INSTITUTE OF MATHEMATICS
of the
Polish Academy of Sciences

ul. Śniadeckich 8, P.O.B. 21, 00-956 Warszawa 10, Poland http://www.impan.pl

IM PAN Preprint 725 (2010)

Jan Kisyński

On the Tarski-Seidenberg Theorem

Published as manuscript

Received 07 June 2010

On the Tarski–Seidenberg theorem

Jan Kisyński
Institute of Mathematics, Polish Academy of Sciences
Śniadeckich 8, 00-956 Warszawa, Poland
E-mail: jan.kisynski@gmail.com

Abstract

Let $\mathcal{K}$ be a real closed field, $\mathcal{R}$ a subring of $\mathcal{K}$, and $\mathcal{A}_n(\mathcal{K};\mathcal{R})$ the algebra of subsets of $\mathcal{K}^n$ generated by sets of the form $\{(y_1,\dots,y_n) \in \mathcal{K}^n : \operatorname{sgn} P(y_1,\dots,y_n) = s\}$ where s ranges over $\{-1,0,1\}$ and P ranges over the polynomials of n variables with coefficients in $\mathcal{R}$. The Tarski–Seidenberg projection theorem ([H3], Theorem A.2.2; [Tr], Theorem A.1) is extended to the algebras $\mathcal{A}_n(\mathcal{K};\mathcal{R})$.

1 Introduction and the main result

Throughout the present paper, $\mathcal{K}$ will denote a *real closed* field, i.e. an ordered field satisfying the equivalent conditions (2.1)–(2.4) of the next section. Let sgn be the map of $\mathcal{K}$ into itself such that, for every $x \in \mathcal{K}$,

$$\operatorname{sgn} x = \begin{cases} -1 & \text{if } x < 0, \\ 0 & \text{if } x = 0, \\ 1 & \text{if } x > 0. \end{cases}$$

For any subring $\mathcal{R}$ of $\mathcal{K}$ and $n = 1,2,\dots$ denote by $\mathcal{R}[Y_1,\dots,Y_n]$ the ring of polynomials of n variables over $\mathcal{R}$, and by $\mathcal{A}_n(\mathcal{K};\mathcal{R})$ the algebra [1] of subsets of $\mathcal{K}^n$ generated by the sets

$$\{(y_1,\dots,y_n) \in \mathcal{K}^n : \operatorname{sgn} P(y_1,\dots,y_n) = s\}$$

2000 *Mathematics Subject Classification*: Primary 12D99, 12E05; Secondary 12L05, 35E99.

Key words and phrases: real-closed field, polynomials over a ring, the signature of a finite sequence of polynomials.

[1] A family F of subsets of a space X is called an *algebra* if $X \setminus A \in F$ whenever $A \in F$, and $A \cap B \in F$ whenever $A, B \in F$.

where $P \in \mathcal{R}[Y_1, \ldots, Y_n]$ and $s \in \{-1, 0, 1\}$. It is not difficult to prove that every set belonging to $\mathcal{A}_n(\mathcal{K}; \mathcal{R})$ may be represented in the form

$$A = \bigcup_{\iota} \bigcap_{\mu} \{(y_1, \ldots, y_n) \in \mathcal{K}^n : \operatorname{sgn} P_{\iota,\mu}(y_1, \ldots, y_n) = s_{\iota,\mu}\} \tag{1.1}$$

where $\bigcup_\iota$ and $\bigcap_\mu$ are finite, $P_{\iota,\mu} \in \mathcal{R}[Y_1, \ldots, Y_n]$, and $s_{\iota,\mu} \in \{-1, 0, 1\}$.

Our aim is to present a detailed proof of the following projection theorem.

Theorem 1.1. *Let $\mathcal{K}$ be a real closed field, $\mathcal{R}$ a subring of $\mathcal{K}$, and $l, n = 1, 2, \ldots$. Let $\mathbf{P}_{\mathcal{K}} : (x_1, \ldots, x_l, y_1, \ldots, y_n) \mapsto (y_1, \ldots, y_n)$ be the projection of $\mathcal{K}^{l+n}$ onto $\mathcal{K}^n$. Then $\mathbf{P}_{\mathcal{K}} A \in \mathcal{A}_n(\mathcal{K}; \mathcal{R})$ for every $A \in \mathcal{A}_{l+n}(\mathcal{K}; \mathcal{R})$.*

If $(\mathcal{K}, \mathcal{R}) = (\mathbb{R}, \mathbb{R})$, then Theorem 1.1 coincides with the *Tarski–Seidenberg theorem* from the Appendix to L. Hörmander's book [H3]. In applications of the projection theorem to PDE, noticed by L. Hörmander ([H1], proof of Lemma 3.9; [H2], proof of Theorem 5.4.1; [H3], proofs of Theorems 12.3.1 and 12.9.2) and discussed also in [G] and [F], one also has $(\mathcal{K}, \mathcal{R}) = (\mathbb{R}, \mathbb{R})$. However, the ideas of various proofs of the projection theorem come from the papers [T1, 2], [S] and [C1, 2] related to mathematical logic where the case of $\mathcal{R} = \mathbb{Z}$ is of particular interest. See also Chapter 23 of [A-Z]. Our proof of Theorem 1.1 refers to the Appendix to [H3], and thus, indirectly, also to [C1, 2].

Theorem 1.1 is equivalent to the statement that *whenever $P_1, \ldots, P_m \in \mathcal{R}[X_1, \ldots, X_l, Y_1, \ldots, Y_n]$, $s_1, \ldots, s_m$ are constants belonging to $\{-1, 0, 1\}$, and*

$$B = \{(y_1, \ldots, y_n) \in \mathcal{K}^n : \exists_{(x_1, \ldots, x_l) \in \mathcal{K}^l} \ [\operatorname{sgn} P_\mu(x_1, \ldots, x_l, y_1, \ldots, y_n) = s_\mu \text{ for every } \mu = 1, \ldots, m]\},$$

then

$$B \in \mathcal{A}_n(\mathcal{K}; \mathcal{R}).$$

This means that *the system of m equations*

$$\operatorname{sgn} P_\mu(x_1, \ldots, x_l, y_1, \ldots, y_n) = s_\mu, \qquad \mu = 1, \ldots, m,$$

with given $(y_1, \ldots, y_n) \in \mathcal{K}^n$ and unknown $(x_1, \ldots, x_l) \in \mathcal{K}^l$ has a solution if and only if $(y_1, \ldots, y_n) \in B$ for a suitable $B \in \mathcal{A}_n(\mathcal{K}; \mathcal{R})$.

Theorem 1.1 is also equivalent to the following *Polynomial Mapping Theorem* which for $\mathcal{K} = \mathcal{R} = \mathbb{R}$ is stated in the Appendix A to [Tr].

Theorem 1.2. *Let Q be a polynomial mapping of $\mathcal{K}^l$ into $\mathcal{K}^n$ such that $Q(x_1,\ldots,x_l) = (Q(x_1,\ldots,x_l),\ldots,Q_n(x_1,\ldots,x_l))$ where $Q_1,\ldots,Q_n \in \mathcal{R}[X_1,\ldots,X_l]$. Then $Q(A) \in \mathcal{A}_n(\mathcal{K}_l;\mathcal{R})$ for every $A \in \mathcal{A}_l(\mathcal{K};\mathcal{R})$.*

Indeed, if

$$A = \bigcup_{\iota} \bigcap_{\mu=1}^{m_\iota} \{(x_1,\ldots,x_l) \in \mathcal{K}^l : \operatorname{sgn} P_{\iota,\mu}(x_1,\ldots,x_l) = s_{\iota,\mu}\} \in \mathcal{A}_\iota(\mathcal{K};\mathcal{R}),$$

then

$$\begin{aligned} Q(A) &= \bigcup_{\iota} Q\Big(\bigcap_{\mu=1}^{m_\iota} \{(x_1,\ldots,x_l) \in \mathcal{K}^l : \operatorname{sgn} P_{\iota,\mu}(x_1,\ldots,x_l) = s_{\iota,\mu}\}\Big) \\ &= \bigcup_{\iota} \{(y_1,\ldots,y_n) \in \mathcal{K}^n : \exists_{(x_1,\ldots,x_l)\in\mathcal{K}^l} \ [\operatorname{sgn}(Q_\nu(x_1,\ldots,x_l) - y_\nu) = 0 \\ &\qquad\qquad \text{for every } \nu = 1,\ldots,n, \\ &\qquad \operatorname{sgn} P_{\iota,\mu}(x_1,\ldots,x_l) = s_{\iota,\mu} \text{ for every } \mu = 1,\ldots,m_\iota]\} \in \mathcal{A}_n(\mathcal{K};\mathcal{R}), \end{aligned}$$

by Theorem 1.1. Hence Theorem 1.1 implies Theorem 1.2. The converse implication is obvious.

Theorem 1.3. *Let $\mathcal{R}$ be a commutative ring. For every finite system of polynomials $P_{i,\mu} \in \mathcal{R}[X_1,\ldots,X_l,Y_1,\ldots,Y_n]$ and numbers $s_{i,\mu} \in \{-1,0,1\}$, $i \in I$, $\mu \in M_i$, there is a finite system of polynomials $\tilde{P}_{j,\nu} \in \mathcal{R}[Y_1,\ldots,Y_n]$ and numbers $\tilde{s}_{j,\nu} \in \{-1,0,1\}$, $j \in J$, $\nu \in N_j$, such that whenever $\mathcal{K}$ is a real closed field containing $\mathcal{R}$ as a subring and*

$$A_{\mathcal{K}} = \bigcup_{i\in I} \bigcap_{\mu\in M_i} \{(x_1,\ldots,x_l,y_1,\ldots,y_n) \in \mathcal{K}^{l+n} : \operatorname{sgn} P_{i,\mu}(x_1,\ldots,x_l,y_1,\ldots,y_n) = s_{i,\mu}\},$$

then

$$\mathbf{P}_{\mathcal{K}} A_{\mathcal{K}} = \bigcup_{j\in J} \bigcap_{\nu\in N_j} \{(y_1,\ldots,y_n) \in \mathcal{K}^n : \operatorname{sgn} \tilde{P}_{j,\nu}(y_1,\ldots,y_n) = \tilde{s}_{j,\nu}\}.$$

Theorem 1.3 implies Theorem 1.1. In the case when $\mathcal{R}$ is the field of rational numbers Theorem 1.3 was proved by A. Seidenberg in [S]. The proof of Theorem 1.3 for general $\mathcal{R}$ may be obtained by the same algorithm which is used in the proof of Theorem 1.1 and is presented in Sections 6 and 7.

2 Real closed fields

An *ordered field* is defined as a field which is linearly ordered in a manner compatible with the field structure. Let $\mathcal{K}$, $\mathcal{H}$ be ordered fields. Then $\mathcal{H}$ is called an *ordered extension* of $\mathcal{K}$ if $\mathcal{K}$ is a subfield of $\mathcal{H}$ and the order induced on $\mathcal{K}$ by $\mathcal{H}$ coincides with the original order on $\mathcal{K}$. An ordered field $\mathcal{K}$ is called *maximal* if there is no ordered field $\mathcal{H}$ strictly larger than $\mathcal{K}$ such that simultaneously $\mathcal{H}$ is an ordered extension of $\mathcal{K}$ and $\mathcal{H}$ is an algebraic extension of $\mathcal{K}$.

