side in the above strong implication, and applies the definition, one obtains exactly the strong incompatibility for the left-hand side of the implication. Thus we can formulate any strong implication in form of strong incompatibility.
2) Let us denote by $\mathbb{H}$ the left-hand side in 1) and by $\mathbb{H}'$ a system of generalized sign conditions $Q_1\ \tau_1\ , \ldots, Q_k\ \tau_k$. We then write : $^*(\mathbb{H} \Longrightarrow \mathbb{H}')^*$
to mean $^*(\mathbb{H} \Longrightarrow Q_1\ \tau_1\ )^*$ and ... and $^*(\mathbb{H} \Longrightarrow Q_k\ \tau_1\ )^*$

The different variants of the real positivstellensatz are consequences of the following general theorem (see [BCR] ch.4) :

Theorem 5 : *Let* $\mathbf{K}$ *be an ordered field and* $\mathbf{R}$ *a be real closed extension of* $\mathbf{K}$. *Let* $\mathbb{H} = [F_>, F_\geq, F_=, F_\neq]$ *a be system of generalized sign conditions on polynomials of* $\mathbf{K}[\mathbf{X}]$ *and* A *be the semi-algebraic set of* $\mathbf{R}^n$ *defined by* :
$A = \{\mathbf{x} \in \mathbf{R}^n / \forall\ f \in F_>, f(\mathbf{x}) > 0, \forall\ g \in F_\geq, g(\mathbf{x}) \geq 0, \forall\ h \in F_=, h(\mathbf{x}) = 0, \forall\ q \in F_\neq, q(\mathbf{x}) \neq 0\}$
The three following conditions are equivalent :

- $\mathbb{H}$ *is strongly incompatible in* $\mathbf{R}$
- A *is empty in* $\mathbf{R}^n$
- A *is empty in any ordered extension of* $\mathbf{K}$.

1.2 A bound on the degree of a strong incompatibility constructed from other strong incompatibilities

We introduce now some results that will be useful for the rest of this note, concerning the manipulation of strong incompatibilities and strong implications (see [Lom2]).

Definition 6 : *We call degree of a strong incompatibility, the maximum degree of polynomials that appear in the corresponding algebraic identity.*

For example, if we have a strong incompatibility : $\downarrow [A > 0, B > 0, C \geq 0, D \geq 0, E = 0, G = 0] \downarrow$ caracterized by the following algebraic identity :

$$A^2.B^6 + C.\sum_{i=1}^{h} p_i.P_i^2 + A.B.D.\sum_{j=1}^{k} q_i.Q_j^2 + E.U + G.V = 0$$

then the degree of this strong incompatibility is :

$$\sup\{deg(A^2.B^6), deg(C.P_i^2)(i = 1, \ldots, h), deg(A.B.D.Q_j^2)(j = 1, \ldots, k), deg(E.U), d(G.\mathrm{V})\}$$

In the following proposition we give some precisions on the degree of some basic constructions of strong incompatibilities (cf [LOM1]).

Proposition 7 : *Let* $\mathbb{H}$ *be a system of generalized sign conditions on polynomials of* $\mathbf{K}[\mathbf{X}]$ *and* $Q \in \mathbf{K}[\mathbf{X}]$. *Then*

(i) *If* $\downarrow [\mathbb{H}, Q \leq 0] \downarrow$ *with the degree* δ *and* $\downarrow [\mathbb{H}, Q \geq 0] \downarrow$ *with the degree* δ', *one has* $\downarrow \mathbb{H} \downarrow$ *with the degree bounded by* $\delta + \delta'$.

(ii) *if* $\downarrow [\mathbb{H}, Q < 0] \downarrow$ *with the degree* δ *and* $\downarrow [\mathbb{H}, Q > 0] \downarrow$ *with the degree* δ', *one has* $\downarrow [\mathbb{H}, Q \neq 0] \downarrow$ *with the degree bounded by* $\delta + \delta'$.

(iii) *if* $\downarrow [\mathbb{H}, Q \neq 0] \downarrow$ *and* $\downarrow [\mathbb{H}, Q = 0] \downarrow$ *one has* $\downarrow \mathbb{H} \downarrow$. *Moreover if* Q *has the degree* q, $\downarrow [\mathbb{H}, \mathrm{Q} \neq 0] \downarrow$ *has the degree* δ *with* $Q^m S$ *in the monoid part and* $\downarrow [\mathbb{H}, \mathrm{Q} = 0] \downarrow$ *has the degree* δ'. *Then one has the strong incompatibility* $\downarrow \mathbb{H} \downarrow$ *with the degree bounded by* $\delta + 2m\delta' - 2mq$.

Proof : We give only the proof for the most intricate case (iii). Call $F_>, F_\geq, F_=, F_\neq$ the four finite subsets of $\mathbf{K}[\mathbf{X}]$ containing in $\mathbb{H}$.
The hypothesis $\downarrow [\mathbb{H}, \mathrm{Q} \neq 0] \downarrow$ corresponds to the identity :

$$Q^{2m} S_1 + P_1 + Z_1 = 0 \quad (1)$$

with

$$S_1 \in \mathcal{M}(F_>^2 \cup F_{\neq 0}^2), P_1 \in \mathcal{C}_p(F_> \cup F_\geq), Z_1 \in \mathcal{I}(F_=)$$

Likewise the second hypothesis means we have an equality :

$$S_2 + P_2 + Z_2 Q + Z_3 = 0 \quad (2)$$

with

$$S_2 \in \mathcal{M}(F_>^2 \cup F_{\neq 0}^2), P_2 \in \mathcal{C}_p(F_> \cup F_\geq), Z_1 \in \mathcal{I}(F_=)$$

In (1) we have $deg(S_1) \leq \delta - 2mq$ and in (2) $deg(Z_2) \leq \delta' - q$. We rewrite the equality (2) :

$$S_2 + P_2 + Z_3 = -Z_2 Q$$

and we take the both sides to the power $2m$, so we obtain the equality :

$$S_3 + P_3 + Z_4 = Q^{2m} Z_5 \quad (3)$$

where $deg(Z_5) \leq 2m(\delta' - q)$. And next we multiply (1) by Z_5 and (3) by S_1 so we get :

$$\underbrace{S_1S_3 + P_3S_1 + Z_4S_1}_{\deg \leq 2m\delta' + (\delta - 2mq)} - \underbrace{P_1Z_5 - Z_1Z_5}_{\deg \leq \delta + 2m(\delta' - q)} = 0$$

2. Mixed and generalized Taylor Formulas

The mixed and generalized Taylor formulas are the main tool for the constructions of algebraic identities leading to Henri Lombardi's proof of real effective Nullstellensatz. The aim of this section is to extend the mixed Taylor formulas to differentiable functions, which allows us to prove by a straightforward way the algebraic theorem given in [LOM1]. Next we study the algebraic identities called generalized Taylor formulas. These formulas generalize the mixed Taylor formulas in the polynomial case.

