united nations educational, scientific and cultural organization

international atomic energy agency

the abdus salam international centre for theoretical physics

SMR1537/3 *(bis)*

Summer School and Conference on Real Algebraic Geometry and its Applications

(4 - 22 August 2003)

Some Algorithms in Real Algebraic Geometry

Marie-Françoise Roy
IRMAR
Université de Rennes I
Campus de Beaulieu
F-35042 Rennes
France

These are preliminary lecture notes, intended only for distribution to participants

Some Algorithms in Real Algebraic Geometry

Marie-Françoise Roy

August 19, 2003

Contents

Chapter 3

Complements

This document correspond to material I alluded to during the lectures and did not include in the previous documents.

3.1 Number of Complex Roots with Negative Real Part

So far Cauchy index was used only for the computation of Sturm-queries. We describe in this section an important application of Cauchy index to the determination of the number of complex roots with negative real part of a polynomial with real coefficients.

Let $P(X) = a_pX^p + \ldots + a_0 \in \mathrm{R}[X], a_p \neq 0$, where R is real closed, and $\mathrm{C} = \mathrm{R}[i]$ is algebraically closed. Define $F(X), G(X)$ by

$$P(X) = F(X^2) + XG(X^2).$$

Note that if $p = 2m$ is even

$$\begin{aligned} F &= a_{2m}X^m + a_{2m-2}X^{m-1} + \cdots, \\ G &= a_{2m-1}X^{m-1} + a_{2m-3}X^{m-2} + \cdots, \end{aligned}$$

and if $p = 2m + 1$ is odd

$$\begin{aligned} F &= a_{2m}X^m + a_{2m-2}X^{m-1} + \cdots, \\ G &= a_{2m+1}X^m + a_{2m-1}X^{m-1} + \cdots. \end{aligned}$$

We are going to prove the following result.

Theorem 3.1.1 *Let $n(P)$ be the difference between the number of roots of P with positive real parts and the number of roots of P with negative real parts.*

$$n(P) = \begin{cases} -\mathrm{Ind}\Big(\dfrac{G}{F}\Big) + \mathrm{Ind}\Big(\dfrac{XG}{F}\Big) & \text{if } p \text{ is even,} \\ -\mathrm{Ind}\Big(\dfrac{F}{XG}\Big) + \mathrm{Ind}\Big(\dfrac{F}{G}\Big) & \text{if } p \text{ is odd.} \end{cases}$$

This result has useful consequences in control theory. When considering a linear differential equation with coefficients depending on parameters a_i,

$$a_p y^{(p)}(t) + a_{p-1} y^{(p-1)}(t) + \ldots + a_0 y(t) = 0, a_p \neq 0, \tag{3.1}$$

it is important to determine for which values of the parameters all the roots of the characteristic equation

$$P = a_p X^p + a_{p-1} X^{p-1} + \ldots a_0, a_p \neq 0, \tag{3.2}$$

have negative real parts. Indeed if $x_1, \ldots, x_r$ are the complex roots of P with respective multiplicities $\mu_1, \ldots, \mu_r$, the functions

$$e^{x_i t}, \ldots, t^{\mu_r - 1} e^{x_i t}, i = 1, \ldots, r$$

form a basis of solutions of Equation (3.1) and when all the x_i have negative real parts, all the solutions of Equation (3.1) tend to 0 as t tends to $+\infty$, for every possible initial value. This is the reason why the set of polynomials of degree p which have all their complex roots with negative real part is called the **domain of stability** of degree p.

We shall prove the following result, as a corollary of Theorem 3.1.1.

Theorem 3.1.2 (Liénard/Chipart) *The polynomial*

$$P = a_p X^p + \ldots + a_0, a_p > 0,$$

belongs to the domain of stability of degree p if and only if all the a_i, $i = 0, \ldots, p$, are strictly positive and

$$\begin{cases} \mathrm{sr}_m(F, G) > 0, \ldots, \mathrm{sr}_0(F, G) > 0 & \text{if } p = 2m \text{ is even,} \\ \mathrm{sr}_{m+1}(XG, F) > 0, \ldots, \mathrm{sr}_0(XG, F) > 0 & \text{if } p = 2m+1 \text{ is odd.} \end{cases}$$

As a consequence, we can decide whether or not P belongs to the domain of stability by testing the signs of some polynomial conditions in the a_i, without having to approximate the roots of P.

Exercise 3.1.3 *Determine the conditions on a, b, c characterizing the polynomials $P = aX^3 + bX^2 + cX + d$, belonging to the domain of stability of degree 3.*

The end of the section is devoted to the proof of Theorem 3.1.1 and Theorem 3.1.2.

Define $A(X), B(X), \deg(A) = p, \deg(B) < p$, as the real and imaginary parts of $(-i)^p P(iX)$. Note that

$$A = a_p X^p - a_{p-2} X^{p-2} + \ldots,$$
$$B = -a_{p-1} X^{p-1} + a_{p-3} X^{p-3} + \ldots,$$

so that when p is even A is even and B is odd (respectively when p is odd A is odd and B is even).

We are going to first prove the following result.

Proposition 3.1.4 *Let $n(P)$ be the difference between the number of roots of P with positive real part and the number of roots of P with negative real part. Then,*

$$n(P) = \mathrm{Ind}\Big(\frac{B}{A}\Big).$$

A preliminary result on Cauchy index is useful.

Lemma 3.1.5 *Denote by $t \mapsto (A_t, B_t)$ a semi-algebraic and continuous map from $[0, 1]$ to the set of pairs of polynomials (A, B) of $\mathrm{R}[X]$ with A monic of degree p, $\deg(B) < p$ (identifying pairs of polynomials with their coefficients). Suppose that A_0 has a root x of multiplicity μ in (a, b) and no other root in $[a, b]$, and B_0 has no root in $[a, b]$. Then, for t small enough,*

$$\mathrm{Ind}\Big(\frac{B_0}{A_0}; a, b\Big) = \mathrm{Ind}\Big(\frac{B_t}{A_t}; a, b\Big).$$

Proof : Using the continuity of roots, there are two cases to consider:

If μ is odd, the number n of roots of A_t in $[a, b]$ with odd multiplicity is odd, and thus the sign of A_t changes n times while the sign of B_t is fixed, and hence for t small enough,

$$\operatorname{Ind}\Big(\frac{B_0}{A_0}; a, b\Big) = \operatorname{Ind}\Big(\frac{B_t}{A_t}; a, b\Big) = \operatorname{sign}(A_0^{(\mu)}(0)B_0(x)).$$

If μ is even, the number of roots of A_t in $[a, b]$ with odd multiplicity is even, and thus for t small enough,

$$\operatorname{Ind}\Big(\frac{B_0}{A_0}; a, b\Big) = \operatorname{Ind}\Big(\frac{B_t}{A_t}; a, b\Big) = 0.$$

□

Proof of Proposition 3.1.4: We can suppose without loss of generality that $P(0) \neq 0$.

If A and B have a common root $a+ib$, $a \in \mathrm{R}, b \in \mathrm{R}$, $b-ia$ is a root of P.

If $b = 0$, ia and $-ia$ are roots of P, and $P = (X^2 + a^2)Q$. Denoting $(-i)^{p-2}Q(iX) = C(X) + iD(X)$, $C \in \mathrm{R}[X], D \in \mathrm{R}[X]$, we have

$$\begin{aligned} A &= (X^2 - a^2)C, \\ B &= (X^2 - a^2)D. \end{aligned}$$

If $b \neq 0$, $b+ia$, $b-ia$,$-b+ia$,$-b-ia$ are roots of P and $P = (X^4+2(a^2-b^2)X^2 + (a^2+b^2)^2)Q$. Denoting $(-i)^{p-4}Q(iX) = C(X) + iD(X)$, $C \in \mathrm{R}[X], D \in \mathrm{R}[X]$, we have

$$\begin{aligned} A &= (X^4 - 2(a^2 - b^2)X^2 + (a^2 + b^2)^2)C, \\ B &= (X^4 - 2(a^2 - b^2)X^2 + (a^2 + b^2)^2)D. \end{aligned}$$

In both cases $n(P) = n(Q)$, $\operatorname{Ind}\Big(\frac{B}{A}\Big) = \operatorname{Ind}\Big(\frac{D}{C}\Big)$.

So we can suppose without loss of generality that P has no two roots on the imaginary axis and no two roots with opposite real part, and A and B are coprime.