For every ordered field the following four conditions are equivalent:

(2.1) $\mathcal{K}$ is a maximal ordered field,

(2.2) the complexification of $\mathcal{K}$ is an algebraically closed field,

(2.3) every positive element of $\mathcal{K}$ is equal to the square of some element of $\mathcal{K}$ and every polynomial over $\mathcal{K}$ of odd degree has a root in $\mathcal{K}$,

(2.4) every polynomial over $\mathcal{K}$, treated as function on $\mathcal{K}$, has the property of passing through intermediate values, i.e. whenever $P \in \mathcal{K}[X]$, $a \in \mathcal{K}$, $b \in \mathcal{K}$ and $a < b$, then

$$\{y \in \mathcal{K} : P(a) \wedge P(b) < y < P(a) \vee P(b)\} \subset \{P(x) : x \in \mathcal{K},\ a < x < b\}.$$

Evidently (2.4) implies (2.3), and conversely (2.3) implies (2.4) by Proposition 5 of Sec. VI.2.5 of [B]. The equivalence of (2.1)–(2.3) follows from Theorem 3 of Sec. VI.2.6 of [B], called there the Euler–Lagrange theorem. One can also refer to Chapter XI of [W] or to Chapter XI of [L] [2].

A field is called *real closed* if it is ordered and satisfies the equivalent conditions (2.1)–(2.4). For every ordered field there is an algebraic extension which is real closed; this algebraic extension is unique up to equivalence of extensions, and is called the *real closure* of the given ordered field. See [W], Sec. XI.82, Theorem 8. Examples of real closed fields are: the field of real numbers and the field of real algebraic numbers.

In the subsequent sections we will refer only to (2.4) and the two propositions formulated below. For any polynomial P of one variable denote by P' the derivative of P defined algebraically.

Proposition 2.1. *Suppose that $\mathcal{K}$ is an ordered field, $0 \not\equiv P \in \mathcal{K}[X]$, $a \in \mathcal{K}$ and $P(a) = 0$. Then there is $h_0 \in \mathcal{K}$ such that $h_0 > 0$ and whenever $h \in \mathcal{K}$ and $0 < |h| < h_0$, then $P(a+h) \neq 0$ and*

$$\operatorname{sgn}(P'(a+h)) = \operatorname{sgn}(h)\operatorname{sgn}(P(a+h)). \tag{2.5}$$

[2] In these references the equivalence of (2.1)–(2.4) is proved with the use of set-theoretical tools permitted in the usual theory of fields, and not with the limited tools of the axiomatic theory of real fields used in [T1, 2] and [C1, 2].

Proof. Since $P \not\equiv 0$ and $P(a) = 0$, one has

$$P(a+h) = a_k h^k + a_{k+1} h^{k+1} + \cdots + a_n h^n = h^k (a_k + a_{k+1} h + \cdots + a_n h^{n-k}) \tag{2.6}$$

for every $h \in \mathcal{K}$, where $1 \leq k \leq n$, $a_k, a_{k+1}, \ldots, a_n \in \mathcal{K}$ and $a_k \neq 0$. Consequently,

$$\begin{aligned} P'(a+h) &= k a_k h^{k-1} + (k+1) a_{k+1} h^k + \cdots + n a_n h^{n-1} \\ &= h^{k-1} (k a_k + (k+1) a_{k+1} h + \cdots + n a_n h^{n-k}) \end{aligned} \tag{2.7}$$

for every $h \in \mathcal{K}$. Let

$$h_0 = 1 \wedge \frac{|a_k|}{2(|a_{k+1}| + \cdots + |a_n|) + 1} \wedge \frac{k|a_k|}{2((k+1)|a_{k+1}| + \cdots + n|a_n|) + 1}.$$

Whenever $h \in \mathcal{K}$ and $0 < |h| < h_0$, then

$$\begin{aligned} \operatorname{sgn}(k a_k + (k+1) a_{k+1} h + \cdots + n a_n h^{n-k}) &= \operatorname{sgn}(k a_k) = \operatorname{sgn}(a_k) \\ &= \operatorname{sgn}(a_k + a_{k+1} h + \cdots + a_n h^{n-k}), \end{aligned}$$

whence (2.5) follows, by (2.6) and (2.7).

Proposition 2.2 ([B], Sec. VI.2.6, Exercise 13)**.** *Suppose that $\mathcal{K}$ is a real closed field, $a \in \mathcal{K}$, $b \in \mathcal{K}$, $a < b$, and $P \in \mathcal{K}[X]$. Then there is $\xi \in \mathcal{K}$ such that $a < \xi < b$ and*

$$P(b) - P(a) = (b-a) P'(\xi).$$

Proposition 2.2 states that the Lagrange theorem about increments, well-known from elementary calculus, remains valid for polynomials over any real closed field.

Proof. Let

$$Q(X) = \frac{P(b) - P(a)}{b - a}(X - a) + P(a) - P(X).$$

Then $Q(a) = Q(b) = 0$. The proof of Proposition 2.2 reduces to showing that there is $\xi \in \mathcal{K}$ such that $a < \xi < b$ and $Q'(\xi) = 0$. If $Q \equiv 0$ then there is nothing to prove. If $Q \not\equiv 0$, then let $b' \in \mathcal{K}$ be the smallest element of the set $\{x \in \mathcal{K} : x > a,\, Q(x) = 0\}$, which is non-empty (because it contains b) and finite (because it consists of some zeros of a polynomial which does not vanish identically). Then $b' \in \mathcal{K}$, $a < b'$, $Q(b') = 0 = Q(a)$ and $Q(x) \neq 0$ whenever $x \in \mathcal{K}$ and $a < x < b'$. By Proposition 2.1, there is $h_0 \in \mathcal{K}$ such that $0 < h_0 < \frac{1}{2}(b' - a)$ and, whenever $h \in \mathcal{K}$ and $0 < h < h_0$, then

$$\operatorname{sgn}(Q'(a+h)) = \operatorname{sgn}(Q(a+h)) \neq 0$$

and

$$\operatorname{sgn}(Q'(b'-h)) = -\operatorname{sgn}(Q(b'-h)) \neq 0.$$

Fix $h \in \mathcal{K}$ such that $0 < h < h_0$. Then $a < a+h < b'-h < b'$. Since $Q(x) \neq 0$ whenever $x \in \mathcal{K}$ and $a < x < b'$, from (2.4) it follows that $\operatorname{sgn}(Q(b'-h)) = \operatorname{sgn}(Q(a+h))$. Therefore $\operatorname{sgn}(Q'(b'-h)) = -\operatorname{sgn}(Q'(a+h)) \neq 0$, and so, by (2.4), there is $\xi \in \mathcal{K}$ such that $a+h < \xi < b'-h$ and $Q'(\xi) = 0$.

3 Division with remainder for polynomials over a ring

Proposition 3.1. *Let $P, S \in K[X]$ be polynomials over a commutative ring K. Suppose that $\deg P = p \geq \deg S = d > 0$, so that*

$$S(X) = \sum_{\nu=0}^{d} b_\nu X^{d-\nu}$$

where $b_\nu \in \mathcal{K}$ for $\nu = 1, \ldots, d$ and $b_0 \neq 0$. Then there is $k_0 \in \{1, \ldots, p-d+1\}$ such that for every $l \in \{k_0, k_0+1, \ldots\}$ there is a unique pair of polynomials $Q, R \in K[X]$ satisfying the conditions

$$\deg R < d \quad \textit{and} \quad b_0^l P(X) = Q(X)S(X) + R(X). \tag{3.1}$$

Proof. For $k = 0, 1, \ldots$ define successively the polynomials

$$R_k(X) = a_{k,0}X^{d_k} + a_{k,1}X^{d_k-1} + \cdots + a_{k,d_k-1}X + a_{k,d_k}$$

such that $R_0(X) = P(X)$, and whenever $\deg R_{k-1} \geq d$, then

$$R_k(X) = b_0 R_{k-1}(X) - a_{k-1,0}X^{d_{k-1}-d}S(X).$$

The procedure terminates once R_{k_0} is defined where k_0 is the first k for which $\deg R_k < d$. Since $p = d_0 > d_1 > \cdots > d_{k_0-1} \geq d$, one has $k_0 - 1 \leq p - d$. For every $k = 1, \ldots, k_0$ one has

$$\begin{aligned} b_0^k P(X) &= b_0^k R_0(X) = b_0^{k-1} a_{0,0} X^{d_0-d} S(X) + b_0^{k-1} R_1(X) \\ &= (b_0^{k-1} a_{0,0} X^{d_0-d} + b_0^{k-2} a_{1,0} X^{d_1-d}) S(X) + b_0^{k-2} R_2(X) \\ &= \cdots = Q_k(X)S(X) + R_k(X) \end{aligned}$$

where

$$\begin{aligned} &Q_k(X) \\ &\quad = b_0^{k-1} a_{0,0} X^{d_0-d} + b_0^{k-2} a_{1,0} X^{d_1-d} + \cdots + b_0 a_{k-2,0} X^{d_{k-2}-d} + a_{k-1,0} X^{d_{k-1}-d}. \end{aligned}$$

As $\deg R_{k_0} < d$ and $k_0 \le p-d+1$, it follows that for every $l \in \{k_0, k_0+1, \dots\}$ the conditions (3.1) are satisfied by $Q = b_0^{l-k_0} Q_{k_0}$ and $R = b_0^{l-k_0} R_{k_0}$.

In order to prove the uniqueness of Q and R, suppose that $Q_i, R_i \in K[X]$, $\deg R_i < d$, and $b_0^l P = Q_i S + R_i$ for $i = 1, 2$ and some natural l. Then $(Q_2 - Q_1)S = R_1 - R_2$, whence $\deg[(Q_2 - Q_1)S] = \deg(R_1 - R_2) < d = \deg S$. It follows that $Q_1 = Q_2$, and consequently also $R_1 = R_2$.

4 Signatures as rectangular matrices

By an *m-dimensional signature* we mean a rectangular matrix

$$\hat{s} = \begin{bmatrix} s_{1,0} & s_{1,1} & \cdots & s_{1,2N} \\ s_{2,0} & s_{2,1} & \cdots & s_{2,2N} \\ \vdots & \vdots & & \vdots \\ s_{m,0} & s_{m,1} & \cdots & s_{m,2N} \end{bmatrix}$$

with m rows and an odd number $2N+1$, $N = 0, 1, \dots,$ of columns such that

(i) the entries $s_{\mu,\nu}$, $\mu = 1, \dots, m$, $\nu = 0, \dots, 2N$, may take only three values $-1, 0, 1$,

(ii) $s_{\mu,\nu-1} \cdot s_{\mu\nu} \neq -1$ for every $\mu = 1, \dots, m$ and $\nu = 1, \dots, 2N$ (i.e. a succession $-1, 1$ or $1, -1$ never occurs in any row of $\hat{s}$),

(iii) no two adjacent columns of $\hat{s}$ are identical,

(iv) for every $\mu = 1, \dots, m$ either $s_{\mu,0} = s_{\mu,1} = \cdots = s_{\mu,2N} = 0$ or $s_{\mu,0} \cdot s_{\mu,2} \cdot \ldots \cdot s_{\mu,2N} \neq 0$.