2.1 Mixed Taylor Formulas

Notations :

Let $\varepsilon = [\epsilon_1, \epsilon_2, \ldots, \epsilon_n]$ $(n > 1)$ be a n-uple of strict sign conditions with $\epsilon_1 = 1$. We denote by

$\varepsilon_k = [\epsilon_1, \ldots, \epsilon_k]$ the k-uple formed by the k first elements of ε

$\xi_{n-1} := \frac{1}{2}(1 + \epsilon_{n-1}\epsilon_n)$

$\mathrm{P}_{\varepsilon_n}$ the polynomial of $\mathbb{Q}[X]$ defined by the induction :

$$\mathrm{P}_{\varepsilon_1}(t) := 1$$

$$\mathrm{P}_{\varepsilon_n}(t) := (-1)^{\xi_{n-1}}(n-1)\int_{\xi_{n-1}}^{t} \mathrm{P}_{\varepsilon_{n-1}}(x)dx$$

$c_{k,\varepsilon}$ the rational number defined by $c_{k,\varepsilon} = k\int_0^1 \mathrm{P}_{\varepsilon_k}(t)dt$

Moreover we denote the differential operator $\frac{d^k}{k!dx^k}$ by D_k

The polynomials $\mathrm{P}_{\varepsilon_n}$ are similar to the polynomials in the remainder of classical Taylor formulas. Thus it is not surprising to find common points in both theories.

Theorem and definition 8 : *If u and v are two reals with $u < v$, we let $\Delta = u - x$ for $u \leq x \leq v$ and $y_k = \begin{cases} x & if \ \ \epsilon_k\epsilon_{k+1} < 0 \\ u & otherwise \end{cases}$ Then for each function $f : [u, v] \longrightarrow \mathbb{R}$ of class C^{n+1}, $n \geq 0$, there exists 2^n mixed Taylor formulas and all the possible sign combinations occur. More precisely let $\varepsilon = [\epsilon_1, \epsilon_2, \ldots, \epsilon_{n+1}]$ be a $(n+1)$-uple of strict sign conditions with $\epsilon_1 = 1$, then one has the following equality*

$$f(x) = f(u) + \sum_{k=1}^{n} \epsilon_k c_{k,\varepsilon}\Delta^k D_k(f)(y_k) + \epsilon_{n+1}\frac{\Delta^{n+1}}{n!}\int_0^1 \mathrm{P}_{\varepsilon_{n+1}}(t)f^{(n+1)}(u + t\Delta)dt \qquad (E_1)$$

The previous formula is called the mixed Taylor formula for f associated to the combination ε.

Proof : We show (E_1) by induction on n. The formula (E_1) is immediate for $n = 0$. Indeed for f of C^1 we have :

$$f(x) - f(u) = \Delta\int_0^1 f'(u + t\Delta)dt$$

Suppose that the formula (E_1) holds for f of class C^n for $n \geq 1$ on $[u, v]$. Then for f of class C^{n+1} we have the following two cases

$\underline{1^{\text{rst}}\text{case}}$: $\epsilon_n \epsilon_{n+1} = -1$

In this case $y_n = x$. Integrating by parts

$$\mathrm{R} = \epsilon_n \frac{\Delta^n}{(n-1)!} \int_0^1 \mathrm{P}_{\varepsilon_n}(t) f^{(n)}(u + t\Delta) dt$$

which is equal by induction to

$$f(x) - f(u) - \sum_{k=1}^{n-1} \epsilon_k c_{k,\varepsilon} \Delta^k D_k(f)(y_k)$$

we obtain

$$\mathrm{R} = \epsilon_n \frac{\Delta^n}{(n-1)!} [\mathrm{Q}(t) f^{(n)}(u + t\Delta)]_0^1 - \epsilon_n \frac{\Delta^{n+1}}{(n-1)!} \int_0^1 \mathrm{Q}(t) f^{(n+1)}(\mathrm{u} + t\Delta) dt$$

where $\mathrm{Q}(t) = \displaystyle\int_0^t \mathrm{P}_{\varepsilon_n}(x) dx = \frac{1}{n} \mathrm{P}_{\varepsilon_{n+1}}(t)$. Consequently we have :

$$\mathrm{R} = \epsilon_n c_{n,\varepsilon} \Delta^n D_n(f)(y_n) + \epsilon_{n+1} \frac{\Delta^{n+1}}{n!} \int_0^1 \mathrm{P}_{\varepsilon_{n+1}}(t) f^{(n+1)}(u + t\Delta) dt$$

with $c_{n,\varepsilon_{n+1}} = n \displaystyle\int_0^1 \mathrm{P}_{\varepsilon_n}(t) dt = \mathrm{P}_{\varepsilon_{n+1}}(1)$.

$\underline{2^{\text{nd}}\text{case}}$: $\epsilon_n \epsilon_{n+1} = 1$

Now $y_n = u$ as in the previous case integrating R by parts we get

$$\mathrm{R} = \epsilon_n \frac{\Delta^n}{(n-1)!} [\mathrm{Q}(t) f^{(n)}(u + t\Delta)]_0^1 - \epsilon_n \frac{\Delta^{n+1}}{(n-1)!} \int_0^1 \mathrm{Q}(t) f^{(n+1)}(u + t\Delta) dt$$

but this time we choose $\mathrm{Q}(t) = \displaystyle\int_1^t \mathrm{P}_{\varepsilon_n}(x) dx = -\frac{1}{n} \mathrm{P}_{\varepsilon_{n+1}}(t)$

which gives exactly

$$\mathrm{R} = \epsilon_n c_{n,\varepsilon} \Delta^n D_n(f)(y_n) + \epsilon_{n+1} \frac{\Delta^{n+1}}{n!} \int_0^1 \mathrm{P}_{\varepsilon_{n+1}}(t) f^{(n+1)}(u + t\Delta) dt$$

with $c_{n,\varepsilon} = n \displaystyle\int_0^1 \mathrm{P}_{\varepsilon_n}(t) dt = \mathrm{P}_{\varepsilon_{n+1}}(0)$ ■

Proposition 9 : *Let n be an integer≥ 1. Then $\mathrm{P}_{\varepsilon_n}$ is a polynomial of degree $n-1$, which is strictly positive on $]0,1[$, with coefficients in $\mathbb{Z}$*

Proof : We show that P_{ε_n} is a polynomial with integer coefficients, the remain properties of P_{ε_n} follow immediatly from the definition.

It is easy for $n = 2$ because $P_{\varepsilon_2}(t) = (-1)^{\xi_1}(t - \xi_1)$. Suppose that P_{ε_n} $n \geq 2$, has integer coefficients. Write

$$P_{\varepsilon_{n+1}}(t) = \sum_{i=0}^{n} a_i t^i$$

$$P^{(k)}_{\varepsilon_{n+1}}(t) = \sum_{i=k}^{n} i(i-1)\dots(i-k+1)a_i t^{i-k}$$

Using the definition it is easy to see that

$$P^{(k)}_{\varepsilon_{n+1}}(t) = k! \binom{n}{k} (-1)^{\left(\sum_{j=n-k+1}^{n} \xi_j\right)} P_{\varepsilon_{n-k+1}}$$

and by identification it follows that

$$a_k = \binom{n}{k} (-1)^{\left(\sum_{j=n-k+1}^{n} \xi_j\right)} P_{\varepsilon_{n-k+1}}(0) \quad k = 1, \dots, n$$

One deduces that $a_k \in \mathbb{Z}$, $k = 1, \dots, n$ and $P_{\varepsilon_{n+1}} \in \mathbb{Z}[t]$ noting that $a_0 = 0$ or $a_0 = -(a_1 + a_2 + \dots + a_n)$ according to $\epsilon_n \epsilon_{n+1} = -1$ or 1 ■