Let $x_1 = a_1 + ib_1, \ldots, x_r = a_r + ib_r$, be the roots of P with multiplicities $\mu_1, \ldots, \mu_r$, c be a positive number smaller than the difference between two distinct absolute values of a_i, M a positive number bigger than twice the absolute value of the b_i. Consider for $t \in [0,1]$, and $i = 1, \ldots, r$,

$$x_{i,t} = (1-t)x_i + t(a_i + \frac{c}{M}b_i),$$

and the polynomial

$$P_t(X) = (X - x_{1,t})^{\mu_1} \ldots (X - x_{r,t})^{\mu_r}.$$

Note that $P_0 = P$, P_1 has only real roots, and for every $t \in [0,1]$ no two roots with opposite real parts, and hence for every $t \in [0,1]$, defining

$$(-i)^p P_t(iX) = A_t(X) + iB_t(X), A_t \in \mathrm{R}[X], B_t \in \mathrm{R}[X],$$

A_t and B_t are coprime. Thus $\mathrm{Res}(A_t, B_t) \neq 0$ and denoting by $M(A_t, B_t)$ the matrix of coefficients of $\mathrm{Bez}(A_t, B_t)$ in the canonical basis $X^{p-1}, \ldots, 1$, $\det(M(A_t, B_t)) \neq 0$. Thus the rank of $M(A_t, B_t)$ is constantly p as t varies in $[0,1]$. Hence the signature of $M(A_t, B_t)$ is constant as t varies in $[0,1]$. We have proved that, for every $t \in [0,1]$, $\mathrm{Ind}\left(\frac{B_t}{A_t}\right) = \mathrm{Ind}\left(\frac{B}{A}\right)$.

So, we need only to prove the claim for a polynomial P with all roots real and no opposite roots. This is done by induction on the degree of P.

The claim is obvious for a polynomial of degree 1 since if $P = X - a$, $A = X, B = a$, and $\mathrm{Ind}\left(\frac{a}{X}\right)$ is equal to 1 when $a > 0$ and -1 when $a < 0$.

Suppose that the claim is true for every polynomial of degree $< p$ and consider P of degree p. Let a be the root of P with minimum absolute value among the roots of P and $P = (X - a)Q$.

If $a > 0$, we are going to prove, denoting

$$(-i)^{p-1}Q(iX) = C(X) + iD(X), C \in \mathrm{R}[X], D \in \mathrm{R}[X],$$

that

$$\mathrm{Ind}\left(\frac{B}{A}\right) = \mathrm{Ind}\left(\frac{D}{C}\right) + 1. \tag{3.3}$$

We define $P_t = (X-t)Q$, $t \in (0,a]$ and denote

$$(-i)^p P_t(iX) = A_t(X) + iB_t(X), A_t \in \mathrm{R}[X], B_t \in \mathrm{R}[X].$$

Note that $P_a = P$, and for every $t \in (0,a]$, P_t has only real roots, no opposite roots, and A_t and B_t are coprime. Thus $\mathrm{Res}(A_t, B_t) \neq 0$ and denoting by $M(A_t, B_t)$ be the matrix of coefficients of $\mathrm{Bez}(A_t, B_t)$ in the canonical basis $X^{p-1}, \ldots, 1$, $\det(M(A_t, B_t)) \neq 0$. Thus the rank of $M(A_t, B_t)$ is constantly p as t varies in $(0,a]$. Thus the signature of $M(A_t, B_t)$ is constant as t varies in $(0,a]$. We have proved that, for every $t \in (0,a]$,

$$\mathrm{Ind}\Big(\frac{B_t}{A_t}\Big) = \mathrm{Ind}\Big(\frac{B}{A}\Big). \tag{3.4}$$

We now prove that

$$\mathrm{Ind}\Big(\frac{B_t}{A_t}\Big) = \mathrm{Ind}\Big(\frac{D}{C}\Big) + 1, \tag{3.5}$$

if t is small enough. Note that, since

$$\begin{aligned} A_t(X) + iB_t(X) &= (-i)^p P_t(iX) \\ = (X+it)(-i)^{p-1}Q(iX) &= (X+it)(C(X)+iD(X)), \end{aligned}$$

$$\begin{aligned} A_t(X) &= XC(X) - tD(X), \\ B_t(X) &= XD(X) + tC(X). \end{aligned}$$

For t small enough, A_t is close to $XC(X)$ and B_t close to $XD(X)$.

If p is even, $C(0) \neq 0$, $D(0) = 0$ since D is odd and C and D have no common root. For t small enough, using the continuity of roots, A_t has a simple root y close to 0. The sign of $B_t(y)$ is the sign of $tC(0)$. Hence for $[a,b]$ small enough containing 0, and t sufficiently small,

$$\mathrm{Ind}\Big(\frac{D}{C}; a, b\Big) = 0, \mathrm{Ind}\Big(\frac{B_t}{A_t}; a, b\Big) = 1.$$

If p is odd, $C(0) = 0$, $D(0) \neq 0$ since C is odd and C and D have no common root.

If $C'(0)D(0) > 0$, there is a jump from $-\infty$ to $+\infty$ in $\dfrac{D}{C}$ at 0, and $A_t(0)$ has two roots close to 0, one positive and one negative. Hence for $[a, b]$ small enough containing 0, and t sufficiently small,

$$\mathrm{Ind}\Big(\frac{D}{C}; a, b\Big) = 1, \mathrm{Ind}\Big(\frac{B_t}{A_t}; a, b\Big) = 2.$$

If $C'(0)D(0) < 0$, there is a jump from $+\infty$ to $-\infty$ in $\dfrac{D}{C}$ at 0 and $A_t(0)$ has no root close to 0. Hence for $[a, b]$ small enough containing 0, and t sufficiently small,

$$\mathrm{Ind}\Big(\frac{D}{C}; a, b\Big) = -1, \mathrm{Ind}\Big(\frac{B_t}{A_t}; a, b\Big) = 0.$$

Equation (3.5) follows. Equation (3.3) follows from Equation (3.4) and Equation (3.5).

If $a < 0$, a similar analysis, left to the reader, proves that

$$\mathrm{Ind}\Big(\frac{B}{A}\Big) = \mathrm{Ind}\Big(\frac{D}{C}\Big) - 1.$$

□

Proof of Theorem 3.1.1: If $p = 2m$, let

$$\varepsilon = \begin{cases} \mathrm{sign}_{x<0, x\to 0}\Big(\dfrac{G(x)}{F(x)}\Big) & \text{if } \lim_{x<0,x\to 0}\left|\dfrac{G(x)}{F(x)}\right| = \infty, \\ 0 & \text{otherwise.} \end{cases}$$

Then, since $A = F(-X^2), B = XG(-X^2)$,

$$\begin{aligned} \mathrm{Ind}\Big(\frac{B}{A}\Big) &= \mathrm{Ind}\Big(\frac{XG(-X^2)}{F(-X^2)}\Big) \\ = \mathrm{Ind}\Big(\frac{XG(-X^2)}{F(-X^2)}; -\infty, 0\Big) &+ \mathrm{Ind}\Big(\frac{XG(-X^2)}{F(-X^2)}; 0 + \infty\Big) + \varepsilon \\ &= 2\mathrm{Ind}\Big(\frac{XG(-X^2)}{F(-X^2)}; -\infty, 0\Big) + \varepsilon \end{aligned}$$

$$= -2\mathrm{Ind}\Big(\frac{G(-X^2)}{F(-X^2)}; -\infty, 0\Big) + \varepsilon$$
$$= -2\mathrm{Ind}\Big(\frac{G(X)}{F(X)}; -\infty, 0\Big) - \varepsilon$$
$$= -\mathrm{Ind}\Big(\frac{G(X)}{F(X)}; -\infty, 0\Big) + \mathrm{Ind}\Big(\frac{XG(X)}{F(X)}; -\infty, 0\Big) + \varepsilon$$
$$= -\mathrm{Ind}\Big(\frac{G}{F}\Big) + \mathrm{Ind}\Big(\frac{XG}{F}\Big).$$

If $p = 2m + 1$, let

$$\varepsilon = \begin{cases} \mathrm{sign}_{x<0,x\to 0}\Big(\frac{F(x)}{G(x)}\Big) & \text{if } \lim_{x<0,x\to 0}\Big(\frac{F(x)}{G(x)}\Big) \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

Then, since $A = XG(-X^2), B = -F(-X^2)$,

$$\mathrm{Ind}\Big(\frac{B}{A}\Big) = -\mathrm{Ind}\Big(\frac{F(-X^2)}{XG(-X^2)}\Big)$$
$$= -\mathrm{Ind}\Big(\frac{F(-X^2)}{XG(-X^2)}; -\infty, 0\Big) - \mathrm{Ind}\Big(\frac{F(-X^2)}{XG(-X^2)}; 0 + \infty\Big) - \varepsilon$$
$$= -2\mathrm{Ind}\Big(\frac{F(-X^2)}{XG(-X^2)}; -\infty, 0\Big) - \varepsilon$$
$$= -2\mathrm{Ind}\Big(\frac{F(X)}{XG(X)}; -\infty, 0\Big) - \varepsilon$$
$$= -\mathrm{Ind}\Big(\frac{F(X)}{XG(X)}; -\infty, 0\Big) + \mathrm{Ind}\Big(\frac{F(X)}{G(X)}; -\infty, 0\Big) - \varepsilon$$
$$= -\mathrm{Ind}\Big(\frac{F}{XG}\Big) + \mathrm{Ind}\Big(\frac{F}{G}\Big).$$