The set of m-dimensional signatures is denoted by S_m. The number of columns of an m-dimensional signature is called the *length* of the signature. The length of an m-dimensional signature is always an odd number $2N+1, N = 0, 1, \dots$. A column of a signature $\hat{s} \in S_m$ will be called *even* or *odd* according as the index of this column belongs to $\{0, 2, \dots, 2N\}$ or $\{1, 3, \dots, 2N-1\}$.

4.1 Cancellation of rows

If $\hat{s} \in S_m$, $m \ge 2$, then the matrix $\hat{s}'$ obtained from $\hat{s}$ by cancelling a row need not be a signature because it may not satisfy condition (iii). If (iii) is not satisfied for $\hat{s}'$, then any succession of two or more adjacent identical columns (s.a.i.c.) of $\hat{s}'$ contains an odd column. By (ii) and (iv), this odd column of $\hat{s}'$ is identical with both the adjacent even columns of $\hat{s}'$. Consequently, any s.a.i.c. of $\hat{s}'$ contains an odd number of columns, and it begins and ends with even columns. It follows that if every s.a.i.c. of $\hat{s}'$ is reduced to one column, then one obtains a signature $\hat{s}'' \in S_{m-1}$ of length no greater than the length of $\hat{s}$. Furthermore, the evenness and the oddness of columns is not changed by the above described compression of $\hat{s}'$.

The cancellation of several rows of a signature, and the related replacement of the resulting s.a.i.c.'s by single columns, is a procedure similar to the one described above.

4.2 Adjoining a special row

Let $\hat{s} = (s_{\mu,\nu})_{\mu=1,\dots,m;\nu=0,\dots,2N} \in S_m$ be a signature of length $2N+1$, and let $(s_1,\dots,s_N) \in \{-1,0,1\}^N$ be a sequence without any pair of adjacent zeros. Then there is a unique signature $\hat{s}' = \mathbf{K}(\hat{s}; s_1,\dots,s_N) \in S_{m+1}$ of length no smaller than $2N+1$ having the form

$$(4.1) \qquad \hat{s}' = \left[\begin{array}{ccc|c|ccccc|} s_{1,0} & & s_{1,1} & & s_{1,2\nu-1} & & s_{1,2\nu} & & s_{1,2\nu+1} \\ \vdots & L_0 & \vdots & \cdots & \vdots & L_\nu^- & \vdots & L_\nu^+ & \vdots \\ s_{m,0} & & s_{m,1} & & s_{m,2\nu-1} & & s_{m,2\nu} & & s_{m,2\nu+1} \\ -s_{m,0} & & s_1 & & s_\nu & & u_\nu & & s_{\nu+1} \end{array}\right.$$
$$\qquad\qquad \left.\begin{array}{c|ccc} & s_{1,2N-1} & & s_{1,2N} \\ \cdots & \vdots & L_N & \vdots \\ & s_{m,2N-1} & & s_{m,2N} \\ & s_N & & s_{m,2N} \end{array}\right]$$

where u_ν, $\nu = 1,\dots,N-1$, are to be determined, and L_0, L_ν^-, L_ν^+ and L_N indicate places where some new columns can be put, if needed, in accordance with the following three rules:

(i) If $s_1 \cdot s_{m,0} \neq 1$, then L_0 is not used. If $s_1 \cdot s_{m,0} = 1$, then in L_0 the following block of two columns is placed:

$$\begin{bmatrix} s_{1,0} & s_{1,0} \\ \vdots & \vdots \\ s_{m,0} & s_{m,0} \\ 0 & s_1 \end{bmatrix}.$$

(ii) If $s_\nu \cdot s_{\nu+1} \neq -1$, then $0 \neq u_\nu \in \{s_\nu, s_{\nu+1}\}$ and L_ν^- and L_ν^+ are not used. If $s_\nu \cdot s_{\nu+1} = -1$, then $u_\nu = 0$, in L_ν^- the column $(s_{1,2\nu},\dots,s_{m,2\nu},s_\nu)^\dagger$ is placed, and in L_ν^+ the column $(s_{1,2\nu},\dots,s_{m,2\nu},s_{\nu+1})^\dagger$ is placed.

(iii) If $s_N \cdot s_{m,2N} \neq -1$, then L_N is not used. If $s_N \cdot s_{m,2N} = -1$, then in L_N the following block of two columns is placed:

$$\begin{bmatrix} s_{1,2N} & s_{1,2N} \\ \vdots & \vdots \\ s_{m,2N} & s_{m,2N} \\ s_N & 0 \end{bmatrix}.$$

It is easy to check that, using the scheme (4.1) and the rules described above, one obtains a signature $\hat{s}' \in S_{m+1}$. Obviously, $\hat{s}'$ is uniquely determined by the given signature $\hat{s}' \in S_m$ of length $2N+1$ and the given sequence $(s_1, \dots, s_n) \in \{-1, 0, 1\}^N$ not containing any pair of consecutive zeros.

4.3 The mapping $\mathcal{H}$ from S_{2m} into S_m

Consider a signature $\hat{s} \in S_{2m}$ of the form

$$\hat{s} = \begin{bmatrix} s_{1,0} & s_{1,1} & \dots & s_{1,2N} \\ \vdots & \vdots & & \vdots \\ s_{m,0} & s_{m,1} & \dots & s_{m,2N} \\ r_{1,0} & r_{1,1} & \dots & r_{1,2N} \\ \vdots & \vdots & & \vdots \\ r_{m,0} & r_{m,1} & \dots & r_{m,2N} \end{bmatrix} \tag{4.2}$$

where the length of $\hat{s}$ is an arbitrary odd number $2N+1$. Let $D(\mathcal{H})$ be the set of the signatures (4.2) belonging to S_{2m} and satisfying the following four conditions:

(4.3) none of the upper m rows of $\hat{s}$ consists only of zeros, so that by (iv) in each of the m upper rows every even element is non-zero,

(4.4) $\#\{\nu = 1, \dots, N : s_{\mu,2\nu-1} = 0 \text{ for some } \mu = 1, \dots, m\} = N' \geq 1$,

(4.5) whenever $\mu_1, \mu_2 \in \{1, \dots, m\}$, $\nu \in \{1, \dots, N\}$ and $s_{\mu_1,2\nu-1} = s_{\mu_2,2\nu-1} = 0$, then $r_{\mu_1,2\nu-1} = r_{\mu_2,2\nu-1}$,

(4.6) if $\nu_1 < \dots < \nu_{N'}$, and $\{s_k\} = \{r_{\mu,2\nu_k-1} : \nu_k \in \{1, \dots, m\},\ s_{\mu,2\nu_k-1} = 0\}$ for $k = 1, \dots, N'$, then the sequence $s_1, \dots, s_{N'}$ does not contain any pair of consecutive zeros.

Conditions (4.3)–(4.6) imply that the upper m rows of $\hat{s}$ constitute a matrix that consists of $N'+1$ s.a.i.c. separated by the columns $(s_{1,2\nu_k-1}, s_{2,2\nu_k-1}, \dots, s_{m,2\nu_k-1})^\dagger$, $k = 1, \dots, N'$. For every $\hat{s} \in D(\mathcal{H})$ we construct the signature $\mathcal{H}(\hat{s}) \in S_m$ as follows.

Step 1. We define the sequence $s_1, \dots, s_{N'}$, $1 \leq N' \leq N$, as in (4.6).

STEP 2. We cancel all the m lower rows of $\hat{s}$ and in the resulting $m \times (2N+1)$-matrix we replace every s.a.i.c. by one column, as described in Section 4.1. We then obtain an $m \times (2N'+1)$-matrix $\hat{s}'$ which is a signature belonging to S_m and having length $2N'+1$. The number N' is the same as in Step 1.

STEP 3. Using the rules described in Section 4.2 we construct the signature $\hat{s}'' = \mathbf{K}(\hat{s}'; s_1, \dots, s_{N'}) \in S_{m+1}$ of length $2N''+1$ no smaller than $2N'+1$.

STEP 4. In the matrix $\hat{s}'' = \mathbf{K}(\hat{s}'; s_1, \dots, s_{N'}) \in S_{m+1}$ we cancel the m-th row, and in the resulting $m \times (2N''+1)$-matrix we replace every s.a.i.c. by one column, as described in Section 4.1. The result is a signature belonging to S_m which we denote by $\mathcal{H}(\hat{s})$.

5 The signature of a finite sequence of polynomials

Let $\mathcal{K}$ be a real closed field, and $P_1, \dots, P_m \in \mathcal{K}[X]$ polynomials of one variable over $\mathcal{K}$ not all of order zero. For every $\mu = 1, \dots, m$ define

$$\mathcal{N}(P_\mu) = \begin{cases} \{x \in \mathcal{K} : P_\mu(x) = 0\} & \text{if } P_\mu \text{ is not identically zero,} \\ \emptyset & \text{if } P_\mu \text{ is identically zero.} \end{cases}$$

Then $\#(\bigcup_{\mu=1}^{m} \mathcal{N}(P_\mu)) = N \geq 1$. Let

$$\bigcup_{\mu=1}^{m} \mathcal{N}(P_\mu) = \{x_1, \dots, x_N\} \quad \text{where } x_1 < \cdots < x_N \text{ if } N > 1.$$

Let $I_0 = \{x \in \mathcal{K} : x < x_1\}$, $I_\nu = \{x \in \mathcal{K} : x_\nu < x < x_{\nu+1}\}$ for $\nu = 1, \dots, N-1$ if $N > 1$, and $I_N = \{x \in \mathcal{K} : x_n < x\}$. Then, for every $\mu = 1, \dots, m$ and $\nu = 0, \dots, N$, the set $\{\operatorname{sgn} P_\mu(x) : x \in I_\nu\}$ is a singleton. We denote this singleton by $\operatorname{sgn} P_\mu(I_\nu)$ and define the *signature* $\mathrm{SGN}(P_1, \dots, P_m)$ *of the sequence of polynomials* $P_1, \dots, P_m$ not all of order zero as the $m \times (2N+1)$-matrix

$$\begin{bmatrix} \operatorname{sgn} P_1(I_0) & \operatorname{sgn} P_1(x_1) & \operatorname{sgn} P_1(I_1) & \dots & \operatorname{sgn} P_1(x_N) & \operatorname{sgn} P_1(I_N) \\ \operatorname{sgn} P_2(I_0) & \operatorname{sgn} P_2(x_1) & \operatorname{sgn} P_2(I_1) & \dots & \operatorname{sgn} P_2(x_N) & \operatorname{sgn} P_2(I_N) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \operatorname{sgn} P_m(I_0) & \operatorname{sgn} P_m(x_1) & \operatorname{sgn} P_m(I_1) & \dots & \operatorname{sgn} P_m(x_N) & \operatorname{sgn} P_m(I_N) \end{bmatrix}.$$

It is easy to check that this matrix is an m-dimensional signature in the sense of Section 4. *The symbol* SGN *denotes the mapping from the set of* *finite sequences of polynomials over $\mathcal{K}$ into the set of signatures defined in Section 4* [3].