Corollary 10 : (polynomial mixed Taylor Formulas)
Let **A** *be a commutative ring. Then for each polynomial of degree* $n \geq 1$, *there exists* 2^{n-1} *mixed Taylor formulas and all the possible sign combinations occur. One considers two variables* U *and* V *and one lets* $\Delta = U - V$. *Let* $\mathfrak{E} = [\epsilon_1, \epsilon_2, \dots, \epsilon_n]$ *be a* n*-uple of strict sign conditions with* $\epsilon_1 = 1$, *then the mixed Taylor formula associated to the combination* $\mathfrak{E}$ *for a polynomial* $P \in \mathbf{A}[X]$ *of degree* $n \geq 1$, *is an algebraic identity of the following form* :

$$P(U) - P(V) = \sum_{k=1}^{n-1} \epsilon_k c_{k,\mathfrak{E}} \Delta^k D_k(P)(Y_k) + \epsilon_n c_{n,\mathfrak{E}} \Delta^n D_n(P) \qquad (E_2)$$

where $c_{k,\mathfrak{E}}$ *are positive integers and*

$$Y_k = \begin{cases} U & if\ \epsilon_k \epsilon_{k+1} > 0 \\ V & otherwise \end{cases}$$

Proof : Since it concerns algebraic identities in variables U, V and the coefficients of the polynomial P, it is enough to show the corollary for the ring **A**=$\mathbb{Z}$, and this can be deduced from the theorem 8 ■

Proposition 11 : *Let* $\mathfrak{E} = [\epsilon_1, \epsilon_2, \dots, \epsilon_n]$ $(n \geq 1)$ *be a* n*-uple of strict sign conditions with* $\epsilon_1 = 1$. *Then the integers* $c_{k,\mathfrak{E}}$ $(k = 1, \dots, n)$ *satisfy the following inequalities* :

$$c_{k+1,\mathfrak{E}} \leq (k+1) c_{k,\mathfrak{E}} \ \ and \ \ c_{k,\mathfrak{E}} \leq 2(n!)\alpha(n) \left(\frac{2}{\pi}\right)^{n+1} \qquad (E_3)$$

$$with \quad \alpha(n) = \begin{cases} 1 & if\ n\ is\ even \\ \frac{2^{n+1}-1}{2^{n+1}-2} & otherwise \end{cases}$$

Proof (see [WAR]). In this proof we establish also the following facts : let $n \geq 2$ be an integer, we denote by E_n the set of all n-uples $\varepsilon = [1, \epsilon_2, \ldots, \epsilon_n]$ with $\epsilon_j = \pm 1$ $j = 2 \cdots n$ and $u_n = \sup_{\varepsilon \in E_n} c_{n,\varepsilon}$. Then u_n is realized by exactly four elements of E_n. Choosing an ε that realize u_n and writing $u_n = n \int_0^1 P_{\varepsilon_n}(t)dt$, we show that the increasing sequence $(u_n)_{n \geq 2}$ is giving by the coefficients of the Taylor expansion at zero of the fonction $\dfrac{t\cos(t)}{1-\sin(t)} = t\left(\dfrac{1}{\cos(t)} + \tan(t)\right)$. One notes that if n is odd u_n is a Euler's number.
Note that the first inequality in proposition 11 means that $c_{k+1,\varepsilon}/(k+1)! \leq c_{k,\varepsilon}/k!$ ■

Proposition 12 : *Let $\varepsilon = [\epsilon_1, \epsilon_2, \ldots, \epsilon_n]$ be a n- uple of strict sign conditions with $\epsilon_1 = 1$. Then the coefficients $c_{\varepsilon,k}$ satisfy :*

$$c_{\varepsilon,1} = 1, \text{ and } \epsilon_k c_{k,\varepsilon} = 1 - \sum_{i=1}^{k-1} \epsilon_i \delta_i c_{i,\varepsilon} \binom{k}{i} \qquad (E_4)$$

with $\delta_i = 1 - \xi_i$ for $i = 1, \ldots, k-1$, $k = 2, \ldots, n$ and the computation of the list $[c_{\varepsilon,1}, c_{\varepsilon,2}, \ldots, c_{\varepsilon,n}]$ takes time $O(n^4 [\log(n)]^2)$ using classical arithmetic.

Proof : The equality (E_4) is obtained taking the particular case $P = X^k$ in the previous corollary 10. By the same equality one deduces that the computation of $c_{\varepsilon,n}$ takes $O(n^2)$ arithmetic operations. And by the inequalty (E_3) the size of the integers and the coefficients $c_{\varepsilon,k}$ $(k \leq n-1)$ previously computed is bounded by $n\log(n)$, so using classical arithmetic operations, our total computation is in $O(n^4 [\log(n)]^2)$ ■

Remark 13 : According the proposition 11 and 12 we deduce that the size of a mixed Taylor formula for a degree n is bounded by $n^2\log(n)$ and this formula can be computed in time $O(n^4[\log(n)]^2)$.

2.2 Generalized Taylor Formulas

Let P be polynomial of degree n with coefficients in a commutative ring and $\sigma_0, \sigma_1, \ldots, \sigma_n$ a list of strict sign conditions. We denote by

$$\mathbb{H}(X) = \left[P(X)\ \sigma_0, P'(X)\ \sigma_1, \ldots, P^{(d)}(X)\ \sigma_n\right]$$

and

$$\mathbb{H}'(X) = \left[P(X)\ \sigma_0', P'(X)\ \sigma_1', \ldots, P^{(d)}\ \sigma_n\right]$$

the system of generalized sign conditions obtained from $\mathbb{H}(X)$ by relaxing all inequalities except the last one. The Thom's lemma claims (among other things) that :

$$[\mathbb{H}'(U), \mathbb{H}'(V),\ U < Z < V] \Rightarrow \mathbb{H}(Z) \qquad (\star)$$

The generalized Taylor formulas will be a way of expressing this geometric fact by particular algebraic identities, as we shall see later on examples. Let $\varepsilon = [\epsilon_0, \ldots, \epsilon_n]$ be $(n+1)$-uple of strict sign conditions. We denote by $\varepsilon^{(k)} = [\epsilon_k, \ldots, \epsilon_{n+1}]$ and $\Delta_{\epsilon_0,\epsilon_1} = \begin{cases} \Delta_1 & \text{if } \epsilon_0\epsilon_1 > 0 \\ \Delta_2 & \text{otherwise} \end{cases}$

Theorem 14 : *Let* $\mathbf{A}$ *be a commutative ring and* $P \in \mathbf{A}[X]$ *a polynomial of degree* $n \geq 1$. *One considers two new variables* U *and* V *and one lets* $\Delta_1 = X - U$, $\Delta_2 = V - X$. *Then there exists an equality of the following type :*

$$P(X) = P(Y_0) + \sum_{k=1}^{n-1} \epsilon_0\epsilon_k D_k(P)(Y_k) H_{k,\varepsilon}(\Delta_1, \Delta_2) + \epsilon_0\epsilon_n D_n(P) H_{n,\varepsilon}(\Delta_1, \Delta_2) \qquad (E_5)$$

where $Y_k = \begin{cases} U & if\ \epsilon_k\epsilon_{k+1} > 0 \\ V & otherwise \end{cases}$

and $H_{k,\varepsilon}$ *is a non zero homogeneous polynomial of degree* k *with positive integer coefficients, given by the inductive relation :*

$$H_{n,\varepsilon}(\Delta_1, \Delta_2) = \sum_{k=1}^{n-1} \frac{1 - \epsilon_0\epsilon_1\epsilon_k\epsilon_{k+1}}{2} \binom{n}{k} c_{k,\varepsilon'} \Delta^k_{\epsilon_0,\epsilon_1} H_{n-k,\varepsilon^{(k)}}(\Delta_1, \Delta_2) + \ c_{n,\varepsilon'} \Delta^n_{\epsilon_0,\epsilon_1}$$

with $\varepsilon' = \left[(\epsilon_0\epsilon_1)^k \epsilon_0\epsilon_k\right]_{k=1\ldots n}$.
The equality (E_5) *is called the generalized Taylor formula for* P *associated to the combination* ε.