This proves the theorem, using Proposition 3.1.4. □

Proof of Theorem 3.1.2: If

$$P = a_pX^p + \ldots + a_0, a_p > 0$$

belongs to the domain of stability of degree p, it is the product of a_p, polynomials $X+u$ with $u > 0 \in \mathrm{R}$, and X^2+sX+t with $s > 0 \in \mathrm{R}, t >$

$0 \in \mathrm{R}$, and hence all the a_i, $i = 0, \ldots, p$, are strictly positive. Thus, F and G have no positive real root, and $\mathrm{sign}(F(0)G(0)) = \mathrm{sign}(a_0 a_1) = 1$. Hence,

if $p = 2m$ is even,

$$\mathrm{Ind}\Big(\frac{G}{F}\Big) = -\mathrm{Ind}\Big(\frac{XG}{F}\Big),$$

and

$$-p = -\mathrm{Ind}\Big(\frac{G}{F}\Big) + \mathrm{Ind}\Big(\frac{XG}{F}\Big) \Leftrightarrow m = \mathrm{Ind}\Big(\frac{G}{F}\Big),$$

if $p = 2m + 1$ is odd,

$$\mathrm{Ind}\Big(\frac{F}{XG}\Big) = -\mathrm{Ind}\Big(\frac{F}{G}\Big) + 1,$$

and

$$-p = -\mathrm{Ind}\Big(\frac{F}{XG}\Big) + \mathrm{Ind}\Big(\frac{F}{G}\Big) \Leftrightarrow m + 1 = \mathrm{Ind}\Big(\frac{F}{XG}\Big).$$

The proof of the theorem follows, using the results already seen on Cauchy index □

The domain of stability has attracted much attention, notably by Routh [6], Hurwitz [4], and Liénart/Chipart [5]. A whole chapter is devoted to this problem in [3].

3.2 Improved Sign Determination

We consider a general real closed field R, not necessarily archimedean. Note that the approximation of the elements of R by rational numbers cannot be performed. Our aim is to give a method for determining the sign conditions realized by a family of polynomials on a finite set Z of points in R^k.

Let Z be a finite subset of R^k. We denote

$$\begin{aligned}
\mathcal{R}(P = 0, Z) &= \{x \in Z \mid P(x) = 0\},\\
\mathcal{R}(P > 0, Z) &= \{x \in Z \mid P(x) > 0\},\\
\mathcal{R}(P < 0, Z) &= \{x \in Z \mid P(x) < 0\},
\end{aligned}$$

and $c(P=0,Z), c(P>0,Z), c(P<0,Z)$ the corresponding numbers of elements. The Sturm-query of P for Z is

$$\mathrm{SQ}(P,Z) = c(P>0,Z) - c(P<0,Z).$$

We consider the computation of $\mathrm{SQ}(P,Z)$ as a basic black box. We have already seen several algorithms for computing it when $Q \in \mathrm{R}[X]$, $Z = \mathrm{Z}(Q,\mathrm{R})$ (Algorithms 1.3.13 and 1.4.48). Later in the book, we shall see other algorithms for the multivariate case.

Consider $\mathcal{P} = P_1, \ldots, P_s$, a finite list of polynomials in $\mathrm{R}[X_1, \ldots, X_k]$.

Let σ be a sign condition on $\mathcal{P}$, i.e. an element of $\{0,1,-1\}^{\mathcal{P}}$. The **realization of the sign condition σ on Z** is

$$\mathcal{R}(\sigma, Z) = \{x \in Z \mid \wedge_{P\in\mathcal{P}} \mathrm{sign}(P(x)) = \sigma(P)\},$$

and its cardinality is denoted $c(\sigma, Z)$.

We write $\mathrm{Sign}(\mathcal{P}, Z)$ for the list of sign conditions realized by $\mathcal{P}$ on Z, i.e. the list of $\sigma \in \{0,1,-1\}^{\mathcal{P}}$ such that $\mathcal{R}(\sigma, Z)$ is non-empty, and $c(\mathcal{P}, Z)$ for the corresponding list of cardinals $c(\sigma, Z) = \#(\mathcal{R}(\sigma, Z))$ for $\sigma \in \mathrm{Sign}(\mathcal{P}, Z)$.

Our aim is to determine $\mathrm{Sign}(\mathcal{P}, Z)$, and, more precisely, to compute the numbers $c(\mathcal{P}, Z)$. The only information we are going to use to compute $\mathrm{Sign}(\mathcal{P}, Z)$ is the Sturm-query of products of elements of $\mathcal{P}$.

A method for sign determination in the univariate case was already presented earlier. This method can be easily generalized to the multivariate case, as we will see now.

Given $\alpha \in \{0,1,2\}^{\mathcal{P}}$, we write $\mathcal{P}^\alpha$ for $\prod_{P\in\mathcal{P}} P^{\alpha(P)}$. When $\mathcal{R}(\sigma, Z) \neq \emptyset$, the sign of $\mathcal{P}^\alpha$ is fixed on $\mathcal{R}(\sigma, Z)$ and is equal to $\prod_{P\in\mathcal{P}} \sigma(P)^{\alpha(P)}$, with the understanding that $0^0 = 1$. Hence, we define the sign of $\mathcal{P}^\alpha$ on σ, $\mathrm{sign}(\mathcal{P}^\alpha, \sigma)$, to be $\prod_{P\in\mathcal{P}} \sigma(P)^{\alpha(P)}$.

We order the elements of $\mathcal{P}$ so that $\mathcal{P} = \{P_1, \ldots, P_s\}$. As in Chapter 2, we order $\{0,1,2\}^{\mathcal{P}}$ lexicographically: $\alpha <_{\mathrm{lex}} \beta$ if and only if $\exists i, 1 \leq i \leq s$ such that $\alpha(P_i) < \beta(P_i)$ and, for all $j > i, \alpha(P_j) = \beta(P_j)$. We also order $\{0,1,-1\}^{\mathcal{P}}$ lexicographically: $\sigma <_{\mathrm{lex}} \tau$ if and only if $\exists i, 1 \leq i \leq s$, such that $\sigma(P_i) \prec \tau(P_i)$ and, for all $j > i, \sigma(P_j) = \tau(P_j)$ (with $0 \prec 1 \prec -1$).

Given $A = \alpha_1, \ldots, \alpha_m$, a list of elements of $\{0,1,2\}^{\mathcal{P}}$ with

$$\alpha_1 <_{\mathrm{lex}} \cdots <_{\mathrm{lex}} \alpha_m,$$

we write $\mathcal{P}^A$ for $\mathcal{P}^{\alpha_1}, \ldots, \mathcal{P}^{\alpha_m}$ and $\mathrm{SQ}(\mathcal{P}^A, Z)$ for $\mathrm{SQ}(\mathcal{P}^{\alpha_1}, Z), \ldots, \mathrm{SQ}(\mathcal{P}^{\alpha_m}, Z)$.

Given $\Sigma = \sigma_1, \ldots, \sigma_n$, a list of elements of $\{0, 1, -1\}^{\mathcal{P}}$, with

$$\sigma_1 <_{\mathrm{lex}} \cdots <_{\mathrm{lex}} \sigma_n,$$

we write $\mathcal{R}(\Sigma, Z)$ for $\mathcal{R}(\sigma_1, Z), \ldots, \mathcal{R}(\sigma_n, Z)$ and $c(\Sigma, Z)$ for $c(\sigma_1, Z), \ldots, c(\sigma_n, Z)$.

The **matrix of signs of $\mathcal{P}^A$ on** Σ is the $m \times n$ matrix $M(\mathcal{P}^A, \Sigma)$ whose i, j-th entry is $\mathrm{sign}(\mathcal{P}^{\alpha_i}, \sigma_j)$.

Proposition 3.2.1 *If* $\cup_{\sigma \in \Sigma} \mathcal{R}(\sigma, Z) = Z$, *then*

$$M(\mathcal{P}^A, \Sigma) \cdot c(\Sigma, Z) = \mathrm{SQ}(\mathcal{P}^A, Z).$$

Proof: This is obvious since the $(i, j)-$th entry of $M(\mathcal{P}^A, \Sigma)$ is the sign of the polynomial $\mathcal{P}^{\alpha_i}$ of $\mathcal{P}^A$ on the sign condition σ_j of Σ. □

When the matrix $M(\mathcal{P}^A, \Sigma)$ is invertible, we can express $c(\Sigma, Z)$ in terms of $\mathrm{SQ}(\mathcal{P}^A, Z)$.