If a sequence of polynomials $P_1, \dots, P_m$ belonging to $\mathcal{K}[X]$ is replaced by its subsequence $P_{\mu_1}, \dots, P_{\mu_k}$, $1 \le \mu_1 < \cdots < \mu_k \le m$, or if we adjoin to the sequence $P_1, \dots, P_m$ a polynomial P_{m+1} such that P_m is the derivative of P_{m+1}, then the matrices $\mathrm{SGN}(P_{\mu_1}, \dots, P_{\mu_k})$ and $\mathrm{SGN}(P_1, \dots, P_m, P_{m+1})$ may be obtained directly from $\mathrm{SGN}(P_1, \dots, P_m)$ by manipulations described in Sections 4.1 and 4.2.

5.1

For instance, if in the sequence $P_1, \dots, P_m$ the last polynomial is cancelled, then the elements of $\bigcup_{\mu=1}^{m-1} \mathcal{N}(P_\mu)$ constitute a subsequence $x_{\nu_1}, \dots, x_{\nu_{N'}}$ ($N' \le N$, $x_{\nu_1} < \cdots < x_{\nu_{N'}}$) of the sequence $x_1, \dots, x_N$ of all elements of $\bigcup_{\mu=1}^{m} \mathcal{N}(P_\mu)$ ordered so that $x_1 < \cdots < x_N$. Then $\mathrm{SGN}(P_1, \dots, P_{m-1})$ is the $(m-1) \times (2N'+1)$-matrix

$$(5.1)\quad \begin{bmatrix} \operatorname{sgn} P_1(-\infty, x_{\nu_1}) & \operatorname{sgn} P_1(x_{\nu_1}) & \operatorname{sgn} P_1(x_{\nu_1}, x_{\nu_2}) & \dots & \operatorname{sgn} P_1(x_{\nu_{N'}}) & \operatorname{sgn} P_1(x_{\nu_{N'}}, \infty) \\ \operatorname{sgn} P_2(-\infty, x_{\nu_1}) & \operatorname{sgn} P_2(x_{\nu_1}) & \operatorname{sgn} P_2(x_{\nu_1}, x_{\nu_2}) & \dots & \operatorname{sgn} P_2(x_{\nu_{N'}}) & \operatorname{sgn} P_2(x_{\nu_{N'}}, \infty) \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ \operatorname{sgn} P_{m-1}(-\infty, x_{\nu_1}) & \operatorname{sgn} P_{m-1}(x_{\nu_1}) & \operatorname{sgn} P_{m-1}(x_{\nu_1}, x_{\nu_2}) & \dots & \operatorname{sgn} P_{m-1}(x_{\nu_{N'}}) & \operatorname{sgn} P_{m-1}(x_{\nu_{N'}}, \infty) \end{bmatrix}$$

and one has

$$(5.2)\quad \begin{aligned} (-\infty, x_{\nu_1}) &= I_0 \cup \{x_1\} \cup I_1 \cup \cdots \cup \{x_{\nu_1 - 1}\} \cup I_{\nu_1 - 1} \quad \text{if } 1 < \nu_1, \\ (x_{\nu_1}, x_{\nu_2}) &= I_{\nu_1} \cup \{x_{\nu_1+1}\} \cup I_{\nu_1+1} \cup \cdots \cup \{x_{\nu_2-1}\} \cup I_{\nu_2-1} \\ &\qquad \text{if } \nu_1 + 1 < \nu_2, \\ &\dots \\ (x_{\nu_{N'}}, \infty) &= I_{\nu_{N'}} \cup \{x_{\nu_{N'}+1}\} \cup I_{\nu_{N'}+1} \cup \cdots \cup \{x_N\} \cup I_N \\ &\qquad \text{if } \nu_{N'} < N. \end{aligned}$$

If some of these unions consists of more than one member, then all the singletons $\{x_k\}$ occurring in the union must be contained in $\mathcal{N}(P_m) \setminus \bigcup_{\mu=1}^{m-1} \mathcal{N}(P_\mu)$, so that $P_\mu(x_k) \ne 0$ for $\mu = 1, \dots, m-1$, and $\operatorname{sgn} P_\mu$ is the same on every

[3] If $P_1, \dots, P_m \in \mathcal{K}[X]$ then $\mathrm{SGN}(P_1, \dots, P_m)$ may be determined by means of the theorem of Sturm ([W], Sec. XI.79), without computing the roots $x_1, \dots, x_N$ exactly. However, this does not influence our subsequent arguments.

member of the union. Thus the decompositions (5.2) correspond to the s.a.i.c.'s of the matrix $\hat{s}'$ obtained from $\mathrm{SGN}(P_1,\dots,P_m)$ by cancelling the mth row, and hence (5.1) is equal to the matrix obtained from $\hat{s}'$ by reducing each s.a.i.c. to a single column.

5.2

Suppose now that $P_1,\dots,P_m,P_{m+1}\in\mathcal{K}[X]$ and $\frac{\partial}{\partial X}P_{m+1}=P_m\not\equiv 0$. Then, following Section 4.2, one can construct the matrix $\mathrm{SGN}(P_1,\dots,P_m,P_{m+1})$ using only $\operatorname{sgn} P_{m+1}|_{\bigcup_{\mu=1}^{m}\mathcal{N}(P_\mu)}$ and the matrix $\mathrm{SGN}(P_1,\dots,P_m)$. To see this, consider the sequence $y_1,\dots,y_{N'}$ such that $\{y_1,\dots,y_{N'}\}=\bigcup_{\mu=1}^{m+1}\mathcal{N}(P_\mu)$ and $y_1<\dots<y_{N'}$. This sequence contains a subsequence $x_1,\dots,x_N$, $N\le N'$, such that $\{x_1,\dots,x_N\}=\bigcup_{\mu=1}^{m}\mathcal{N}(P_\mu)$ and $x_1<\dots<x_N$. Any of the sets $(-\infty,x_1)\cup\{x_1\}$, $\{x_N\}\cup(x_n,\infty)$, $\{x_\nu\}\cup(x_\nu,x_{\nu+1})\cup\{x_{\nu+1}\}$, $\nu=1,\dots,N-1$, may contain at most one element of the sequence $y_1,\dots,y_{N'}$. Indeed, suppose for instance that $y_n,y_{n'}\in\mathcal{N}(P_{m+1})\cap(\{x_\nu\}\cup(x_\nu,x_{\nu+1})\cup\{x_{\nu+1}\})$. If y_n and $y_{n'}$ were distinct, then, by the Lagrange theorem, there would exist a root of $P_m=\frac{\partial}{\partial X}P_{m+1}$ between them, and hence in $(x_\nu,x_{\nu+1})$. But this is impossible, because all the roots of P_m belong to the sequence $x_1,\dots,x_N$. Let

$$s_\nu=\operatorname{sgn} P_{m+1}(x_\nu),\qquad \nu=1,\dots,N.$$

From what we have proved above it follows that the sequence $s_1,\dots,s_N$ does not contain any pair of adjacent zeros.

Following Section 4.2 we represent $\mathrm{SGN}(P_1,\dots,P_m,P_{m+1})$ by the scheme

$$\left[\begin{array}{ccc} \operatorname{sgn} P_1(-\infty,x_1) & & \operatorname{sgn} P_1(x_1) \\ \vdots & L_0 & \vdots \\ \operatorname{sgn} P_m(-\infty,x_1) & & \operatorname{sgn} P_m(x_1) \\ -\operatorname{sgn} P_m(-\infty,x_1) & & s_1 \end{array}\right|$$

$$\cdots\left|\begin{array}{ccccc} \operatorname{sgn} P_1(x_\nu) & & \operatorname{sgn} P_1(x_\nu,x_{\nu+1}) & & \operatorname{sgn} P_1(x_{\nu+1}) \\ \vdots & L_\nu^- & \vdots & L_\nu^+ & \vdots \\ \operatorname{sgn} P_m(x_\nu) & & \operatorname{sgn} P_m(x_\nu,x_{\nu+1}) & & \operatorname{sgn} P_m(x_{\nu+1}) \\ s_\nu & & u_\nu & & s_{\nu+1} \end{array}\right|$$

$$\cdots\left|\begin{array}{ccc} \operatorname{sgn} P_1(x_N) & & \operatorname{sgn} P_1(x_N,\infty) \\ \vdots & L_N & \vdots \\ \operatorname{sgn} P_m(x_N) & & \operatorname{sgn} P_m(x_N,\infty) \\ s_N & & \operatorname{sgn} P_m(x_N,\infty) \end{array}\right].$$

The rules presented in Section 4.2 give the unique possibility of filling up this scheme so that the result is an $(m+1)$-dimensional signature. We are going to show that this last signature is equal to $\mathrm{SGN}(P_1, \dots, P_m, P_{m+1})$. To this end, it is sufficient to express the results of the operations (i), (ii) and (iii) from Section 4.2 in terms of $\mathrm{SGN}(P_1, \dots, P_m, P_{m+1})$.

(i) If $s_1 \cdot \operatorname{sgn} P_m(-\infty, x_1) \neq 1$, then $\frac{\partial}{\partial X} P_{m+1} = P_m$ does not vanish in the interval $(-\infty, x_1)$ because $P_m \not\equiv 0$. Therefore if $s_1 \cdot \operatorname{sgn} P_m(-\infty, x_1) \neq 1$, then P_{m+1} does not vanish in $(-\infty, x_1)$, and $\operatorname{sgn} P_{m+1}(-\infty, x_1) = \operatorname{sgn} P_m(-\infty, x_1)$. The leftmost block in the scheme (4.1) consists in this case of two columns and has the form

$$\begin{bmatrix} \operatorname{sgn} P_1(-\infty, x_1) & \operatorname{sgn} P_1(x_1) \\ \vdots & \vdots \\ \operatorname{sgn} P_m(-\infty, x_1) & \operatorname{sgn} P_m(x) \\ \operatorname{sgn} P_{m+1}(-\infty, x_1) & s_1 \end{bmatrix} = \begin{bmatrix} \operatorname{sgn} P_1(-\infty, x_1) & \operatorname{sgn} P_1(x_1) \\ \vdots & \vdots \\ \operatorname{sgn} P_m(-\infty, x_1) & \operatorname{sgn} P_m(x_1) \\ \operatorname{sgn} P_{m+1}(-\infty, x_1) & \operatorname{sgn} P_{m+1}(x_1) \end{bmatrix}.$$

If $s_1 \cdot \operatorname{sgn} P_m(-\infty, x_1) = 1$, then $\operatorname{sgn} P_{m+1}(x_1) \cdot \operatorname{sgn}(\frac{\partial}{\partial X} P_{m+1})(-\infty, x_1) = 1$ and therefore $(-\infty, x_1) \cap \mathcal{N}(P_{m+1}) \neq \emptyset$. Consequently, $y_1 < x_1$. The leftmost block in (4.1) then consists of four columns and has the form

$$\begin{bmatrix} \operatorname{sgn} P_1(-\infty, x_1) & \operatorname{sgn} P_1(-\infty, x_1) & \operatorname{sgn} P_1(-\infty, x_1) & \operatorname{sgn} P_1(x_1) \\ \vdots & \vdots & \vdots & \vdots \\ \operatorname{sgn} P_m(-\infty, x_1) & \operatorname{sgn} P_m(-\infty, x_1) & \operatorname{sgn} P_m(-\infty, x_1) & \operatorname{sgn} P_m(x_1) \\ \operatorname{sgn} P_m(-\infty, x_1) & 0 & s_1 & s_1 \end{bmatrix}$$

$$= \begin{bmatrix} \operatorname{sgn} P_1(-\infty, y_1) & \operatorname{sgn} P_1(y_1) & \operatorname{sgn} P_1(y_1, x_1) & \operatorname{sgn} P_1(x_1) \\ \vdots & \vdots & \vdots & \vdots \\ \operatorname{sgn} P_m(-\infty, y_1) & \operatorname{sgn} P_m(y_1) & \operatorname{sgn} P_m(y_1, x_1) & \operatorname{sgn} P_m(x_1) \\ \operatorname{sgn} P_{m+1}(-\infty, y_1) & \operatorname{sgn} P_{m+1}(y_1) & \operatorname{sgn} P_{m+1}(y_1, x_1) & \operatorname{sgn} P_{m+1}(x_1) \end{bmatrix}$$

where the equality of the first m rows follows from the fact that $(-\infty, x_1) \cap \mathcal{N}(P_\mu) = \emptyset$ for $\mu = 1, \dots, m$, and the equality of the bottom rows follows from the fact that $((-\infty, x_1) \cup \{x_1\}) \cap \mathcal{N}(P_{m+1}) = \{y_1\}$.