Proof : By induction on the degree n of P. If $n = 1$ the theorem is easy. Suppose that the equality (E_5) holds for a degree $n - 1 \geq 0$. Let $\varepsilon = [\epsilon_0, \epsilon_2, \ldots, \epsilon_n]$ be a $(n+1)$-uple of strict sign condtions and P be a polynomial of degree n. We distinguish two cases :

case1 : $\epsilon_0\epsilon_1 = -1$ We write the mixed Taylor formula corresponding to the combination $\sigma = [\sigma_k]$ where $\sigma_k = (-1)^k \epsilon_0\epsilon_k, k = 1, \ldots, n$:

$$\begin{aligned} P(X) &= P(V) + \sum_{k=1}^{n-1} \sigma_k c_{k,\sigma} (X - V)^k D_k(P)(Z_k) + \sigma_n c_{n,\sigma} (X - V)^n D_n(P) \\ &= P(V) + \epsilon_0 \sum_{k=1}^{n-1} \epsilon_k c_{k,\sigma} \Delta_2^k D_k(P)(Z_k) + \epsilon_0\epsilon_n c_{n,\sigma} \Delta_2^n D_n(P) \end{aligned}$$

with $Z_k = \begin{cases} V & \text{if } \epsilon_k\epsilon_{k+1} = -1 \\ X & \text{otherwise} \end{cases}$
Then either $Z_k = V, k = 1, \ldots, n-1$ and then the theorem is proved or there are two set I and J such that $I \cup J = \{1, \ldots, n\}$, $I \cap J = \emptyset$ and $J \neq \emptyset$ and :

$$P(X) = P(V) + \epsilon_0 \sum_{k \in I} \epsilon_k c_{k,\sigma} \Delta_2^k D_k(P)(V) + \epsilon_0 \sum_{k \in J} \epsilon_k c_{k,\sigma} \Delta_2^k D_k(P)(X) + \epsilon_0\epsilon_n c_{n,\sigma} \Delta_2^n D_n(P)$$

Let

$$Q(X) = \epsilon_0 \sum_{k \in J} \epsilon_k c_{k,\sigma} \Delta_2^k D_k(P)(X)$$

By induction one has :

$$D_k(P)(X) = D_k(P)(Y_k) + \epsilon_k \sum_{j=1}^{n-k} \epsilon_{k+j} D_j[D_k(P)](Y_{k+j}) H_{j,\mathfrak{E}^{(k)}}(\Delta_1, \Delta_2)$$

$$= D_k(P)(Y_k) + \epsilon_k \sum_{m=k+1}^{n} \epsilon_m \binom{m}{m-k} D_m(P)(Y_m) H_{m-k,\mathfrak{E}^{(k)}}(\Delta_1, \Delta_2)$$

with $H_{m-k,\mathfrak{E}^{(k)}}$ homogeneous, with positive integer coefficients, of degree $m-k$ and $Y_m = U$ or V. If j_0 is the smallest index in J then

$$Q(X) = \epsilon_0 \sum_{k \in J} \sum_{j=k}^{n} \epsilon_j D_j(P)(Y_j) G_{j,\mathfrak{E}^{(k)}}(\Delta_1, \Delta_2)$$

$$= \epsilon_0 \sum_{l=j_0}^{n} \epsilon_l D_l(P)(Y_l) G_{l,\mathfrak{E}}(\Delta_1, \Delta_2)$$

with $G_{j,\mathfrak{E}^{(k)}} = \binom{j}{j-k} c_{k,\sigma} \Delta_2^k H_{j-k,\mathfrak{E}^{(k)}}$ $j \geq k$ and $G_{l,\mathfrak{E}} = \sum_{k \in J} G_{l,\mathfrak{E}^{(k)}}$ (**h**). One deduces

$$P(X) = P(V) + \epsilon_0 \sum_{k \in I} \epsilon_k D_k(P)(V) c_k \Delta_2^k + \epsilon_0 \sum_{l=j_0}^{n} \epsilon_l D_l(P)(Y_l) G_{l,\mathfrak{E}}(\Delta_1, \Delta_2)$$

One remarks now that if $l \in I$ then $\epsilon_l \epsilon_{l+1} = -1$ and by induction $Y_l = V$.

For the case $\epsilon_0 \epsilon_1 = 1$ write the mixed Taylor formula for P associated to the n-uple $(\sigma_k = \epsilon_0 \epsilon_k)_k = 1, \ldots, n$ and use the same argument as in the previous case ■

Remark 15 : For a degree n we have 2^n generalized Taylor formulas and all the possible sign combinations do appear.

Proposition 16 : *Let $\mathfrak{E} = [\epsilon_0, \ldots, \epsilon_n]$ be a combination of strict sign conditions. Then the sum of coefficients of the homogeneous polynomial $H_{k,\mathfrak{E}}$, $k = 1, \ldots, n$ is bounded by :*

$$\frac{n!}{2}\left(\left[1 + \sqrt{2}\left(\frac{2}{\pi}\right)^{\frac{3}{2}}\right]^n + \left[1 - \sqrt{2}\left(\frac{2}{\pi}\right)^{\frac{3}{2}}\right]^n\right) \leq \frac{n!}{2}\Big((1,75)^n + 1\Big)$$

Proof : Can be deduced easily by from proposition 11 and theorem 14 ■

2.3 Some explicit examples of generalized Taylor Formulas

We consider two variables U and V and we let $\Delta_1 = X - U$ and $\Delta_2 = V - X$. Let P be a polynomial with coefficients in a commutative ring **A**.

If $deg(P) = 3$, one has eight generalized Taylor formulas : the following 4 and their symetrics obtained by exchanging U and V (which implies the remplacement of Δ_1 by $-\Delta_2$ and Δ_2 by $-\Delta_1$) :

$$P(X) = P(U) + D_1(P)(U).\Delta_1 + D_2(P)(U).\Delta_1^2 + D_3(P).\Delta_1^3$$
$$P(X) = P(U) + D_1(P)(U).\Delta_1 + D_2(P)(V).\Delta_1^2 - D_3(P).\left[2\Delta_1^3 + 3\Delta_1^2\Delta_2\right]$$
$$P(X) = P(U) + D_1(P)(V).\Delta_1 - D_2(P)(V).\left[\Delta_1^2 + 2\Delta_1\Delta_2\right] + D_3(P).\left[\Delta_1^3 + 3\Delta_1^2\Delta_2 + 3\Delta_1\Delta_2^2\right]$$
$$P(X) = P(U) + D_1(P)(V).\Delta_1 - D_2(P)(U).\left[\Delta_1^2 + 2\Delta_1\Delta_2\right] - D_3(P).\left[2\Delta_1^3 + 6\Delta_1^2\Delta_2 + 3\Delta_1\Delta_2^2\right]$$

Assume that U and V give the same relaxed sign condition $\sigma_0', \sigma_1', \sigma_2'$ to $P, P', P^{(2)}$ respectively, the same strict sign condition σ_3 to $P^{(3)}$ and $U < X < V$. Then one of the eight generalized Taylor formulas is strong evidence showing that $P(X)$ has the strict sign condition σ_0. For example, If σ_0' is ≥ 0, $\sigma_1' : \geq 0$, $\sigma_2' : \leq 0$, $\sigma_3 : < 0$ and if $\Delta_1 > 0$, $\Delta_2 > 0$, the fourth generalized Taylor formula can be reread :

$$-P(X)+P(U)+D_1(P)(V).\Delta_1-D_2(P)(U).\left[\Delta_1^2 + 2\Delta_1\Delta_2\right]-D_3(P).\left[2\Delta_1^3 + 6\Delta_1^2\Delta_2 + 3\Delta_1\Delta_2^2\right] = 0$$

The equality provides the above implication as strongly evident.