Note also that when $\mathcal{P} = \{P\}$, $A = \{0, 1, 2\}^{\{P\}}$, and $\Sigma = \{0, 1, -1\}^{\{P\}}$, the conclusion of Proposition 3.2.1 is

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ 0 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} c(P = 0, Z) \\ c(P > 0, Z) \\ c(P < 0, Z) \end{bmatrix} = \begin{bmatrix} \mathrm{SQ}(1, Z) \\ \mathrm{SQ}(P, Z) \\ \mathrm{SQ}(P^2, Z) \end{bmatrix}. \qquad (3.6)$$

This is a generalization to Z of Equation (2.1) which had been stated for the set of zeroes of a univariate polynomial.

We shall express each $c(\sigma, Z)$ in terms of $\mathrm{SQ}(\mathcal{P}^\alpha, Z)$, using all $\alpha \in \{0, 1, 2\}^{\mathcal{P}}$. So we take $A = \{0, 1, 2\}^{\mathcal{P}}$ and $\Sigma = \{0, 1, -1\}^{\mathcal{P}}$.

As in Chapter 2, Notation 2.1.6, let M_s be the $3^s \times 3^s$ matrix defined inductively by

$$M_1 = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ 0 & 1 & 1 \end{bmatrix}$$

and

$$M_{t+1} = M_t \otimes M_1.$$

We generalize Proposition 2.1.8 and obtain

Proposition 3.2.2 *Let $\mathcal{P}$ be a set of polynomials with s elements, $A = \{0,1,2\}^{\mathcal{P}}$, and $\Sigma = \{0,1,-1\}^{\mathcal{P}}$ ordered lexicographically. Then,*

$$M(\mathcal{P}^A, \Sigma) = M_s.$$

Proof: The proof is by induction on s. If s=1, the claim is Equation (3.6). If the claim holds for s, it holds also for $s+1$ given the definitions of M_{s+1} and $M(\mathcal{P}^A, \Sigma)$, and the orderings on $A = \{0,1,2\}^{\mathcal{P}}$ and $\Sigma = \{0,1,-1\}^{\mathcal{P}}$. □

As a consequence:

Corollary 3.2.3

$$M_s \cdot c(\Sigma, Z) = \mathrm{SQ}(\mathcal{P}^A, Z).$$

The preceding results give the following algorithm for sign determination, by using repeatedly the Sturm-query black box.

Algorithm 3.2.4 (Naive Sign Determination) Input: *a finite subset $Z \subset \mathrm{R}^k$ with r elements and a finite list $\mathcal{P} = P_1, \ldots, P_s$ of polynomials of* $\mathrm{R}[X_1, \ldots, X_k]$.

Output: *the list of sign conditions realized by $\mathcal{P}$ on Z,* $\mathrm{Sign}(\mathcal{P}, Z)$.

Blackbox: *For a polynomial P, the Sturm-query* $\mathrm{SQ}(P, Z)$.

Procedure: *Define $A = \{0,1,2\}^{\mathcal{P}}$ and $\Sigma = \{0,1,-1\}^{\mathcal{P}}$, ordered lexicographically. Call the Sturm-query black box 3^s times with input the elements of $\mathcal{P}^A$ to obtain* $\mathrm{SQ}(\mathcal{P}^A, Z)$. *Solve the $3^s \times 3^s$ system*

$$M_s \cdot c(\Sigma, Z) = \mathrm{SQ}(\mathcal{P}^A, Z)$$

to obtain the vector $c(\Sigma, Z)$of length 3^s. Keep the sign conditions σ with $c(\sigma, Z) \neq 0$

Complexity analysis: The number of calls to the Sturm-query black box is 3^s. The calls to the Sturm-query black box are done for polynomials which are products of at most s polynomials of the form P or P^2, $P \in \mathcal{P}$. □

To avoid the exponential number of calls to the Sturm-query black box in Algorithm 3.2.4 (Naive Sign Determination), notice that

$$\#(\mathrm{Sign}(\mathcal{P}, Z)) \leq \#(Z),$$

so that the number of realizable sign conditions does not exceed $\#(Z)$. We are now going to determine the non-empty sign conditions inductively getting rid of the empty sign conditions at each step of the computation, in order to control the size of the data we manipulate.

Notation 3.2.5 We need to introduce some more notation. Let $\mathcal{P}_i = P_1, \ldots, P_i$. For $\sigma \in \{0, 1, -1\}^{\mathcal{P}_{i-1}}$ and $\tau \in \{0, 1, -1\}$, we define $\sigma \wedge \tau$ to be the element of $\{0, 1, -1\}^{\mathcal{P}_i}$ defined by

$$\begin{cases} (\sigma \wedge \tau)(P) = \sigma(P) & \text{if } P \in \mathcal{P}_{i-1}, \\ (\sigma \wedge \tau)(P_i) = \tau. \end{cases}$$

If $\Sigma = \sigma_1, \ldots, \sigma_m$ is a list of elements of $\{0, 1, -1\}^{\mathcal{P}_i}$ with

$$\sigma_1 <_{\mathrm{lex}} \ldots <_{\mathrm{lex}} \sigma_m$$

and $T = \tau_1, \ldots, \tau_n$ is a list of element of $\{0, 1, -1\}$ with

$$\tau_1 <_{\mathrm{lex}} \ldots <_{\mathrm{lex}} \tau_n,$$

then $\Sigma \wedge T$ is the list

$$\sigma_1 \wedge \tau_1 <_{\mathrm{lex}} \ldots <_{\mathrm{lex}} \sigma_1 \wedge \tau_n <_{\mathrm{lex}} \ldots <_{\mathrm{lex}} \sigma_m \wedge \tau_1 <_{\mathrm{lex}} \ldots <_{\mathrm{lex}} \sigma_m \wedge \tau_n.$$

For $\alpha \in \{0, 1, 2\}^{\mathcal{P}_{i-1}}$ and $\beta \in \{0, 1, 2\}$, we define $\alpha \times \beta \in \{0, 1, 2\}^{\mathcal{P}_i}$ by

$$\begin{cases} (\alpha \times \beta)(P) = \alpha(P) & \text{if } P \in \mathcal{P}_{i-1}, \\ (\alpha \times \beta)(P_i) = \beta. \end{cases}$$

If $A = \alpha_1 <_{\mathrm{lex}} \ldots <_{\mathrm{lex}} \alpha_m$ and $B = \beta_1 <_{\mathrm{lex}} \ldots <_{\mathrm{lex}} \beta_n$ are lists of elements of $\{0, 1, 2\}^{\mathcal{P}_{i-1}}$ and $\{0, 1, 2\}$ we define $A \times B$ to be the list

$$\alpha_1 \times \beta_1 <_{\mathrm{lex}} \ldots <_{\mathrm{lex}} \alpha_1 \times \beta_n <_{\mathrm{lex}} \ldots <_{\mathrm{lex}} \alpha_m \times \beta_1 <_{\mathrm{lex}} \ldots <_{\mathrm{lex}} \alpha_m \times \beta_n$$

in $\{0, 1, 2\}^{\mathcal{P}_i}$.

The list ${\mathcal{P}_i}^{A \times B}$ is defined to be

$$\mathcal{P}_{i-1}^{\alpha_1} P_i^{\beta_1}, \ldots, \mathcal{P}_{i-1}^{\alpha_1} P_i^{\beta_n}, \ldots, \mathcal{P}_{i-1}^{\alpha_m} P_i^{\beta_1}, \ldots \mathcal{P}_{i-1}^{\alpha_m} P_i^{\beta_n}.$$

Recall that the matrix of signs of $\mathcal{P}^A$ (of length m) on Σ (of length n) is the $m \times n$ matrix $M(\mathcal{P}^A, \Sigma)$ whose i, j-th entry is $\mathrm{sign}(\mathcal{P}^{\alpha_i}, \sigma_j)$ and that $\mathrm{SQ}(\mathcal{P}^A, Z)$ is the vector $\mathrm{SQ}(\mathcal{P}^{\alpha_1}, Z), \ldots, \mathrm{SQ}(\mathcal{P}^{\alpha_m}, Z)$. Using Notation 2.1.4 we have

Proposition 3.2.6 *If* $\cup_{\sigma \in \Sigma} \mathcal{R}(\sigma, Z) = Z$ *and* $B = 0, 1, 2$,

$$(M(\mathcal{P}_{i-1}^A, \Sigma) \otimes M(\{P_i\}^B, T))c(\Sigma \wedge T, Z) = \mathrm{SQ}(\mathcal{P}_i^{A \times B}, Z).$$

Proof: Immediate from Proposition 3.2.1. □

Let $Z \subset \mathrm{R}^k$ be a finite set, and let $\mathcal{P}$ be a finite list of polynomials of $\mathrm{R}[X_1, \ldots, X_k]$. A list A of elements in $\{0, 1, 2\}^{\mathcal{P}}$ is **adapted to sign determination for $\mathcal{P}$ on Z** if the matrix of signs of $\mathcal{P}^A$ over $\mathrm{Sign}(\mathcal{P}, Z)$ is invertible.