(ii) If $s_\nu \cdot s_{\nu+1} \neq -1$, then $(x_\nu, x_{\nu+1}) \cap \{y_1, \dots, y_{N'}\} = \emptyset$, and we take $u_\nu = \{s_\nu, s_{\nu+1}\} \setminus \{0\}$ without using L_ν^-, L_ν^+. The middle block in (4.1) then consists of three columns and has the form

$$\begin{bmatrix} \operatorname{sgn} P_1(x_\nu) & \operatorname{sgn} P_1(x_\nu, x_{\nu+1}) & \operatorname{sgn} P_1(x_{\nu+1}) \\ \vdots & \vdots & \vdots \\ \operatorname{sgn} P_m(x_\nu) & \operatorname{sgn} P_m(x_\nu, x_{\nu+1}) & \operatorname{sgn} P_m(x_{\nu+1}) \\ s_\nu & u_\nu & s_{\nu+1} \end{bmatrix}$$

$$= \begin{bmatrix} \operatorname{sgn} P_1(x_\nu) & \operatorname{sgn} P_1(x_\nu, x_{\nu+1}) & \operatorname{sgn} P_1(x_{\nu+1}) \\ \vdots & \vdots & \vdots \\ \operatorname{sgn} P_m(x_\nu) & \operatorname{sgn} P_m(x_\nu, x_{\nu+1}) & \operatorname{sgn} P_m(x_{\nu+1}) \\ \operatorname{sgn} P_{m+1}(x_\nu) & \operatorname{sgn} P_{m+1}(x_\nu, x_{\nu+1}) & \operatorname{sgn} P_{m+1}(x_{\nu+1}) \end{bmatrix}$$

where $s_\nu = \operatorname{sgn} P_{m+1}(x_\nu)$ and $s_{\nu+1} = \operatorname{sgn} P_{m+1}(x_{\nu+1})$ by definition, and $\operatorname{sgn} P_{m+1}(x_\nu, x_{\nu+1}) \in \{\operatorname{sgn} P_{m+1}(x_\nu), \operatorname{sgn} P_{m+1}(x_{\nu+1})\} \setminus \{0\}$. To see that this last must hold, it is sufficient to recall that $\{x_\nu\} \cup (x_\nu, x_{\nu+1}) \cup \{x_{\nu+1}\}$ contains at most one element of $\mathcal{N}(P_{m+1})$, and to show that if $s_\nu \cdot s_{\nu+1} \neq -1$, then P_{m+1} does not vanish in $(x_\nu, x_{\nu+1})$. To this end, notice that if $\operatorname{sgn} P_{m+1}(x_\nu) \cdot \operatorname{sgn} P_{m+1}(x_{\nu+1}) = 0$, then P_m cannot vanish in $(x_\nu, x_{\nu+1})$ because $\#[(\{x_\nu\} \cup (x_\nu, x_{\nu+1}) \cup \{x_{\nu+1}\}) \cap \mathcal{N}(P_{m+1})] \leq 1$. If $\operatorname{sgn} P_{m+1}(x_\nu) \cdot \operatorname{sgn} P_{m+1}(x_{\nu+1}) = 1$, then P_{m+1} cannot vanish in $(x_\nu, x_{\nu+1})$ either because if $(x_\nu, x_{\nu+1}) \cap \mathcal{N}(P_{m+1}) = \{y\}$ then

$$\operatorname{sgn} P_{m+1}(x_\nu, y) = \operatorname{sgn} P_{m+1}(x_\nu) = \operatorname{sgn} P_{m+1}(x_{\nu+1}) = \operatorname{sgn} P_m(y, x_{\nu+1}) \neq 0,$$

whence $P_m(y) = (\frac{\partial}{\partial X} P_{m+1})(y) = 0$, by Proposition 2.1 and (2.4). However, this last is impossible, because all the roots of P_m belong to the sequence $x_1, \ldots, x_N$.

If $s_\nu \cdot s_{\nu+1} = -1$, then $u_\nu = 0$ and the interval $(x_\nu, x_{\nu+1})$ contains exactly one element of $\mathcal{N}(P_{m+1})$, say y_l. In this case the middle block in (4.1) consists of five columns and takes the form

$$\begin{bmatrix} \operatorname{sgn} P_1(x_\nu) & \operatorname{sgn} P_1(x_\nu, x_{\nu+1}) & \operatorname{sgn} P_1(x_\nu, x_{\nu+1}) & \operatorname{sgn} P_1(x_\nu, x_{\nu+1}) & \operatorname{sgn} P_1(x_{\nu+1}) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \operatorname{sgn} P_m(x_\nu) & \operatorname{sgn} P_m(x_\nu, x_{\nu+1}) & \operatorname{sgn} P_m(x_\nu, x_{\nu+1}) & \operatorname{sgn} P_m(x_\nu, x_{\nu+1}) & \operatorname{sgn} P_m(x_{\nu+1}) \\ s_\nu & s_\nu & u_\nu & s_{\nu+1} & s_{\nu+1} \end{bmatrix}$$
$$= \begin{bmatrix} \operatorname{sgn} P_1(x_\nu) & \operatorname{sgn} P_1(x_\nu, y_l) & \operatorname{sgn} P_1(y_l) & \operatorname{sgn} P_1(y_l, x_{\nu+1}) & \operatorname{sgn} P_1(x_{\nu+1}) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \operatorname{sgn} P_m(x_\nu) & \operatorname{sgn} P_m(x_\nu, y_l) & \operatorname{sgn} P_m(y_l) & \operatorname{sgn} P_m(y_l, x_{\nu+1}) & \operatorname{sgn} P_m(x_{\nu+1}) \\ \operatorname{sgn} P_{m+1}(x_\nu) & \operatorname{sgn} P_{m+1}(x_\nu, y_l) & \operatorname{sgn} P_{m+1}(y_l) & \operatorname{sgn} P_{m+1}(y_l, x_{\nu+1}) & \operatorname{sgn} P_{m+1}(x_{\nu+1}) \end{bmatrix}$$

where the equality of the first m rows follows from the fact that the polynomials $P_1, \ldots, P_m$ do not vanish in the interval $(x_\nu, x_{\nu+1})$, and the equality of the bottom rows follows from the fact that $(\{x_\nu\} \cup (x_\nu, x_{\nu+1}) \cup \{x_{\nu+1}\}) \cap \mathcal{N}(P_{m+1}) = \{y_l\}$.

(iii) For the rightmost block in (4.1) the reasoning is similar to case (i).

The result of Section 5.2 may be summarized as follows.

Lemma 5.1. *Let* $P_1, \ldots, P_m, P_{m+1} \in \mathcal{K}[X]$, $\frac{\partial}{\partial X} P_{m+1} = P_m \not\equiv 0$, *and*

$$s_k = \operatorname{sgn} P_{m+1}(x_k) \quad \textit{for } k = 1, \ldots, N$$

where $x_1, \ldots, x_N$ *is the sequence of elements of the field* $\mathcal{K}$ *such that*

$$\{x_1, \ldots, x_n\} = \bigcup_{\mu=1}^{m} \mathcal{N}(P_\mu) \quad \textit{and} \quad x_1 < \cdots < x_N.$$

Then the sequence $s_1, \ldots, s_N$ *does not contain any pair of successive zeros and*

$$\mathrm{SGN}(P_1, \ldots, P_m, P_{m+1}) = \mathbf{K}(\mathrm{SGN}(P_1, \ldots, P_m); s_1, \ldots, s_N)$$

where

$$\begin{aligned}\mathbf{K} : \{&m\text{-dimensional signatures of length } 2N+1\} \\ &\times \{\text{sequences in } \{-1,0,1\}^N \text{ without any pair of adjacent zeros}\} \\ &\qquad \to \{(m+1)\text{-dimensional signatures}\}\end{aligned}$$

is the mapping from Section 4.2*.*

5.3 The L. Hörmander division proposition

We shall use the following definition of the degree with respect to X, denoted by $\deg_X P$, of a polynomial $P \in \mathcal{R}[X, Y_1, \ldots, Y_m]$:

(a) if P is identically zero, then $\deg_X P = 0$,

(b) if P is not identically zero, then $\deg_X P = d$ if and only if $P(X, Y_1, \ldots, Y_n) = \sum_{k=0}^{d} a_k(Y_1, \ldots, Y_n) X^k$ where $a_k \in \mathcal{R}[Y_1, \ldots, Y_n]$ for $k = 0, \ldots, d$ and the polynomial a_d is not identically zero.

The polynomial $a_d \in \mathcal{R}[Y_1, \ldots, Y_n]$ occurring in (b) is called the *leading coefficient* of $P \in \mathcal{R}[X, Y_1, \ldots, Y_m]$ with respect to X.