If $deg(P) = 4$, one has sixteen generalized Taylor formulas : the following eight and their symetrics obtained by exchanging U and V :

$$P(X) = P(U) + D_1(P)(U).\Delta_1 + D_2(P)(U).\Delta_1^2 + D_3(P).\Delta_1^3 + D_4(P).\Delta_1^4$$
$$P(X) = P(U) + D_1(P)(U).\Delta_1 + D_2(P)(U).\Delta_1^2 + D_3(P)(V).\Delta_1^3 - D_4(P).\left[4\Delta_1^3\Delta_2 + 3\Delta_1^4\right]$$
$$P(X) = P(U) + D_1(P)(U).\Delta_1 +$$
$$D_2(P)(V).\Delta_1^2 - D_3(P)(V).\left[3\Delta_1^2\Delta_2 + 2\Delta_1^3\right] + D_4(P).\left[6\Delta_1^2\Delta_2^2 + 8\Delta_1^3\Delta_2 + 3\Delta_1^4\right]$$
$$P(X) = P(U) + D_1(P)(U).\Delta_1 +$$
$$D_2(P)(V).\Delta_1^2 - D_3(P)(U).\left[2\Delta_1^3 + 3\Delta_1^2\Delta_2\right] - D_4(P).\left[12\Delta_1^3\Delta_2 + 6\Delta_1^2\Delta_2^2 + 5\Delta_1^4\right]$$
$$P(X) = P(U) + D_1(P)(V).\Delta_1 - D_2(P)(V).\left[\Delta_1^2 + 2\Delta_1\Delta_2\right] +$$
$$D_3(P)(U).\left[\Delta_1^3 + 3\Delta_1\Delta_2^2 + 3\Delta_1^2\Delta_2\right] + D_4(P).\left[18\Delta_1^2\Delta_2^2 + 8\Delta_1\Delta_2^3 + 12\Delta_1^3\Delta_2 + 3\Delta_1^4\right]$$
$$P(X) = P(U) + D_1(P)(V).\Delta_1 - D_2(P)(V).\left[2\Delta_1\Delta_2 + \Delta_1^2\right] +$$
$$D_3(P)(V).\left[3\Delta_1\Delta_2^2 + 3\Delta_1^2\Delta_2 + \Delta_1^3\right] - D_4(P).\left[4\Delta_1\Delta_2^3 + 6\Delta_1^2\Delta_2^2 + 4\Delta_1^3\Delta_2 + \Delta_1^4\right]$$
$$P(X) = P(U) + D_1(P)(V).\Delta_1 - D_2(P)(U).\left[\Delta_1^2 + 2\Delta_1\Delta_2\right] -$$
$$D_3(P)(V).\left[3\Delta_1\Delta_2^2 + 6\Delta_1^2\Delta_2 + 2\Delta_1^3\right] + D_4(P).\left[24\Delta_1^2\Delta_2^2 + 20\Delta_1^3\Delta_2 + 8\Delta_1\Delta_2^3 + 5\Delta_1^4\right]$$
$$P(X) = P(U) + D_1(P)(V).\Delta_1 - D_2(P)(U).\left[\Delta_1^2 + 2\Delta_1\Delta_2\right] -$$
$$D_3(P)(U).\left[2\Delta_1^3 + 6\Delta_1^2\Delta_2 + 3\Delta_1\Delta_2^2\right] - D_4(P).\left[12\Delta_1^3\Delta_2 + 12\Delta_1^2\Delta_2^2 + 4\Delta_1\Delta_2^3 + 3\Delta_1^4\right].$$

3. Algorithm for the construction of the identity providing the positivstellensatz

Let $\mathbf{D}$ be an ordered domain, $\mathbf{K}$ its fraction field and $\mathbf{R}$ the real closure of $\mathbf{K}$. Let $F_1, \ldots, F_k \in \mathbf{A}[X]$, we shall call the complete sign tableau of the F_i denoted by $\mathcal{T} = \mathcal{T}_k[F_1, \ldots, F_k]$ the data of the number N of distinct real roots in $\mathbf{R}$: $\zeta_1 < \zeta_2 < \ldots < \zeta_N$ of F_j, $(j = 1, \ldots, k)$ and a tableau with k rows and $2N + 1$ columns giving the sign of each F_j at each zero ζ_i and on each open interval $]-\infty, \zeta_1[,]\zeta_j, \zeta_{j+1}[,]\zeta_N, +\infty[$ $j = 1, \ldots, N-1$.

Note that the tableau do not provides the value of roots but simply their Thom code.

Proposition 17 : *Let (P_j) be a family in $\mathbf{D}[X]$ stable by derivation. Let (ζ_j) be the family of real roots of P_j in $\mathbf{R}$. Then one can set up the complete sign tableau $\mathcal{T}$ for the family (P_j) using only the signs of $P_j(\zeta_i)$*

Proof : It is a easy consequence of Thom's Lemma ■

Let $L = [P_1, \ldots, P_s]$ be a list of polynomials of $\mathbf{D}[X]$ and $\sigma = (\sigma_i)_{i=1,\ldots,s}$ be a n-uple of generalized sign conditions and $\mathbb{H} = [P_1\sigma_1 0, \ldots, P_s\sigma_s 0]$ be the system of generalized sign conditions corresponding to L and σ. One considers the family $\mathcal{P}$ generated by L and by the operation $P \mapsto P'$, $\zeta_1 < \zeta_2 < \ldots < \zeta_r$ the real roots of polynomials in $\mathcal{P}$ and $\mathcal{T}$ the corresponding complete sign tableau.

Lemma 18 : *if one has :*
a) *the incompatibilities* $\downarrow [\mathbb{H}, X < \zeta_1] \downarrow, \downarrow [\mathbb{H}, \zeta_1 < X < \zeta_2] \downarrow, \downarrow [\mathbb{H}, \zeta_2 < X < \zeta_3] \downarrow, \ldots,$
$\downarrow [\mathbb{H}, X < \zeta_r] \downarrow$ *with degree bounded by* δ.
b) *the incompatibilities* $\downarrow [\mathbb{H}, X = \zeta_i] \downarrow \ i = 1, \ldots, r$ *with degree bounded by* δ'.
Then one can construct $\downarrow \mathbb{H} \downarrow$ *with a degree bounded by* $2r\delta\delta'$.