Example 3.2.7 Consider the set of polynomials $\{P_i\}$. In this case, $\{0, 1, 2\}^{\{P_i\}}$ can be identified with $\{0, 1, 2\}$. Note that when Z is non-empty, $\mathrm{Sign}(\{P_i\}, Z)$ is also non-empty.

If $\mathrm{Sign}(\{P_i\}, Z) = \{0, 1, -1\}$, $B_i = 0, 1, 2$ is adapted to sign determination for $\{P_i\}$ on Z, since $\{P_i\}^{0,1,2} = 1, P_i, P_i^2$, and the matrix M_i of signs of $1, P_i, P_i^2$ over $0, 1, -1$ is $\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ 0 & 1 & 1 \end{bmatrix}$, which is invertible.

If $\mathrm{Sign}(\{P_i\}, Z) = \{1, -1\}$ (respectively $\{0, 1\}$, respectively $\{0, -1\}$), $B_i = 0, 1$ is adapted to sign determination for $\{P_i\}$ on Z, since $\{P_i\}^{0,1} = 1, P_i$ and the matrix of signs M_i of $1, P_i$ over $1, -1$ (respectively $0, 1$, respectively $0, -1$) is $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ (respectively $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, respectively $\begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}$), which is invertible.

If $\mathrm{Sign}(\{P_i\}, Z) = \{0\}$ (respectively $\{1\}$, respectively $\{-1\}$), $B_i = 0$ is adapted to sign determination for $\{P_i\}$ on Z, since $\{P_i\}^0 = 1$ and the matrix M_i of signs of 1 over 0 (respectively 1, respectively -1) is $[\,1\,]$, which is invertible.

Definition 3.2.8 Let $Z \subset \mathrm{R}^k$ be a finite set, let $\mathcal{P} = P_1, \ldots, P_s$ be a finite list of polynomials of $\mathrm{R}[X_1, \ldots, X_k]$, and let $\mathcal{P}_i = P_1, \ldots, P_i$, for $0 \leq i \leq s$. We now describe a method for determining inductively a list $A_i(Z)$ of elements in $\{0, 1, 2\}^{\mathcal{P}_i}$ adapted to sign determination for $\mathcal{P}_i$ on Z.

The case $i = 1$ has been already treated in Example 3.2.7.

Choose i, $1 \leq i \leq s$, and consider P_i. Let $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_1$ (respectively $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_2$, respectively $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_3$) be the subset of $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)$ of sign conditions which are partitioned into at least 1 (respectively 2, respectively 3) distinct subsets by sign conditions on P_i.

Let

$$Z' = \bigcup_{\sigma \in \mathrm{Sign}(\mathcal{P}_{i-1}, Z)_2 \cup \mathrm{Sign}(\mathcal{P}_{i-1}, Z)_3} \mathcal{R}(\sigma, Z), \tag{3.7}$$

$$Z'' = \bigcup_{\sigma \in \mathrm{Sign}(\mathcal{P}_{i-1}, Z)_3} \mathcal{R}(\sigma, Z). \tag{3.8}$$

Note that

$$\begin{aligned} \mathrm{Sign}(\mathcal{P}_{i-1}, Z') &= \mathrm{Sign}(\mathcal{P}_{i-1}, Z)_2 \cup \mathrm{Sign}(\mathcal{P}_{i-1}, Z)_3, \\ \mathrm{Sign}(\mathcal{P}_{i-1}, Z') &= \mathrm{Sign}(\mathcal{P}_{i-1}, Z)_3. \end{aligned}$$

Let

$$\begin{aligned} r_{i-1} &= \#(\mathrm{Sign}(\mathcal{P}_{i-1}, Z)), \\ r_{i-1,1} &= \#(\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_2) \cup \mathrm{Sign}(\mathcal{P}_{i-1}, Z)_3), \\ r_{i-1,2} &= \#(\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_3), \\ r_i &= \#(\mathrm{Sign}(\mathcal{P}_i, Z)). \end{aligned}$$

Then $r_i = r_{i-1} + r_{i-1,1} + r_{i-1,2}$.

Consider the matrix $M(\mathcal{P}_{i-1}^{A_{i-1}(Z)}, \mathrm{Sign}(\mathcal{P}_{i-1}, Z'))$ and extract from it the first $r_{i-1,1}$ linearly independent rows defining a list $A_{i-1}(Z')$ adapted to sign determination on Z'.

Similarly, consider the matrix $M(\mathcal{P}_{i-1}^{A_{i-1}(Z)}, \mathrm{Sign}(\mathcal{P}_{i-1}, Z''))$ and extract from it the first $r_{i-1,2}$ linearly independent rows defining a list $A_{i-1}(Z'')$ adapted to sign determination on Z''.

Define

$$A_i(Z) = A_{i-1}(Z) \times 0, A_{i-1}(Z') \times 1, A_{i-1}(Z'') \times 2.$$

If $\tau \in \mathrm{Sign}(\mathcal{P}_i, Z)$, we denote by $\tau' \in \mathrm{Sign}(\mathcal{P}_{i-1}, Z)$ the sign condition defined by $\tau'(P_j) = \tau(P_j)$,$j < i$.

Proposition 3.2.9 *The list $A_i(Z)$ is adapted to sign determination for $\mathcal{P}_i$ on Z.*

Proof: The proof is by induction on i. The claim is obviously true for $i = 1$.

The r_{i-1} first rows of $M(\mathcal{P}_i^{A_i(Z)}, \mathrm{Sign}(\mathcal{P}_i, Z))$ are obtained as follows. Let C_σ be the column of $M(\mathcal{P}_{i-1}^{A_{i-1}(Z)}, \mathrm{Sign}(\mathcal{P}_{i-1}, Z))$ corresponding to $\sigma \in \mathrm{Sign}(\mathcal{P}_{i-1}, Z)$.

For every $\tau \in \mathrm{Sign}(\mathcal{P}_i, Z)$, let the column of $M(\mathcal{P}_{i-1}^{A_{i-1}(Z)}, \mathrm{Sign}(\mathcal{P}_i, Z))$ with index τ be $C_{\tau'}$. The $r_{i-1,1}$ following rows of $M(\mathcal{P}_i^{A_i(Z)}, \mathrm{Sign}(\mathcal{P}_i, Z))$, are obtained as follows. Let C_σ be the column of $M(\mathcal{P}_{i-1}^{A_{i-1}(Z')}, \mathrm{Sign}(P_{i-1}, Z))$ corresponding to $\sigma \in \mathrm{Sign}(\mathcal{P}_{i-1}, Z)$. For every $\tau \in \mathrm{Sign}(\mathcal{P}_i, Z)$, let the column of $M(\mathcal{P}_{i-1}^{A_{i-1}(Z')\times 1}, \mathrm{Sign}(\mathcal{P}_i, Z))$ with index τ be $\tau(P_i)C_{\tau'}$.

The $r_{i-1,2}$ following rows of $M(\mathcal{P}_i^{A_i(Z)}, \mathrm{Sign}(\mathcal{P}_i, Z))$, are obtained as follows. Let C_σ be the column of $M(\mathcal{P}_{i-1}^{A_{i-1}(Z'')}, \mathrm{Sign}(P_{i-1}, Z))$ corresponding to $\sigma \in \mathrm{Sign}(\mathcal{P}_{i-1}, Z)$. For every $\tau \in \mathrm{Sign}(\mathcal{P}_i, Z)$, let the column of $M(\mathcal{P}_{i-1}^{A_{i-1}(Z'')}P_i^2, \mathrm{Sign}(\mathcal{P}_i, Z))$ with index τ be $\tau(P_i)^2 C_{\tau'}$.