Proposition 5.2. *Let* $\mathcal{R}$ *be a subring of a real closed field* $\mathcal{K}$*, and let* $P_1, \ldots, P_m \in \mathcal{R}[X, Y_1, \ldots, Y_n]$*. Let* $d_\mu = \deg_X P_\mu$ *and assume that* $1 \le d_\mu \le d_m$ *for every* $\mu = 1, \ldots, m-1$*. For every* $\mu = 1, \ldots, m$ *let* $a_\mu \in \mathcal{R}[Y_1, \ldots, Y_n]$ *be the leading coefficient of* P_μ *with respect to* X*. For every* $\mu = 1, \ldots, m-1$ *fix* $l_\mu \in \mathbb{N}$ *such that* $2l_\mu > d_m - d_\mu$*. Then, by Proposition* 3.1*, there are unique polynomials* $Q_1, \ldots, Q_m, R_1, \ldots, R_m \in \mathcal{R}[X, Y_1, \ldots, Y_n]$ *such that* $\deg_X R_\mu < d_\mu$ *for* $\mu = 1, \ldots, m$*,*

$$a_\mu^{2l_\mu} P_m = Q_\mu P_\mu + R_\mu \quad \text{for } \mu = 1, \ldots, m-1 \tag{5.3}$$

and

$$a_m^2 P_m = Q_m \tfrac{\partial}{\partial X} P_m + R_m. \tag{5.4}$$

Let $\mathcal{H}$ *be the mapping from* S_{2m} *into* S_m *defined in Section* 4.3*. Finally, suppose that* $y = (y_1, \ldots, y_n) \in \mathcal{K}^n$ *and*

$$\prod_{\mu=1}^{m} a_\mu(y) \ne 0.$$

Then

$$\mathrm{SGN}(P_1(\cdot, y), \ldots, P_{m-1}(\cdot, y), \tfrac{\partial}{\partial X} P_m(\cdot, y), R_1(\cdot, y), \ldots, R_m(\cdot, y)) \in D(\mathcal{H})$$

and

$$\mathcal{H}(\mathrm{SGN}(P_1(\cdot,y),\ldots,P_{m-1}(\cdot,y),\tfrac{\partial}{\partial X}P_m(\cdot,y),R_1(\cdot,y),\ldots,R_m(\cdot,y))) = \mathrm{SGN}(P_1(\cdot,y),\ldots,P_m(\cdot,y)).$$

The above proposition refines L. Hörmander's Lemma A.2.3 from the Appendix to [H3] stating that, for polynomials of one variable, $\mathrm{SGN}(P_1,\ldots,P_{m-1},\frac{\partial}{\partial X}P_m,R_1,\ldots,R_m)$ determines $\mathrm{SGN}(P_1,\ldots,P_m)$. In the proof of the projection theorem for semi-algebraic sets, Lemma A.2.3 (or our Proposition 5.2) is applied in the situation where division is made in the ring of polynomials of the variable X over the ring of polynomials of the variables $Y_1,\ldots,Y_n$. The assumption that $\prod_{\nu=1}^m a_\nu(y)\neq 0$ then causes difficulties mentioned in [H3] in the proof of Theorem A.2.2. The splitting discussed in Section 6 below permits us to overcome these difficulties.

Proof of Proposition 5.2. Fix $\mathring{y}\in\mathcal{K}^n$ such that

$$\prod_{\mu=1}^m a_\mu(\mathring{y})\neq 0 \tag{5.5}$$

and let

$$\begin{aligned}
&\mathrm{SGN}(P_1(\cdot,\mathring{y}),\ldots,P_{m-1}(\cdot,\mathring{y}),\tfrac{\partial}{\partial X}P_m(\cdot,\mathring{y}),R_1(\cdot,\mathring{y}),\ldots,R_m(\cdot,\mathring{y}))\\
&=\left[\begin{matrix}
\operatorname{sgn}P_1((-\infty,x_1),\mathring{y}) & \cdots & \operatorname{sgn}P_1(x_\nu,\mathring{y}) & \operatorname{sgn}P_1((x_\nu,x_{\nu+1}),\mathring{y})\\
\vdots & & \vdots & \vdots\\
\operatorname{sgn}P_{m-1}((-\infty,x_1),\mathring{y}) & \cdots & \operatorname{sgn}P_{m-1}(x_\nu,\mathring{y}) & \operatorname{sgn}P_{m-1}((x_\nu,x_{\nu+1}),\mathring{y})\\
\operatorname{sgn}\frac{\partial}{\partial X}P_m((-\infty,x_1),\mathring{y}) & \cdots & \operatorname{sgn}\frac{\partial}{\partial X}P_m(x_\nu,\mathring{y}) & \operatorname{sgn}\frac{\partial}{\partial X}P_m((x_\nu,x_{\nu+1}),\mathring{y})\\
\operatorname{sgn}R_1((-\infty,x_1),\mathring{y}) & \cdots & \operatorname{sgn}R_1(x_\nu,\mathring{y}) & \operatorname{sgn}R_1((x_\nu,x_{\nu+1}),\mathring{y})\\
\vdots & & \vdots & \vdots\\
\operatorname{sgn}R_m((-\infty,x_1),\mathring{y}) & \cdots & \operatorname{sgn}R_m(x_\nu,\mathring{y}) & \operatorname{sgn}R_m((x_\nu,x_{\nu+1}),\mathring{y})
\end{matrix}\right.\\
&\qquad\left.\begin{matrix}
\operatorname{sgn}P_1(x_{\nu+1},\mathring{y}) & \cdots & \operatorname{sgn}P_1((x_N,\infty),\mathring{y})\\
\vdots & & \vdots\\
\operatorname{sgn}P_{m-1}(x_{\nu+1},\mathring{y}) & \cdots & \operatorname{sgn}P_{m-1}((x_N,\infty),\mathring{y})\\
\operatorname{sgn}\frac{\partial}{\partial X}P_m(x_{\nu+1},\mathring{y}) & \cdots & \operatorname{sgn}\frac{\partial}{\partial X}P_m((x_N,\infty),\mathring{y})\\
\operatorname{sgn}R_1(x_{\nu+1},\mathring{y}) & \cdots & \operatorname{sgn}R_1((x_N,\infty),\mathring{y})\\
\vdots & & \vdots\\
\operatorname{sgn}R_m(x_{\nu+1},\mathring{y}) & \cdots & \operatorname{sgn}R_m((x_N,\infty),\mathring{y})
\end{matrix}\right]\\
&=\begin{bmatrix}
s_{1,0} & \cdots & s_{1,2\nu-1} & s_{1,2\nu} & s_{1,2\nu+1} & \cdots & s_{1,2N}\\
\vdots & & \vdots & \vdots & \vdots & & \vdots\\
s_{m-1,0} & \cdots & s_{m-1,2\nu-1} & s_{m-1,2\nu} & s_{m-1,2\nu+1} & \cdots & s_{m-1,2N}\\
s_{m,0} & \cdots & s_{m,2\nu-1} & s_{m,2\nu} & s_{m,2\nu+1} & \cdots & s_{m,2N}\\
r_{1,0} & \cdots & r_{1,2\nu-1} & r_{1,2\nu} & r_{1,2\nu+1} & \cdots & r_{1,2N}\\
\vdots & & \vdots & \vdots & \vdots & & \vdots\\
r_{m,0} & \cdots & r_{m,2\nu-1} & r_{m,2\nu} & r_{m,2\nu+1} & \cdots & r_{m,2N}
\end{bmatrix}.
\end{aligned}\tag{5.6}$$

Then conditions (4.3) and (4.4) are satisfied because $\deg_X P_\mu \geq 1$ for every $\mu = 1, \dots, m$. We are going to check that also conditions (4.5) and (4.6) are satisfied. Indeed, whenever $\nu = 1, \dots, N$ and

$$s_{\mu_i,2\nu-1} = \left.\begin{cases} \operatorname{sgn} P_{\mu_i}(x_\nu, \mathring{y}) & \text{if } \mu_i = 1, \dots, m-1 \\ \operatorname{sgn} \frac{\partial}{\partial X} P_m(x_\nu, \mathring{y}) & \text{if } \mu_i = m \end{cases}\right\} = 0, \qquad i = 1, 2, \dots,$$

for some $\mu_1, \mu_2 \in \{1, \dots, m\}$, then, by (5.3)–(5.4),

$$r_{\mu_1,2\nu-1} = \operatorname{sgn} R_{\mu_1}(x_\nu, \mathring{y}) = \operatorname{sgn} P_m(x_\nu, \mathring{y}) = \operatorname{sgn} R_{\mu_2}(x_\nu, \mathring{y}) = r_{\mu_2,2\nu-1},$$

so that condition (4.5) is satisfied. Finally, by (5.3) and (5.4), in the present situation for the sequence $s_1, \dots, s_{N'}$ defined in (4.6) one has

$$s_k = \operatorname{sgn} P_m(x_{\nu_k}, \mathring{y}) \quad \text{for } k = 1, \dots, N', \tag{5.7}$$

the subsequence $\nu_1, \dots, \nu_N$ being characterized by the condition that $\nu \in \{\nu_1, \dots, \nu_{N'}\}$ if and only if $0 \in \{\operatorname{sgn} P_1(x_\nu, \mathring{y}), \dots, \operatorname{sgn} P_{m-1}(x_\nu, \mathring{y}), \frac{\partial}{\partial X} P_m(x_\nu, \mathring{y})\}$. If for some $k = 1, \dots, N'$ both s_k and s_{k+1} were equal to zero, then, by (5.7) and the Lagrange theorem, some x-root of $\frac{\partial}{\partial X} P_m(x, \mathring{y})$ would belong to $(x_{\nu_k}, x_{\nu_{k+1}})$. But this is impossible, because by the characterization of the sequence $\nu_1, \dots, \nu_N$ just given, every x-root of $\frac{\partial}{\partial X} P_m(x, \mathring{y})$ must be one of $x_{\nu_1}, \dots, x_{\nu_N}$. Therefore condition (4.6) is satisfied.

Since conditions (4.3)–(4.6) are satisfied, the signature

$$\hat{s} = \operatorname{SGN}(P_1(\cdot, \mathring{y}), \dots, P_{m-1}(\cdot, \mathring{y}), \tfrac{\partial}{\partial X} P_m(\cdot, \mathring{y}), R_1(\cdot, \mathring{y}), \dots, R_m(\cdot, \mathring{y}))$$

belongs to the set $D(\mathcal{H}) \subset S_{2m}$ defined in Section 4.3, and so $\mathcal{H}(\hat{s})$ makes sense. Let us examine the results of the consecutive steps of the construction of $\mathcal{H}(\hat{s})$ for this $\hat{s}$.

Step 1. As already proved, the sequence $s_1, \dots, s_{N'}$ defined as in (4.6) coincides with $\operatorname{sgn} P_m(x_{\nu_1}, \mathring{y}), \dots, \operatorname{sgn} P_m(x_{\nu_{N'}}, \mathring{y})$.

Step 2. If in the matrix (5.6) we cancel all the m bottom rows, and next in the resulting $m \times (2N+1)$-matrix we reduce every s.a.i.c. to a single column, then we obtain an $m \times (2N'+1)$-matrix $\hat{s}'$ which is a signature belonging to S_m and having length $2N'+1$, where N' is the same as in Step 1. According to Section 5.1,

$$\hat{s}' = \operatorname{SGN}(P_1(\cdot, \mathring{y}), \dots, P_{m-1}(\cdot, \mathring{y})). \tag{5.8}$$

Step 3. By (5.7), (5.8) and by Lemma 5.1, if the matrix $\mathbf{K}(\hat{s}'; s_1, \dots, s_{N'})$ is constructed in accordance with the rules given in Section 4.2, then

$$\begin{aligned} &\mathbf{K}(\operatorname{SGN}(P_1(\cdot, \mathring{y}), \dots, P_{m-1}(\cdot, \mathring{y}), \tfrac{\partial}{\partial X} P_m(\cdot, \mathring{y}); s_1, \dots, s_{N'})) \\ &\qquad\qquad = \operatorname{SGN}(P_1(\cdot, \mathring{y}), \dots, P_{m-1}(\cdot, \mathring{y}), \tfrac{\partial}{\partial X} P_m(\cdot, \mathring{y}), P_m(\cdot, \mathring{y})). \end{aligned}$$

Step 4. In accordance with Section 4.3, in order to obtain $\mathcal{H}(\hat{s})$ we have to cancel in the matrix $\operatorname{SGN}(P_1(\cdot, \mathring{y}), \dots, P_{m-1}(\cdot, \mathring{y}), \frac{\partial}{\partial X} P_m(\cdot, \mathring{y}), P_m(\cdot, \mathring{y}))$ the mth row and next replace each s.a.i.c. by a single column. According to Section 5.1 we then obtain $\operatorname{SGN}(P_1(\cdot, \mathring{y}), \dots, P_{m-1}(\cdot, \mathring{y}), P_m(\cdot, \mathring{y}))$, and this completes the proof of Proposition 5.2.