Proof : We denote by $\mathbb{E}_1 = \downarrow [\mathbb{H}, X < \zeta_1] \downarrow$, $\mathbb{E}_k = \downarrow [\mathbb{H}, \zeta_{k-1} < X < \zeta_k] \downarrow$ for $k = 2, \ldots, r$, $\mathbb{E}_{r+1} = \downarrow [\mathbb{H}, X < \zeta_r] \downarrow$ and $Q_k = X - \zeta_k$, $k = 1, \ldots, r$. Applying r-times the proposition 7 (ii) one constructs $\downarrow [\mathbb{H}, Q_1 \neq 0, Q_2 \neq 0, \ldots, Q_r \neq 0] \downarrow$ with a degree bounded by $(r+1)\delta$ according to the following diagram :

$$\underbrace{\underbrace{\mathbb{E}_1 \ \mathbb{E}_2}_{\mathbf{E}_{1,2}} \ \mathbb{E}_3 \cdots\cdots \mathbb{E}_{r+1}}_{\mathbf{E}_{1,2,3}}$$
$$\vdots$$
$$\underbrace{\qquad\qquad\qquad\qquad}_{\mathbf{E}_{1,\ldots,r+1}}$$

The incompatibility $\mathbb{E}_{1,2} = \downarrow [\mathbb{H}, Q_1 \neq 0, Q_2 < 0] \downarrow$ is obtained by applying from proposition 7 (ii) to $\mathbb{E}_1$ and to $\mathbb{E}_2$. The incompatibility $\mathbb{E}_{1,2,3} = \downarrow [\mathbb{H}, Q_1 \neq 0, Q_2 \neq 0, Q_3 < 0] \downarrow$ is obtained by applying proposition 7 (ii) to $\mathbb{E}_{1,2}$ and to $\mathbb{E}_3$ as previously. Iterating this process until $\mathbb{E}_{r+1}$ provides us the incompatibility $\mathbb{E}_{1,\ldots,r+1} := \downarrow [\mathbb{H}, Q_1 \neq 0, Q_2 \neq 0, \ldots, Q_r \neq 0] \downarrow$. We apply next r-times the proposition 7 (iii) with $q = 1$ and noticing that the exponent of Q_i is bounded by 2δ at each step, one deduces that the degree increases at most by $2\delta(\delta' - 1)$. Finaly one gets the bound $(r+1)\delta + 2r\delta(\delta' - 1)$ ■

Theorem 19 :(real effectif positivstellensatz in one variable)
Let **D** *be an ordered domain,* **K** *its fraction field and* **R** *the real closure of* **K**.
Let L *be a list of polynomials of* $\mathbf{D}[X]$ *of degree at most* d, r *be the number of real roots in* **R** *of the family generated by* L *and the operation* $P \mapsto P'$ *and* $\mathbb{H}(X)$ *be a system of generalized sign conditions on elements of* L.
Then :

either $\mathbb{H}(x)$ *is possible in* **R**

or $\mathbb{H}(x)$ *is impossible in* **R** *and then* $\downarrow \mathbb{H} \downarrow$ *in* **R**. *Moreover the degree of* $\downarrow \mathbb{H} \downarrow$ *is bounded by* $8rd^2$.

Proof : Let $\mathcal{T}$ be the complete tableau of the family generated by L and the operation $P \mapsto P'$ and $\zeta_1 < \zeta_2 < \ldots < \zeta_r$ be the ordered list of finite points of $\mathcal{T}$. We set $\zeta_0 = -\infty$ et $\zeta_{r+1} = +\infty$.

The existence of x in $\mathbf{R}$ verifying $\mathbb{H}(x)$ is directly readable from the complete tableau $\mathcal{T}$ and can be tested by computation in $\mathbf{D}$. To do this one compares on each open interval and for each finite point of $\mathcal{T}$, the generalized sign condition of a polynomial in $\mathbb{H}(X)$ and its sign given in $\mathcal{T}$. If no contradiction is revealed for the polynomials of L on at least an interval or on a point then $\mathbb{H}(x)$ is possible in $\mathbf{R}$.
Otherwise if on each open interval and for each point $\zeta_k, k = 1, \ldots, r$ of $\mathcal{T}$ there exists a polynomial of L of reverse sign condition to its sign given in $\mathcal{T}$ then $\mathbb{H}(x)$ is impossible. On each open interval $I_k =]\zeta_{k-1}, \zeta_k[$ $(k = 2, \ldots, r)$ one chooses a polynomial P of L of reverse sign condition to its sign given in $\mathcal{T}$. One will take as possible a polynomial P of lower degree of L to prevent the growth of the final degree of the desired identity. If deg(P)=d, one denotes $(\epsilon_0, \epsilon_1, \ldots, \epsilon_d)$ the $(d+1)$-uple of strict sign conditions of $P, P', \ldots, P^{(d)}$ on I_k respectively. According theorem 14 there exits a generalized Taylor formula which shows the strong evidence of the generalized sign condition of P on I_k and hence the incompatibility $\downarrow [\mathbb{H}, \zeta_{k-1} < \mathrm{X} < \zeta_k] \downarrow$. This generalized Taylor formula can be rewriten :

$$Q_{k-1}^{2n_{k,1}} Q_k^{2n_{k,2}} \alpha_k + S_{k,1} + Q_{k-1} S_{k,2} - Q_k S_{k,3} - Q_{k-1} Q_k S_{k,4} + Z_k = 0$$

where $Q_{k-1} = X - \zeta_{k-1}, Q_k = X - \zeta_k, \alpha_k \in \mathbf{R}, S_{k,j}, j = 1,2,3,4$ are sums of squares in $\mathbf{R}[X]$ with positive weights. On intervals $]-\infty, \zeta_1[$ and $]\zeta_k, +\infty[$ the incompatibility $\downarrow [\mathbb{H}, X < \zeta_1] \downarrow$ (respectively $\downarrow [\mathbb{H}, \zeta_r < \mathrm{X}] \downarrow$) is given by the suitable ordinary Taylor formula of a polynomial of L. Now on a point $\zeta_k, k = 1, \ldots, r$ the incompatibilty $\downarrow [\mathbb{H}, X = \zeta_k] \downarrow$ is given by a polynomial with reverse sign condition at ζ_k. It is writen by an equality of the form :

$$P(X) = P(\zeta_k) + (X - \zeta_k) Q(X)$$

One concludes by applying the lemma 18 ■

4. Some precisions about implementation and cost of the algorithms in Axiom

Given $L = [P_1, \ldots, P_s]$ a list of univariate polynomials of $\mathbf{D}[X]$. We denote by :

d_i the degree of P_i and $n = \sum_{i=1}^{s} d_i$

$\mathcal{P}$ the family of the polynomials of L and their derivatives

$\zeta_1 < \zeta_2 < \cdots, < \zeta_r$ the sorted list of real roots of the polynomials of $\mathcal{P}$ and $\zeta_0 = -\infty$ and $\zeta_{r+1} = +\infty$

$\varepsilon_{k,j}$ the $(d_j + 1)$-uple formed of the $sign(P_j^{(i)})$ $i = d_j, \ldots, 0$, on the open interval $]\zeta_k, \zeta_{k+1}[$ $k = 0, \ldots, r$

$$\sigma_k = \Big[sign(P_1^{(d_1-1)}(\zeta_k)), sign(P_1^{(d_1-2)}(\zeta_k)), \ldots, sign(P_1(\zeta_k)), \ldots, sign(P_s^{(d_s-1)}(\zeta_k)), sign(P_s^{(d_s-2)}(\zeta_k)), \ldots, sign(P_s(\zeta_k))\Big]$$

The procedure TS which we describe now, allows us to get the complete sign tableau $\mathcal{T}$ of the family $\mathcal{P}$.