We want to prove that $M(\mathcal{P}_i^{A_i(Z)}, \mathrm{Sign}(\mathcal{P}_i, Z))$ is invertible. Denoting by C_τ the column of $M(\mathcal{P}_i^{A_i(Z)}, \mathrm{Sign}(P_i, Z))$ indexed by τ, consider a zero linear combination of columns of $M(\mathcal{P}_i^{A_i(Z)}, \mathrm{Sign}(P_i, Z))$:

$$\sum_{\tau \in \mathrm{Sign}(P_i, Z)} \lambda_\tau C_\tau = 0.$$

We want to prove that all λ_τ are zero. If $\sigma \in \mathrm{Sign}(\mathcal{P}_{i-1}, Z)_3$, we denote by $\sigma_1 <_{\mathrm{lex}} \sigma_2 <_{\mathrm{lex}} \sigma_3$ the sign conditions $\mathrm{Sign}(\mathcal{P}_i, Z)$ of such that $\sigma_1' = \sigma_2' = \sigma_3' = \sigma$. Similarly, if $\sigma \in \mathrm{Sign}(\mathcal{P}_{i-1}, Z)_2$, we denote by $\sigma_1 <_{\mathrm{lex}} \sigma_2$ the sign conditions of $\mathrm{Sign}(\mathcal{P}_i, Z)$ such that $\sigma_1' = \sigma_2' = \sigma$. Finally if $\sigma \in \mathrm{Sign}(\mathcal{P}_{i-1}, Z)_1$ we denote by σ_1 the sign condition of $\mathrm{Sign}(\mathcal{P}_i, Z)$ such that $\sigma_1' = \sigma$.

Since $M(\mathcal{P}_{i-1}^{A_{i-1}(Z)}, \mathrm{Sign}(P_{i-1}, Z))$ is invertible, by the induction hypothesis, $\lambda_{\sigma_1} = 0$, for every $\sigma \in \mathrm{Sign}(\mathcal{P}_{i-1}, Z)_1$.

Now using the fact that, by the induction hypothesis,

$$M(\mathcal{P}_{i-1}^{A_{i-1}(Z')}, \mathrm{Sign}(P_{i-1}, Z'))$$

is invertible, for every $\sigma \in \mathrm{Sign}(\mathcal{P}_{i-1}, Z)_2$

$$\lambda_{\sigma_1} + \lambda_{\sigma_2} = \sigma_1(P_i)\lambda_{\sigma_1} - \sigma_2(P_i)\lambda_{\sigma_2} = 0.$$

Thus $\lambda_{\sigma_1} = \lambda_{\sigma_2} = 0$, for every $\sigma \in \mathrm{Sign}(\mathcal{P}_{i-1}, Z)_2$.

Finally, using the fact that, by the induction hypothesis,

$$M(\mathcal{P}_{i-1}^{A_{i-1}(Z'')}, \mathrm{Sign}(P_{i-1}, Z''))$$

is invertible, for every $\sigma \in \mathrm{Sign}(\mathcal{P}_{i-1}, Z)_3$

$$\lambda_{\sigma_1} + \lambda_{\sigma_2} + \lambda_{\sigma_3} = \lambda_{\sigma_2} - \lambda_{\sigma_3} = \lambda_{\sigma_2} + \lambda_{\sigma_3} = 0.$$

Thus $\lambda_{\sigma_1} = \lambda_{\sigma_2} = \lambda_{\sigma_3} = 0$ for every $\sigma \in \mathrm{Sign}(\mathcal{P}_{i-1}, Z)_3$.

This proves that the matrix $M(\mathcal{P}_i^{A_i(Z)}, \mathrm{Sign}(\mathcal{P}_i, Z))$ is invertible. □

Remark 3.2.10 The list $A_i(Z) \subset \{0,1,2\}^{\mathcal{P}_i}$ adapted to sign determination constructed above depends only on the list of non-empty sign conditions $\mathrm{Sign}(\mathcal{P}, Z)$, since the list $A_i(Z) \subset \{0,1,2\}^{\mathcal{P}_i}$ is constructed inductively from $A_{i-1}(Z)$ and $\mathrm{Sign}(\mathcal{P}_i, Z)$.

We are now ready for the Sign Determination algorithm.

Algorithm 3.2.11 (Sign Determination) Input: *a finite subset $Z \subset \mathrm{R}^k$ with r elements and a finite list $\mathcal{P} = P_1, \ldots, P_s$ of polynomials in $\mathrm{R}[X_1, \ldots, X_k]$.*

Output: *the list of sign conditions realized by $\mathcal{P}$ on Z, $\mathrm{Sign}(\mathcal{P}, Z)$.*

Blackbox: *for a polynomial P, the Sturm-query $\mathrm{SQ}(P, Z)$.*

Procedure:

Use the Sturm-query black box with input 1 to determine $r = \mathrm{SQ}(1, Z)$. If $r = 0$, output $\emptyset$.

Initialization: $\mathrm{Sign}(\mathcal{P}_0, Z) := \emptyset, A_0(Z) := \emptyset$.

```
Let $\mathcal{P}_i = P_1, \ldots, P_i$. We are going to determine iteratively, for i from
    1 to s, $\mathrm{Sign}(\mathcal{P}_i, Z)$ the non-empty sign conditions for $\mathcal{P}_i$ on $Z$.
    More precisely, we are going to compute $\mathrm{Sign}(\mathcal{P}_i, Z)$ and $A_i(Z)$,
    a list of elements in $\{0,1,2\}^{\mathcal{P}_i}$ adapted to sign determination for
    $\mathcal{P}_i$ on $Z$. starting from $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)$ and $A_{i-1}(Z)$ .

For i from 1 to s

        Determine $\mathrm{Sign}(\mathcal{P}_i, Z)$, the list of sign conditions realized by $P_i$
            on $Z$, and a list $B_i$ of elements in $\{0,1,2\}$ adapted to sign
            determination for $P_i$ on $Z$ as follows:
            Use the Sturm-query black box with inputs $P_i$ and $P_i^2$ to
                determine $\mathrm{SQ}(P_i, Z)$ and $\mathrm{SQ}(P_i^2, Z)$.
            From these values, using the equality

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} c(P_i = 0, Z) \\ c(P_i > 0, Z) \\ c(P_i < 0, Z) \end{bmatrix} = \begin{bmatrix} \mathrm{SQ}(1, Z) \\ \mathrm{SQ}(P_i, Z) \\ \mathrm{SQ}(P_i^2, Z) \end{bmatrix},$$

                compute $c(P_i = 0, Z)$, $c(P_i > 0, Z)$ and $c(P_i < 0, Z)$ and
                output $\mathrm{Sign}(P_i, Z)$.
            If $r(P_i) = \#(\mathrm{Sign}(P_i, Z)) = 3$, output $B_i = \{0,1,2\}$.
            If $r(P_i) = \#(\mathrm{Sign}(P_i, Z)) = 2$, output $B_i = \{0,1\}$.
            If $r(P_i) = \#(\mathrm{Sign}(P_i, Z)) = 1$, output $B_i = \{0\}$.
            Define $M_i = M(P_i^{B_i}, \mathrm{Sign}(P_i, Z))$.
        Compute $\mathrm{Sign}(\mathcal{P}_i, Z)$, the list of sign conditions realized by $\mathcal{P}_i$
            on $Z$, as follows:
            Use the Sturm-query black box with input the elements of
                $\mathcal{P}_i^{A_{i-1}(Z) \times B_i}$ to determine $d' = \mathrm{SQ}(\mathcal{P}_i^{A_{i-1}(Z) \times B_i}, Z)$.
            Take the matrix

$$M_i' := M(\mathcal{P}_{i-1}^{A_{i-1}(Z)}, \mathrm{Sign}(\mathcal{P}_{i-1}, Z)) \otimes M_i.$$

                Compute the list $c' = c(\mathrm{Sign}(\mathcal{P}_{i-1}, Z) \wedge \mathrm{Sign}(P_i, Z))$ from
                the equality $M_i' \cdot c' = d'$ by inverting $M_i'$. Compute
                $\mathrm{Sign}(\mathcal{P}_i, Z)$, removing from $\mathrm{Sign}(\mathcal{P}_{i-1}, Z) \wedge \mathrm{Sign}(P_i, Z)$
                the sign conditions with empty realization, which corre-
                spond to the zeroes in $c'$.
```

Let $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_1$ *(respectively* $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_2$*) be the subset of* $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)$ *of sign conditions that are partitioned into at least* 2 *(respectively 3) distinct subsets by sign conditions on* P_i*. Extract from* $M(\mathcal{P}_{i-1}^{A_{i-1}(Z)})$ *the corresponding columns to get* $M(\mathcal{P}_{i-1}^{A_{i-1}(Z)}, \mathrm{Sign}(\mathcal{P}_{i-1}, Z'))$ *(respectively* $M(\mathcal{P}_{i-1}^{A_{i-1}(Z)}, \mathrm{Sign}(\mathcal{P}_{i-1}, Z''))$*) (see (3.7) and (3.8)). Determine the set* $A_{i-1}(Z') \subset A_{i-1}(Z)$ *(respectively* $A_{i-1}(Z'') \subset A_{i-1}(Z)$*) indexing the first independent* $r_{i-1,1}$ *(resp* $r_{i-1,2}$*) rows of* $M(\mathcal{P}_{i-1}^{A_{i-1}(Z)}, \mathrm{Sign}(\mathcal{P}_{i-1}, Z'))$ *(respectively* $M(\mathcal{P}_{i-1}^{A_{i-1}(Z)}, \mathrm{Sign}(\mathcal{P}_{i-1}, Z''))$*). Take*

$$A_i(Z) = A_{i-1}(Z) \times 0, A_{i-1}(Z') \times 1, A_{i-1}(Z'') \times 2.$$

Output $\mathrm{Sign}(\mathcal{P}, Z) = \mathrm{Sign}(\mathcal{P}_s, Z)$.