6 Some splitting algorithms

Let $\mathcal{K}$ be a real closed field and $\mathcal{R}$ a subring of $\mathcal{K}$. Write y and Y instead of $(y_1, \dots, y_n)$ and $(Y_1, \dots, Y_n)$. For every $P_1, \dots, P_m \in \mathcal{R}[X, Y]$ and $\hat{s} \in S_m$ define

$$B_{P_1,\dots,P_m;\hat{s}} = \{y \in \mathcal{K}^n : \mathrm{SGN}(P_1(\cdot, y), \dots, P_m(\cdot, y)) = \hat{s}\}.$$

For fixed $P_1, \dots, P_m$ define $\alpha = \{\mu \in \{1, \dots, m\} : \deg_X P_\mu \geq 1\}$ and $\beta = \{\mu \in \{1, \dots, m\} : \deg_X P_\mu = 0\}$. If $\alpha \neq \emptyset$, then let $\alpha = \{\alpha_1, \dots, \alpha_k\}$ where $1 \leq \alpha_1 < \dots < \alpha_k \leq m$. If $\beta \neq \emptyset$, then let $\beta = \{\beta_1, \dots, \beta_l\}$ where $1 \leq \beta_1 < \dots < \beta_l \leq m$. If $\beta \neq \emptyset$, then the polynomials $P_{\beta_1}, \dots, P_{\beta_l}$ do not depend on X, so that $B_{P_1,\dots,P_m;\hat{s}}$ may be non-empty only if $s_{\beta_\lambda,0} = s_{\beta_\lambda,1} = \dots = s_{\beta_\lambda,2N}$ for every $\lambda = 1, \dots, l$, and if this is the case, then

$$(6.1) \quad B_{P_1,\dots,P_m;\hat{s}} = B_{P_{\alpha_1},\dots,P_{\alpha_k};\hat{s}'} \cap \bigcap_{\lambda=1}^{l} \{y \in \mathcal{K}^n : \operatorname{sgn} P_{\beta_\lambda}(y) = s_{\beta_\lambda,0} = s_{\beta_\lambda,1} = \dots = s_{\beta_\lambda,2N}\}$$

where $\hat{s}' = (s_{\alpha_\kappa,\nu})_{\kappa=1,\dots,k;\nu=0,\dots,2N} \in S_k$ and $2N + 1 = \mathrm{length}(\hat{s})$. If either $\alpha = \emptyset$ or $\beta = \emptyset$, then on the right of (6.1) either $B_{P_{\alpha_1},\dots,P_{\alpha_k};\hat{s}'}$ or $\bigcap_{\lambda=1}^{l} \cdots$ has to be omitted.

Proposition 6.1. *If* $\max_{\mu=1,\dots,m} \deg_X P_\mu = 0$, *then* $B_{P_1,\dots,P_m;\hat{s}} \in \mathcal{A}_n(\mathcal{K}; \mathcal{R})$. *If* $\max_{\mu=1,\dots,m} \deg_X P_\mu = d \geq 1$, *then*

$$(6.2) \quad B_{P_1,\dots,P_m;\hat{s}} = A \cup \bigcup_{\iota \in J} (A_\iota \cap B_{P_{\iota,1},\dots,P_{\iota,m_\iota};\hat{s}})$$

where

(6.3) J *is a finite set,*

(6.4) $\mathcal{A} \in \mathcal{A}_n(\mathcal{K}; \mathcal{R})$ *and* $\mathcal{A}_\iota \in \mathcal{A}_n(\mathcal{K}; \mathcal{R})$ *for every* $\iota \in J$,

(6.5) $1 \leq m_\iota \leq m$ *and* $\hat{s}_\iota \in S_{m_\iota}$ *for every* $\iota \in J$,

and the polynomials $P_{\iota,\mu} \in \mathcal{R}[X, Y]$, $\iota \in J$, $\mu = 1, \dots, m_\iota$, *have the following properties:*

(6.6) $1 \leq \deg_X P_{\iota,\mu} \leq d$ *for every* $\iota \in J$ *and* $\mu = 1, \dots, m_\iota$,

(6.7) $\#\{\mu = 1, \dots, m_\iota : \deg_X P_{\iota,\mu} = d\} \leq \#\{\mu = 1, \dots, m : \deg_X P_\mu = d\}$ *for every* $\iota \in J$,

(6.8) *whenever* $\iota \in J$, *then* $y \in A_\iota \Rightarrow (a_{\iota,1}(y) \neq 0) \wedge \dots \wedge (a_{\iota,m_\iota}(y) \neq 0)$ *where* $a_{\iota,\mu} \in \mathcal{R}[Y]$ *is the leading coefficient in the development of* $P_{\iota,\mu} \in \mathcal{R}[X, Y]$ *with respect to* X.

Proof. The statement concerning the case when $\deg_X P_\mu = 0$ for every μ follows directly from (6.1). If $\max_{\mu=1,\dots,m} \deg_X P_\mu = d \geq 1$, then for every μ consider the development

$$P_\mu(X,Y) = \sum_{k=0}^{d} a_{\mu,k}(Y)X^k$$

where $a_{\mu,k} \in \mathcal{R}[Y]$ for $k = 0,\dots,d$, and some of the polynomials $a_{\mu,k}$ may be identically zero.

For $\mu = 1,\dots,m$ and $\nu = 0,\dots,d$ consider the polynomials

$$P_{\mu,\nu}(X,Y) = \sum_{k=0}^{\nu} a_{\mu,k}(Y)X^k$$

belonging to $\mathcal{R}[X,Y]$, and the sets

$$A_{\mu,0} = \{y \in \mathcal{K}^n : a_{\mu,k}(y) = 0 \text{ for } k = 1,\dots,d\},$$
$$A_{\mu,\nu} = \{y \in \mathcal{K}^n : \sup\{k = 0,\dots,d : a_{\mu,k}(y) \neq 0\} = \nu\} \quad \text{for } \nu = 1,\dots,d$$

belonging to $\mathcal{A}_n(\mathcal{K};\mathcal{R})$, some of which may be empty. Then

(6.9) for every $\mu = 1,\dots,m$ the sets $A_{\mu,0},\dots,A_{\mu,d}$ are mutually disjoint and $\bigcup_{\nu=0}^{d} A_{\mu,\nu} = \mathcal{K}^n$,

(6.10) whenever $\mu = 1,\dots,m$, $\nu = 0,\dots,d$ and $A_{\mu,\nu} \neq \emptyset$, then $P_\mu(x,y) = P_{\mu,\nu}(x,y)$ for every $x \in \mathcal{K}$ and $y \in A_{\mu,\nu}$,

(6.11) $\deg_X P_{\mu,0} = 0$ for $\mu = 1,\dots,m$,

(6.12) whenever $\mu = 1,\dots,m$, $\nu = 1,\dots,d$ and $A_{\mu,\nu} \neq \emptyset$, then $\deg_X P_{\mu,\nu} = \nu \geq 1$ and in the development of $P_{\mu,\nu}$ with respect to X the leading coefficient $a_{\mu,\nu} \in \mathcal{R}[Y]$ does not vanish on $A_{\mu,\nu}$.

By (6.9) and (6.10) one has

$$B_{P_1,\dots,P_m;\hat{s}} = \bigcup_{(\nu_1,\dots,\nu_m)\in(0,\dots,d)^m} A_{1,\nu_1} \cap \dots \cap A_{m,\nu_m} \cap B_{P_{1,\nu_1},\dots,P_{m,\nu_m};\hat{s}}$$

whence the conditions (6.2)–(6.8) follow from (6.1), (6.11) and (6.12).

Proposition 6.2. *Let* $P_1,\dots,P_m \in \mathcal{R}[X,Y_1,\dots,Y_n]$ *and define* $d = \max_{\mu=1,\dots,m} d_\mu$ *where* $d_\mu = \deg_X P_\mu$. *Assume that*

$$d_m = d \quad \text{and} \quad d_\mu \geq 1 \quad \text{for every } \mu = 1,\dots,m.$$

Assume further that

$$\mathcal{A} \in \mathcal{A}_n(\mathcal{K},\mathcal{R}) \quad \text{and} \quad \prod_{\mu=1}^{m} a_\mu(y_1,\dots,y_m) \neq 0 \quad \text{for every } (y_1,\dots,y_m) \in \mathcal{A}$$

where $a_1, \dots, a_m \in \mathcal{R}[Y_1, \dots, Y_n]$ *are the leading coefficients in the developments of* $P_1, \dots, P_m$ *with respect to* X. *For every* $\mu = 1, \dots, m-1$ *fix* $l_\mu \in \mathbb{N}$ *such that* $2l_\mu > d - d_\mu$, *and let* $R_1, \dots, R_m \in \mathcal{R}[X, Y_1, \dots, Y_n]$ *be the remainders of* $a_1^{2l_1} P_m, \dots, a_{m-1}^{2l_{m-1}} P_m$, $a_m^2 P_m$ *divided by* $P_1, \dots, P_{m-1}, \frac{\partial}{\partial X} P_m$. *Finally, let* $\hat{s} \in S_m$. *Then*

$$A \cap B_{P_1,\dots,P_m;\hat{s}} = \bigcup_{\substack{\hat{s}' \in D(\mathcal{H}) \\ \mathrm{length}(\hat{s}') \le l \\ \mathcal{H}(\hat{s}') = \hat{s}}} (A \cap B_{P_1,\dots,P_{m-1},\frac{\partial}{\partial X}P_m, R_1,\dots,R_m;\hat{s}'}) \tag{6.13}$$

where $\mathcal{H} : S_{2m} \supset D(\mathcal{H}) \to S_m$ *is the mapping defined in Section* 4.3 *and*

$$l = 1 + 2((m-1)d + (m+1)(d-1)).$$

Proposition 6.2 constitutes a basic element of the proof of the projection theorem for semi-algebraic sets sketched by L. Hörmander in the Appendix to [H3]. Let

$$\begin{aligned} k &= \#\{\mu = 1, \dots, m : d_\mu = d\}, \\ d' &= \max\{\deg_X P_1, \dots, \deg_X \tfrac{\partial}{\partial X} P_m, \deg_X R_1, \dots, \deg_X R_m\}, \\ k' &= \#\{P \in \{P_1, \dots, P_{m-1}, \tfrac{\partial}{\partial X} P_m, R_1, \dots, R_m\} : \deg_X P = d'\}. \end{aligned}$$

In Proposition 6.2 it is important that

(i) either $d' < d$ or ($d' = d$ and $k' < k$).

It is also important that

(ii) the union in (6.13) is finite.