Procedure TS :

It's input is a list L of polynomials with coefficients in $\mathbf{D}$

It's output is formed of :

- the list $[\varepsilon_{0,1}, \varepsilon_{0,2}, \varepsilon_{0,s}], \ldots, , [\varepsilon_{m,1}, \ldots, \varepsilon_{r,s}]$ of $(r+1)$ uples, each uple is

formed of s (d_j+1)-uple of sign conditions realized by the polynomials $P_j^{(d_j)}, P_j^{(d_j-1)}, \ldots, P_j', P_j$, $j = 1\ldots, s$ on the open interval $]\zeta_k, \zeta_{k+1}[$, $k = 0, \ldots, r$.

- the list $\sigma_1, \ldots, \sigma_r$ of n-uple of sign conditions realized by the polynomials of $\mathcal{P}$ at the real zero ζ_k, $k = 1\ldots, r$

Remark : We use Roy's algorithm SI (simultaneous inequalities) [see RS] in the procedure TS to obtain the complete signs tableau. The procedure TS performs then n times the procedure SI .

Proposition 20 *Let* $\mathbf{D} = \mathbb{Z}$, $[P_1, \ldots, P_s]$ *be a list of polynomials with integer coefficients, and* d *the maximum of their degree,* t *the maximum of their size and* r *be the number of real roots of* $P_1, \ldots, P_s$ *and their successive derivatives. The procedure TS runs in time* $O(s^2 d^6 r(\log\ r)^3 t^2)$.

Proof : TS performs at most sd times the procedure SI. Each call of SI takes $O(sd^5(\log r)^3 t^2)$, so we get the stated total computation time by multiplication by sd

About the algebraic identity which provides the positivestellensatz we introduce for each ζ_i a variable x_i which represents it. The algebraic identity computed can be represented in compact form. To avoid the growth, we introduce elsewhere some formal operations. These operations occur when one eliminates the $X - x_i$ using the (iii) of the proposition 7. The proposition 7 (iii) consists to take the both sides of an identity of the following type :

$$M + C + Y_2 = -(X - \zeta_i)Y_1$$

to the power $2h$ with h integer ≥ 1. We shall write this manipulation by

$$\left[-(X - \zeta_i)\mathrm{Y}_1\right]^{2h} = \mathrm{M}^{2h} + \mathrm{MC}diffp1(\mathrm{M}, \mathrm{C}, 2h) + diffp_2(\mathrm{M}, \mathrm{C}, 2h) + \mathrm{Y}_2 diffp0(\mathrm{M}, \mathrm{C}, \mathrm{Y}_2, 2h)$$

with $\quad diffp1(\mathrm{M}, \mathrm{C}, 2h) := \sum_{j=0}^{h-1} \binom{2h}{2j+1} \mathrm{M}^{2(h-j-1)} \mathrm{C}^{2j}, \quad diffp2(\mathrm{M}, \mathrm{C}, 2h) := \sum_{j=1}^{h} \binom{2h}{2j} \mathrm{M}^{2(h-j)} \mathrm{C}^{2j},$

$diffp0(\mathrm{M}, \mathrm{C}, \mathrm{Y}_2, 2h) := \sum_{j=1}^{2h} \binom{2h}{j} (\mathrm{M} + \mathrm{C})^{2h-j} \mathrm{Y}_2^{j-1}$. The result of the two first operations are sums of squares with positive weights in $\mathbf{R}[X]$. Our algorithm produces, from the procedure TS, a straigth-line program which gives the desired identity. The evaluation of the last instruction of this straight-line program is an algebraic expression in the variables X and $P_j(\zeta_i)$ which is a suitable incompatibility as far as that the x_i are replaced by the ζ_i. It follows that this expression is an identity with coefficients in $\mathbb{R}_{alg}$ (the real closure of $\mathbb{Q}$). Whenever $P_j(\zeta_i) = 0$ we have substituded the term $P_j(x_i)$ by 0 in the expression which has been especially simplified. The final identity is hence an equality in $\mathbb{Z}[\mathrm{X}, (x_i)]/\mathbf{I}$ where $\mathbf{I}$ the ideal generated by $P_j(x_i)$ corresponding to the zero value of $P_j(\zeta_i)$. In pratice the computation time by straight-line program of the algebraic identity, is negligible comparing to the time of the computation of the complete sign tableau.

Example :
Let us consider the following polynomial

$$P = -7X^3 + 5X^2 + 2X + 3$$

We have the following complete sign tableau of P and its successives derivatives :

	x_1		x_2		x_3		x_4		
$P^{(3)}$	(-)	−	(-)	−	(-)	−	(-)	−	(-)
$P^{(2)}$	(+)	+	(+)	0	(-)	−	(-)	−	(-)
P'	(-)	0	(+)	+	(+)	0	(-)	−	(-)
P	(+)	+	(+)	+	(+)	+	(+)	0	(-)

We denote by $\mathbb{E}_1 = \downarrow [\mathbb{H}, X < x_1] \downarrow$, $\mathbb{E}_2 = \downarrow [\mathbb{H}, x_1 < X < x_2] \downarrow$ $\mathbb{E}_3 = \downarrow [\mathbb{H}, x_2 < X < x_3] \downarrow$, $\mathbb{E}_4 = \downarrow [\mathbb{H}, x_3 < X < x_4] \downarrow$ and $\mathbb{E}_5 = \downarrow [\mathbb{H}, x_4 < X] \downarrow$ the strong incompatibilities of generalized the sign condition $\mathbb{H} = [P = 0, P' \geq 0]$ on respectively the open intervals $I_1 =]-\infty, x1[$, $I_2 =]x_1, x_2[$, $I_3 =]x_2, x_3[$,$I_4 =]x_3, x_4[$ and $I_5 =]x_4, +\infty[$. Then $\mathbb{E}_k$ $k = 1, \ldots, 5$ are given respectively by the following generalized formulas :

$$
\begin{aligned}
&21Q_1^2 + S_{11} - Q_1.S_{13} = 0\\
&P_2(x_1) + S_{21} + Q_1.S_{22} - Q_2.S_{23} - Q_1Q_2.S_{24} - P_2 = 0\\
&P_2(x_2) + S_{31} + Q_2.S_{32} - Q_3.S_{33} - Q_2Q_3.S_{34} - P_2 = 0\\
&21Q_3^2 + S_{41} + Q_3.S_{42} - Q_4.S_{43} - Q_3Q_4.S_{44} = 0\\
&-P_1(x_4) + S_{51} + Q_4.S_{52} = 0
\end{aligned}
$$

where

$$
\begin{aligned}
&Q_k = X - x_k, \text{ for } k = 1, \ldots, 4\\
&S_{11} = -P'(x_1) + P_1;\ S_{13} = P^{(2)}(x_1)\\
&S_{21} = 0;\ S_{22} = 14Q_1^2;\ S_{23} = 21Q_1^2;\ S_{24} = 0\\
&S_{31} = 0;\ S_{32} = 21Q_3^2 + 14Q_2^2;\ S_{33} = 42Q_2^2;\ S_{34} = 0\\
&S_{41} = P';\ S_{42} = -P^{(2)}(x_3);\ S_{43} = S_{44} = 0\\
&S_{51} = 21Q_4^2 + P';\ S_{52} = -P^{(2)}(x_4)
\end{aligned}
$$