Remark 3.2.12 We denote by $\mathcal{B}(\mathrm{Sign}(\mathcal{P}, Z)) \subset \{0,1,2\}^{\mathcal{P}}$ the set constructed inductively as follows:

$$\mathcal{B}(\mathrm{Sign}(\mathcal{P}_1, Z)) = \{0,1,2\}_1$$
$$\mathcal{B}(\mathrm{Sign}(\mathcal{P}_{i+1}, Z)) = \mathcal{B}(\mathrm{Sign}(\mathcal{P}_i, Z)) \cup \{0,1,2\}_{i+1} \cup A_i(Z) \times B_i,$$

denoting by $\{0,1,2\}_i$ the subset of $\{0,1,2\}^{\mathcal{P}}$ with three elements defined by

$$\alpha \in \{0,1,2\}_i \text{ if and only if } \alpha(j) = 0\ \forall j \neq i,$$

and identifying $\alpha \in \{0,1,2\}^{\mathcal{P}_i}$ with $\alpha' \in \{0,1,2\}^{\mathcal{P}}$ such that

$$\alpha'(P_j) = \alpha(P_j), j \leq i, \alpha'(P_j) = 0, j > i,$$

and using the notation of the algorithm. It is clear that $\mathcal{B}(\mathrm{Sign}(\mathcal{P}, Z))$ is nothing but the list of elements $\alpha \in \{0,1,2\}^{\mathcal{P}}$ such that the Sturm-query of P^α has been computed in the algorithm. Using Remark 3.2.10, it is clear that $\mathcal{B}(\mathrm{Sign}(\mathcal{P}, Z))$ can be determined from $\mathrm{Sign}(\mathcal{P}, Z)$.

Before discussing the correctness and complexity of the Sign Determination Algorithm, we first give an example.

Example 3.2.13 Consider

$$Q = (X^3 - 1)(X^2 - 9), Z = \mathrm{Z}(P, R)$$
$$P_1 = X, P_2 = X + 1, P_3 = X - 2,$$

$Z = \mathrm{Z}(P, \mathbb{Q})$. The call to the Sturm-query black box with input 1 determines $\mathrm{SQ}(1, Z) = 3$. So P has 3 real roots (which is not a real surprise).

The call to the Sturm-query black box with inputs P_1 and P_1^2 determines $\mathrm{SQ}(P_1, Z) = 1$ and $\mathrm{SQ}(P_1^2, Z) = 3$. Thus

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ 0 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} c(P_1 = 0, Z) \\ c(P_1 > 0, Z) \\ c(P_1 < 0, Z) \end{bmatrix} = \begin{bmatrix} 3 \\ 1 \\ 3 \end{bmatrix},$$

which means, after solving the system, that P has

$$\begin{cases} 0 & \text{root with } P_1 = 0 \\ 2 & \text{roots with } P_1 > 0 \\ 1 & \text{root with } P_1 < 0 \end{cases}.$$

Hence $c(P_1 = 0, Z) = 0$. So we have $\mathrm{Sign}(P_1, Z) = 1, -1$ and $A_1 = B_1 = 0, 1$. The matrix $M(\mathcal{P}_1^{A_1}, \mathrm{Sign}(\mathcal{P}_1, Z))$ of signs of $\mathcal{P}_1^{0,1} = 1, P_1$ on $1, -1$ is $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.

We now consider $\mathcal{P}_2 = P_1, P_2$.

The call to the Sturm-query black box with inputs P_2 and P_2^2 determines $\mathrm{SQ}(P_2, Z) = 1, \mathrm{SQ}({P_2}^2, Z) = 3$. Hence,

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ 0 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} c(P_2 = 0, Z) \\ c(P_2 > 0, Z) \\ c(P_2 < 0, Z) \end{bmatrix} = \begin{bmatrix} 3 \\ 1 \\ 3 \end{bmatrix},$$

which means, after solving the system, that P has

$$\begin{cases} 0 & \text{root with } P_2 = 0 \\ 2 & \text{roots with } P_2 > 0 \\ 1 & \text{root with } P_2 < 0 \end{cases}.$$

Hence $c(P_2 = 0, Z) = 0$. So we have $\mathrm{Sign}(P_2, Z) = 1, -1$ and $B_2 = 0, 1$. The matrix M_2 of signs of $\{P_2\}^{0,1} = 1, P_2$ on $1, -1$ is $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.

The call to the Sturm-query black box with input P_1P_2 determines $\mathrm{SQ}(P, P_1P_2)$, which is equal to 3. Hence we have

$$M_2' = M(\mathcal{P}_1^{A_1}, \mathrm{Sign}(\mathcal{P}_1, Z)) \otimes M_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} c(P_1 > 0 \wedge P_2 > 0, Z) \\ c(P_1 > 0 \wedge P_2 < 0, Z) \\ c(P_1 < 0 \wedge P_2 > 0, Z) \\ c(P_1 < 0 \wedge P_2 < 0, Z) \end{bmatrix} = \begin{bmatrix} 3 \\ 1 \\ 1 \\ 3 \end{bmatrix}.$$

Solving the system we find that P has

$$\begin{cases} 2 & \text{roots with } P_1 > 0 \text{ and } P_2 > 0 \\ 0 & \text{roots with } P_1 > 0 \text{ and } P_2 < 0 \\ 0 & \text{roots with } P_1 < 0 \text{ and } P_2 > 0 \\ 1 & \text{root with } P_1 < 0 \text{ and } P_2 < 0 \end{cases}.$$

Hence $c(P_1 > 0 \wedge P_2 < 0, Z) = c(P_1 < 0 \wedge P_2 > 0, Z) = 0$. So we have $\mathrm{Sign}(\mathcal{P}_2, Z) = (1,1), (-1,-1)$. There is no sign condition on P_1 which is partitioned by sign conditions on P_2, so $A_2 = (0,0), (1,0)$. The matrix $M(\mathcal{P}_2^{A_2}, \mathrm{Sign}(\mathcal{P}_2, Z))$ of signs of $\mathcal{P}_2^{(0,0),(1,0)} = 1, P_1$ on $(1,1), (-1,-1)$ is $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.

Finally we consider $\mathcal{P} = P_1, P_2, P_3$.

The call to the Sturm-query black box with inputs P_3 and P_3^2 determines $\mathrm{SQ}(P_3, Z) = -1, \mathrm{SQ}({P_3}^2, Z) = 3$. Hence $c(P_3 = 0, Z) = 0$. So,

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ 0 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} c(P_3 = 0, Z) \\ c(P_3 > 0, Z) \\ c(P_3 < 0, Z) \end{bmatrix} = \begin{bmatrix} 3 \\ -1 \\ 3 \end{bmatrix},$$

which means, after solving the system, that P has

$$\begin{cases} 0 & \text{root with } P_3 = 0 \\ 1 & \text{root with } P_3 > 0 \\ 2 & \text{roots with } P_3 < 0 \end{cases}.$$

So we have $\mathrm{Sign}(P_3, Z) = \{1, -1\}$, $B_3 = \{0, 1\}$. The matrix M_3 of signs of $\{P_3\}^{0,1} = 1, P_3$ on $1, -1$ is $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.

The call to the Sturm-query black box with input P_1P_3 determines $\mathrm{SQ}(P_1P_3,$
$Z)$ which is equal to 1. Hence we have

$$M_3' = M(\mathcal{P}_2^{A_2}, \mathrm{Sign}(\mathcal{P}_2, Z)) \otimes M_3 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} c(P_1 > 0, P_2 > 0, P_3 > 0, Z) \\ c(P_1 > 0, P_2 > 0, P_3 < 0, Z) \\ c(P_1 < 0, P_2 < 0, P_3 > 0, Z) \\ c(P_1 < 0, P_2 < 0, P_3 < 0, Z) \end{bmatrix} = \begin{bmatrix} 3 \\ 1 \\ -1 \\ 1 \end{bmatrix}.$$

Solving the system, we find that P has

$$\begin{cases} 1 & \text{root with } P_1 > 0 \text{ and } P_2 > 0 \text{ and } P_3 > 0 \\ 1 & \text{root with } P_1 > 0 \text{ and } P_2 > 0 \text{ and } P_3 < 0 \\ 0 & \text{root with } P_1 < 0 \text{ and } P_2 < 0 \text{ and } P_3 > 0 \\ 1 & \text{root with } P_1 < 0 \text{ and } P_2 < 0 \text{ and } P_3 < 0 \end{cases}.$$

So we have $\mathrm{Sign}(\mathcal{P}) = \{(1, 1, 1), (1, 1, -1), (-1, -1, -1)\}$. There is only one sign condition which is partitioned into exactly two sign conditions by sign conditions on P_3, thus $A = \{(0, 0, 0), (1, 0, 0), (0, 0, 1)\}$.