Proof of Proposition 6.2. Let us write y instead of $(y_1, \dots, y_n)$. By Proposition 5.2, one has

$$\mathrm{SGN}(P_1(\cdot, y), \dots, P_{m-1}(\cdot, y), \tfrac{\partial}{\partial X} P_m(\cdot, y), R_1(\cdot, y), \dots, R_m(\cdot, y)) \in D(\mathcal{H})$$

for every $y \in A$, and

$$\begin{aligned} A \cap B_{P_1,\dots,P_m;\hat{s}} &= A \cap \{y \in \mathcal{K}^n : \mathrm{SGN}(P_1(\cdot, y), \dots, P_m(\cdot, y)) = \hat{s}\} \\ &= A \cap \{y \in \mathcal{K}^n : \mathcal{H}(\mathrm{SGN}(P_1(\cdot, y), \dots, P_{m-1}(\cdot, y), \tfrac{\partial}{\partial X} P_m(\cdot, y), \\ &\qquad R_1(\cdot, y), \dots, R_m(\cdot, y))) = \hat{s}\}. \end{aligned}$$

It follows that

$$\begin{aligned} A \cap B_{P_1,\dots,P_m;\hat{s}} = A \cap \{y \in \mathcal{K}^n : \mathcal{H}_l(\mathrm{SGN}(P_1(\cdot, y), \dots, P_{m-1}(\cdot, y), \tfrac{\partial}{\partial X} P_m(\cdot, y), \\ R_1(\cdot, y), \dots, R_m(\cdot, y))) = \hat{s}\} \end{aligned}$$

where $\mathcal{H}_l = \mathcal{H}|_{D(\mathcal{H}_l)}$ and $D(\mathcal{H}_l) = \{\hat{s}' \in D(\mathcal{H}) : \mathrm{length}(\hat{s}') \le l\}$. Hence

$$\begin{aligned} A \cap B_{P_1,\dots,P_m;\hat{s}} &= A \cap \{y \in \mathcal{K}^n : \mathrm{SGN}(P_1(\cdot, y), \dots, P_{m-1}(\cdot, y), \tfrac{\partial}{\partial X} P_m(\cdot, y), \\ &\qquad R_1(\cdot, y), \dots, R_m(\cdot, y)) \in \mathcal{H}_l^{-1}(\hat{s})\} \\ &= \bigcup_{\hat{s}' \in \mathcal{H}_l^{-1}(\hat{s})} (A \cap B_{P_1,\dots,P_{m-1},\frac{\partial}{\partial X}P_m, R_1,\dots,R_m;\hat{s}'}). \end{aligned}$$

7 Proof of Theorem 1

In the present section, J denotes a finite set, ι is an element of J, and, for every ι, m_ι is a finite natural number. It is sufficient to prove Theorem 1 for $l = 1$. In this case $\mathbf{P}$ is the projection of $\mathcal{K}^{1+n}$ onto $\mathcal{K}^n$ such that $\mathbf{P}(x, y_1, \ldots, y_n) = (y_1, \ldots, y_n)$ for every $x, y_1, \ldots, y_n \in \mathcal{K}$.

In accordance with (1.1) each set belonging to $\mathcal{A}_{1+n}(\mathcal{K}; \mathcal{R})$ has the form

$$A = \bigcup_{\iota \in J} \bigcap_{\mu=1}^{m_\iota} \{(x, y_1, \ldots, y_n) \in \mathcal{K}^{1+n} : \operatorname{sgn} P_{\iota,\mu}(x, y_1, \ldots, y_n) = s_{\iota,\mu}\}$$

where $P_{\iota,\mu} \in \mathcal{R}[X, Y_1, \ldots, Y_n]$ and $s_{\iota,\mu} \in \{-1, 0, 1\}$. It follows that

$$\begin{aligned} (7.1) \qquad \mathbf{P}A &= \bigcup_{\iota \in J} \{(y_1, \ldots, y_n) \in \mathcal{K}^n : \exists_{x \in \mathcal{K}} \, [\operatorname{sgn} P_{\iota,\mu}(x, y_1, \ldots, y_n) = s_{\iota,\mu} \\ &\qquad\qquad \text{for every } \mu = 1, \ldots, m_\iota]\} \\ &= \bigcup_{\iota \in J} \{(y_1, \ldots, y_n) \in \mathcal{K}^n : \text{ the matrix } \operatorname{SGN}(P_{\iota,1}(\cdot, y), \ldots, P_{\iota,m_\iota}(\cdot, y)) \\ &\qquad\qquad \text{contains a column equal to } (s_{\iota,1}, \ldots, s_{\iota,m_\iota})^\dagger\} \\ &= \bigcup_{\iota \in J} \bigcup_{\hat{s} \in F_\iota} B_{P_{\iota,1}, \ldots, P_{\iota,m_\iota}; \hat{s}} \end{aligned}$$

where

$$\begin{aligned} F_\iota = \Big\{ \hat{s} \in S_{m_\iota} : \operatorname{length}(\hat{s}) \le 1 + 2 \sum_{\mu=1}^{m_\iota} \deg_X P_{\iota,\mu}, \\ \hat{s} \text{ contains a column equal to } (s_{\iota,1}, \ldots, s_{\iota,m_\iota})^\dagger \Big\} \end{aligned}$$

is a finite subset of S_{m_ι}.

For every $d = 0, 1, \ldots$ and $k = 1, 2, \ldots$ denote by $\mathcal{B}_{d,k}$ the family of all the subsets B of $\mathcal{K}^n$ of the form

$$(7.2) \qquad B = \bigcup_{\iota \in J} (A_\iota \cap B_{P_{\iota,1}, \ldots, P_{\iota,m_\iota}; \hat{s}_\iota})$$

such that J is a finite set and, whenever $\iota \in J$, then $A_\iota \in \mathcal{A}_n(\mathcal{K}; \mathcal{R})$, $m_\iota \in \mathbb{N}$, $\hat{s}_\iota \in S_{m_\iota}$, $P_{\iota,1}, \ldots, P_{\iota,m_\iota} \in \mathcal{R}[X, Y_1, \ldots, Y_n]$, $\deg_X P_{\iota,\mu} \le d$ for every $\mu = 1, \ldots, m_\iota$ and $\#\{\mu = 1, \ldots, m_\iota : \deg_X P_{\iota,\mu} = d\} \le k$. From (7.1) it follows that

(7.3) whenever $A \in \mathcal{A}_{1+n}(\mathcal{K}; \mathcal{R})$, then $\mathbf{P}A \in \mathcal{B}_{d,k}$ for some d and k.

If $d = 0$, then all the polynomials of $P_{\iota,\mu}$ occurring in (7.2) are independent of X, so that $B_{P_{\iota,1}, \ldots, P_{\iota,m_\iota}; \hat{s}_\iota}$ may be non-empty only if $\hat{s}_\iota$ consists of a single column, say $(s_{\iota,1},\dots,s_{\iota,m_\iota})^\dagger$, and then

$$B_{P_{\iota,1},\dots,P_{\iota,m_\iota};\hat{s}_\iota} = \bigcap_{\iota\in J}\bigcup_{\mu=1}^{m_\iota}\{(y_1,\dots,y_n)\in\mathcal{K}^n : \operatorname{sgn} P_{\iota,\mu}(y_1,\dots,y_n) = s_{\iota,\mu}\} \in \mathcal{A}_n(\mathcal{K};\mathcal{R}).$$

Therefore

$$\bigcup_{k=1}^{\infty}\mathcal{B}_{0,k} = \mathcal{A}_n(\mathcal{K};\mathcal{R}). \tag{7.4}$$

Furthermore, a subsequent application of Propositions 6.1 and 6.2 shows that for all $d = 1,2,\dots,$

$$\begin{aligned} \mathcal{B}_{d,k_0} &= \mathcal{B}_{d,k_0-1} && \text{if } k_0 > 1,\\ \mathcal{B}_{d,k_0} &= \bigcup_{k=1}^{\infty}\mathcal{B}_{d-1,k} && \text{if } k_0 = 1. \end{aligned} \tag{7.5}$$

If $A\in\mathcal{A}_{n+1}(\mathcal{K};\mathcal{R})$, then, by (7.3), $\mathbf{P}A\in\mathcal{B}_{d,k_0}$ for some $d = 0,1,\dots$ and $k_0 = 1,2,\dots.$ If $d = 0$, then $\mathbf{P}A\in\mathcal{A}_n(\mathcal{K};\mathcal{R})$ by (7.4). If $d > 0$, then by (7.5) there are $k_1,\dots,k_d\in\{1,2,\dots\}$ such that

$$\begin{aligned} \mathbf{P}A\in\mathcal{B}_{d,k_0} = \mathcal{B}_{d,k_0-1} = \dots = \mathcal{B}_{d,1} &\Rightarrow \mathbf{P}A\in\mathcal{B}_{d-1,k_1} = \dots = \mathcal{B}_{d-1,1}\\ &\Rightarrow \mathbf{P}A\in\mathcal{B}_{d-2,k_2} = \dots = \mathcal{B}_{d-2,1}\\ &\dots\\ &\Rightarrow \mathbf{P}A\in\mathcal{B}_{0,k_d}\subset\mathcal{A}_n(\mathcal{K};\mathcal{R}). \end{aligned}$$

References

[A-Z] Z. Adamowicz and P. Zbierski, *Logic of Mathematics, A Modern Course of Classical Logic*, Wiley, 1997.

[B] N. Bourbaki, *Eléments de Mathématique, Livre II, Algèbre*, ch. VI, 2nd ed., Hermann, Paris, 1959; Russian transl., Nauka, Moscow, 1965.

[C1] P. J. Cohen, *A simple proof of Tarski's theorem on elementary algebra*, Mimeographed manuscript, Stanford Univ., 1967.

[C2] P. J. Cohen, *Decision procedures for real and p-adic fields*, Comm. Pure Appl. Math. 22 (1969), 131–151.

[F] A. Friedman, *Generalized Functions and Partial Differential Equations*, Prentice-Hall, 1963.

[G] E. A. Gorin, *Asymptotic properties of polynomials and algebraic functions of several variables*, Uspekhi Mat. Nauk 16 (1961), no. 1, 91–118 (in Russian).

[H1] L. Hörmander, *On the theory of general partial differential operators*, Acta Math. 94 (1955), 161–248.

[H2] L. Hörmander, *Linear Partial Differential Operators*, Springer, 1963.

[H3] L. Hörmander, *The Analysis of Linear Partial Differential Operators II. Operators with Constant Coefficients*, Springer, 1983.

[L] S. Lang, *Algebra*, Addison-Wesley, 1965; Russian translation, Mir, Moscow, 1968.

[S] A. Seidenberg, *A new decision method for elementary algebra*, Ann. of Math. 60 (1954), 365–374.

[T1] A. Tarski, *A Decision Method for Elementary Algebra and Geometry*, RAND Corporation, 1948.

[T2] A. Tarski, *A Decision Method for Elementary Algebra and Geometry*, 2nd ed., Univ. of California Press, Berkeley and Los Angeles, 1951.

[Tr] F. Treves, *Lectures on Linear Partial Differential Equations with Constant Coefficients*, Inst. Mat. Pura Apl., Rio de Janeiro, 1961.

[W] B. L. van der Waerden, *Algebra I*, 8th ed., Springer 1971 (in German); Russian transl., Nauka, Moscow, 1979.