On x_k $(k = 1, \ldots, 4)$ the following identities provide respectively, the strong incompatibility $\mathbb{P}_k = \downarrow [\mathbb{H}, Q_k = 0] \downarrow$:

$$
\begin{aligned}
&P(x_1) + Q_1G_1 - P = 0\\
&P(x_2) + Q_2G_2 - P = 0\\
&P(x_3) + Q_3G_3 - P = 0\\
&-P'(x_4) + P' - Q_4G_4 = 0
\end{aligned}
$$

Let us construct $\mathbb{E}_{1,2} = \downarrow [\mathbb{H}, Q_1 \neq 0, Q_2 < 0] \downarrow$. We rewrite $\mathbb{E}_1$ and $\mathbb{E}_2$ and multiply respectively the right and left sides of the two equations :

$$
\begin{aligned}
&21Q_1^2 + S_{11} = Q_1S_{13}\\
&P(x_1) - Q_2S_{23} - P = -Q_1S_{22}
\end{aligned}
$$

we obtain

$$21P(x_1)Q_1^2 + P(x_1)S_{11} + Q_1^2S_{13}S_{22} - Q_2\big(21Q_1^2 + S_{11}\big)S_{23} - \big(21Q_1^2 + S_{11}\big)P = 0$$

We perform the same operation with $\mathbb{E}_3$ and $\mathbb{E}_{1,2}$ so we obtain $\mathbb{E}_{1,2,3} =\downarrow [\mathbb{H}, Q_1 \neq 0, Q_2 \neq 0, Q_3 < 0] \downarrow$:

$$21P(x_1)P(x_2)Q_1^2 + \Big[P(x_1)S_{11} + Q_1^2S_{13}S_{22}\Big]P(x_2)$$
$$+ Q_2^2\Big(21Q_1^2 + S_{11}\Big)S_{23}S_{32} - Q_3\Big[21P(x_1)Q_1^2 + P(x_1)S_{11} + Q_1^2S_{13}S_{22}\Big]S_{33}$$
$$-\Big(21Q_1^2 + S_{11}\Big)\Big(P(x_2) - Q_3S_{33} + Q_2S_{23}\Big)P = 0$$

In the same way we get $\mathbb{E}_{1,2,3,4} =\downarrow [\mathbb{H}, Q_1 \neq 0, Q_2 \neq 0, Q_3 \neq 0, Q_4 < 0] \downarrow$:

$$441P(x_1)P(x_2)Q_1^2Q_3^2 + 21P(x_1)P(x_2)Q_1^2S_{41} +$$
$$\Big[P(x_1)P(x_2)S_{11} + P(x_2)Q_1^2S_{13}S_{22} + 21Q_1^2Q_2^2S_{23}S_{32} + Q_2^2S_{11}S_{23}S_{32}\Big]\Big(21Q_3^2 + S_{41}\Big)$$
$$+ Q_3^2\Big[21P(x_1)Q_1^2 + P(x_1)S_{11} + Q_1^2S_{13}S_{22}\Big]S_{33}S_{42}$$
$$+ \Big(21Q_1^2 + S_{11}\Big)\Big(P(x_2) - Q_3S_{33} + Q_2S_{23}\Big)Q_3S_{42}P = 0 \qquad (1)$$

We remark that in the previous identity the polynomial Q_4 does not appear, so we can take $\downarrow [\mathbb{H}, Q_1 \neq 0, Q_2 \neq 0, Q_3 \neq 0, Q_4 \neq 0] \downarrow= \mathbb{E}_{1,2,3,4}$. We apply now the second procedure of "glueing" to eliminate Q_1 and Q_3 in the identity (1). We rewrite the strong incompatibility $\mathbb{P}_1$:

$$-Q_1G_1 = P(x_1) - P$$

and we take the both sides of this equality to the power 2 :

$$Q_1^2G_1^2 = P(x_1)^2 - (2P(x_1) - P)P \qquad (\mathbb{P}_1')$$

and we multiply (1) by G_1^2 and $(\mathbb{P}_1')$ by $441P(x_1)P(x_2)Q_3^2$ so we get

$$441P(x_1)^3P(x_2)Q_3^2 + 21P(x_1)P(x_2)G_1^2Q_1^2S_{41} +$$
$$\Big[P(x_1)P(x_2)S_{11} + P(x_2)Q_1^2S_{13}S_{22} + 21Q_1^2Q_2^2S_{23}S_{32} + Q_2^2S_{11}S_{23}S_{32}\Big]\Big(21Q_3^2 + S_{41}\Big)G_1^2$$
$$+ \Big[21P(x_1)Q_1^2 + P(x_1)S_{11} + Q_1^2S_{13}S_{22}\Big]Q_3^2G_1^2S_{33}S_{42} - 441P(x_1)P(x_2)\Big(2P(x_1) - P\Big)Q_3^2P$$
$$+ \Big(21Q_1^2 + S_{11}\Big)\Big(P(x_2) - Q_3S_{33} + Q_2S_{23}\Big)Q_3S_{42}G_1^2P = 0 \qquad (2)$$

To eliminate Q_3 we proceed as above with $\mathbb{P}_2$ and (2) so we get finaly the desired identity :

$$441P(x_1)^3P(x_2)P(x_3)^2 + 21P(x_1)P(x_2)G_1^2G_3^2Q_1^2S_{41} +$$
$$\Big[P(x_1)P(x_2)S_{11} + P(x_2)Q_1^2S_{13}S_{22} + 21Q_1^2Q_2^2S_{23}S_{32} + Q_2^2S_{11}S_{23}S_{32}\Big]\Big(21Q_3^2 + S_{41}\Big)G_1^2G_3^2$$
$$+ \Big[21P(x_1)Q_1^2 + P(x_1)S_{11} + Q_1^2S_{13}S_{22}\Big]Q_3^2G_1^2G_3^2S_{33}S_{42} - 441P(x_1)P(x_2)\Big(2P(x_1) - P\Big)Q_3^2G_3^2P$$
$$- 441P(x_1)^3P(x_2)\Big(2P(x_3) - P\Big)P + \Big(21Q_1^2 + S_{11}\Big)\Big(P(x_2) - Q_3S_{33} + Q_2S_{23}\Big)Q_3S_{42}G_1^2G_3^2P = 0$$

REFERENCES

[BCR] J. Bochnak, M. Coste and Roy M-F, "Géométrie algébrique réelle", A series of Modern Surveys in Mathematics 11, Spinger-Verlag, 1987

[LOM1] H. Lombardi, *Effective real Nullstellensatz and variants*, Effective Methods in Algebraic Geometry-Progess in Mathematics vol 94 1991, p.263-288.

[LOM2] H. Lombardi, *Une borne sur les dégrés pour le théorème des zéros réel effectif*, Lecture Notes in Mathematics 1524, eds M.Coste, L.Mahe, Roy M-F,"Real Algebraic Geometry", 1991, p.323-345.

[RS] M.F Roy and A. Szpirglass, *Complexity of computation on real algebraic numbers*, J. of Symb. comp., 1990, 10, 39-51

[CLGR] F. Cucker, L. Gonzalez, F. Rosselo *On algorithms for real algebraic plane curves*, Effective Methods in Algebraic Geometry - Progress in Math. vol 94 1991,p.63-87.

[WAR] H. Warou "Thèse Univ. de Rennes1 en préparation".

WAROU HAROUNA
Institut de Recherche Mathématique de Rennes,
Université de Rennes I, Campus de Beaulieu,
F-35042 Rennes Cedex, France