Proof of correctness of Algorithm 3.2.11: It follows from Corollary 3.2.6 and from Proposition 3.2.9. □

In order to study the complexity of the Algorithm 3.2.11 (Sign Determination) we need the following proposition.

Proposition 3.2.14 *Let Z be a finite subset of R^k and $r = \#(Z)$. Consider $A_s(Z) \subset \{0, 1, 2\}^{\mathcal{P}}$ computed by Algorithm 3.2.11 (Sign Determination). For every $\alpha \in A_s(Z)$, the number $\#(\{P \in \mathcal{P} \mid \alpha(P) \neq 0\})$ is at most* $\log_2(r)$.

We need the following definition. Let α and β be elements of $\{0,1,2\}^{\mathcal{P}}$. We say that β precedes α if for every $P \in \mathcal{P}$, $\beta(P) \neq 0$ implies $\beta(P) = \alpha(P)$. Note that if β precedes α, then $\beta <_{\text{lex}} \alpha$.

Proof of Proposition 3.2.14 : Let α be such that $\#(\{P \in \mathcal{P} \mid \alpha(P) \neq 0\}) = k$. Since the number of elements β of $\{0,1,2\}^{\mathcal{P}}$ preceding α is 2^k, and the total number of polynomials in A_s is at most r, we have $2^k \leq r$ and $k \leq \log_2(r)$. So, the proposition follows immediately from the next lemma. □

Lemma 3.2.15 *If β precedes α and $\alpha \in A_s(Z)$ then $\beta \in A_s(Z)$*

Proof: We prove by induction on i that, for every finite set Z, if $\beta \notin A_i(Z)$ then $\alpha \notin A_i(Z)$. The claim is obvious for $i = 1$. If $\alpha \in \{0,1,2\}^{\mathcal{P}_i}$ we denote by α' the element of $\{0,1,2\}^{\mathcal{P}_{i-1}}$ such that $\alpha'(P_j) = \alpha(P_j)$, $j < i$. Note that, by definition of $A_i(Z)$, if $\alpha' \notin A_{i-1}(Z)$, $\alpha \notin A_i(Z)$.

Suppose that β precedes α and that $\beta \notin A_i(Z)$. There are several cases to consider:

If $\alpha(P_i) = 0$, then $\beta(P_i) = 0$ and $\beta' \notin A_{i-1}(Z)$ by definition of A_i. By the induction hypothesis, $\alpha' \notin A_{i-1}(Z)$ and $\alpha = \alpha' \times 0 \notin A_i(Z)$ by the definition of $A_i(Z)$.

If $\alpha(P_i) = 1$ (respectively 2), and $\beta(P_i) = 0$, thus $\alpha' \notin A_{i-1}(Z)$ by induction hypothesis, and $\alpha \notin A_i(Z)$.

If $\alpha(P_i) = 1$ (respectively 2), and $\beta(P_i) = \alpha(P_i)$, then $\beta' \notin A_{i-1}(Z')$ (respectively $A_{i-1}(Z''))$. Thus, the row of signs of $\mathcal{P}_{i-1}^{\beta'}$ on $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_1$ (respectively $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_2$) is a linear combination of rows of signs of $\mathcal{P}_{i-1}^{\lambda}$ on $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_1$ (respectively $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_2$), with $\lambda <_{\text{lex}} \beta'$ in the lexicographical order. Denoting by γ the element in $\{0,1,2\}^{\mathcal{P}_{i-1}}$ such that $\mathcal{P}_{i-1}^{\beta'}\mathcal{P}_{i-1}^{\gamma} = \mathcal{P}_{i-1}^{\alpha'}$, the row of signs of $\mathcal{P}_{i-1}^{\alpha'}$ on $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_1$ (respectively $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_2$) is a linear combination of rows of signs of $\mathcal{P}_{i-1}^{\lambda}\mathcal{P}_{i-1}^{\gamma}$ on $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_1$ (respectively $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_2$). Defining λ' by $\lambda'(P_j) = \lambda(P_j) + \gamma(P_j)$ modulo 2, the row of signs of $\mathcal{P}_{i-1}^{\lambda}\mathcal{P}_{i-1}^{\gamma}$ on $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_1$ (respectively $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_2$) coincides with the row of signs of $\mathcal{P}_{i-1}^{\lambda'}$ on $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_1$ (respectively $\mathrm{Sign}(\mathcal{P}_{i-1}, Z)_2$). Since it is clear that $\lambda' <_{\text{lex}} \alpha'$ in the lexicographical order, $\alpha' \notin A_{i-1}(Z')$ (respectively $A_{i-1}(Z''))$. Thus $\alpha \notin A_i(Z)$.

□

Complexity analysis: There are s steps in Algorithm 3.2.11 (Sign Determination). In each step, the number of calls to the Sturm-query black box is bounded by $2r$. Indeed, in Step i, there are at most $3r_{i-1}$ Sturm-queries to compute and r_{i-1} of these Sturm-queries have been determined in Step $i-1$. So, in Step i, there are at most $2r_{i-1}$ Sturm-queries to determine. The total number of calls to the to the Sturm-query black box is bounded by $1+2sr$. The calls to the Sturm-query black box are done for polynomials which are product of at most $\log_2(r)$ products of polynomials of the form P or P^2, $P \in \mathcal{P}$ by Proposition 3.2.14. □

Note that we did not count the complexity of performing the linear algebra involved in the algorithm. This is because when we consider particular ways of realization the Sturm-query black box later, we bound only the number of arithmetic operations in the ring. Since the complexity of linear algebra is polynomial in the size of the matrix, the maximum size of the matrices is $3r$, and their entries are $0, 1$ or -1, taking into account the linear algebra part of the algorithm would not change the linearity in s and the polynomial time in r character of the algorithm.

We can now describe in a more specific way how the Sturm-query black box can be implemented in the univariate case.

Algorithm 3.2.16 (Univariate Sign Determination) Structure: *an ordered integral domain* D*, contained in a real closed field* R.

Input: *a non-zero univariate polynomial* Q *and a list* $\mathcal{P}$ *of univariate polynomials with coefficients in* D*. The degree of* Q *is bounded by* p*, its number of real roots is bounded by* r*. The degree of* $P \in \mathcal{P}$ *is bounded by* q *and the number of polynomials in* $\mathcal{P}$ *is bounded by* s*. Let* $Z = \mathrm{Z}(Q, \mathrm{R})$.

Output: *the list of sign conditions realized by* $\mathcal{P}$ *on* Z, $\mathrm{Sign}(\mathcal{P}, Z)$*, and a list* A *of elements in* $\{0,1,2\}^{\mathcal{P}}$ *adapted to sign determination for* $\mathcal{P}$ *on* Z.

Procedure: *Perform Algorithm 3.2.11 (Sign Determination), using as Sturm-query black box Algorithm 1.4.48 (Univariate Sturm-query).*

Complexity analysis: According to the complexity of Algorithm 3.2.11 (Sign Determination), the number of calls to the Sturm-query black box is bounded by $1 + 2sp$, since $r \leq p$. The calls to the Sturm-query black box are done for P and polynomials of degree at most $q\log_2(p)$. The complexity is thus $O(sp^2(p + q\log_2(p)))$, using the complexity of Algorithm 1.4.48 (Univariate Sturm-query). □

The basic idea of the sign determination algorithm appears in [2]. The algorithm presented here appears in [7].

Bibliography

[1] S. Basu, R. Pollack, M.-F. Roy, *Algorithms in real algebraic geometry,* Springer, (2003).

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

[3] F. R. Gantmacher, *Theory of matrices, Vol I.* AMS-Chelsea (2000).

[4] A. Hurwitz, *Uber die Bedingunger, under welchen eine Gleichnun nur Worzeln it negative Tellec bezitzt,* Math. Annalen, vol. 46, 273-284 (1895).

[5] A. Liénard, M. H. Chipart *Sur le signe de la partie réelle des racines d'une équation algébrique*, J. Math. Pures Appl. (6) 10 291-346 (1914).

[6] M.-F. Routh, *Stability of a given state of motion,* London (1877), The advanced part of a treatise of the system of rigid bodies Dover, New York (1955).

[7] M.-F. Roy, A. Szpirglas, *Complexity of the computations with real algebraic numbers,* Journal of Symbolic computation 10 39-51 (1990).