Proofs of the Lemmas stated in
"Algebraic Certificates of (Semi)Definiteness for Polynomials Over Fields Containing the Rationals"

Laura Menini*, Corrado Possieri† and Antonio Tornambè‡

Dipartimento di Ingegneria Civile e Ingegneria Informatica,
Università di Roma Tor Vergata, 00133 Roma, Italy
Technical Report RR-17.13

Abstract

In this document, the proofs of the lemmas stated in [1] are reported.

Proof. (of Lemma 4) Let \( p \in \tilde{\Sigma}^{K}_{2d,m}[x] \) be written as \( p = \sum_{i=1}^{m} w_{i}h_{i}^{2} \). By absurd, assume that there exists \((c_{1}, \ldots , c_{m}) \neq (0, \ldots , 0)\), such that \( c_{1}h_{1} + \ldots + c_{m}h_{m} = 0 \) in \( K[x] \). If \( c_{i} \neq 0 \), then \( h_{i} \) can be expressed as a linear combination of the other \( m - 1 \) forms. Hence, \( p \) is a quadratic function of \( h_{1}, \ldots , h_{i-1}, h_{i+1}, \ldots , h_{m} \), whence, by applying Algorithm 1, that \( p \) is a wSOS with at most \( m - 1 \) squares, which contradicts the hypothesis that \( p \in \tilde{\Sigma}^{K}_{2d,m}[x] \). The case \( w_{i} = 0 \) is trivial. \( \square \)

Proof. (of Lemma 5) Proof of (5.1). The proof is trivial if \( m = 1 \). Let \( m \geq 2 \). Let \( m^{*} \in Z \) be such that \( m \geq m^{*} \geq 1 \) and \( \Sigma^{K}_{2d,m^{*}}[x] \neq \emptyset \). Since \( \Sigma^{K}_{2d,m^{*}}[x] \cup \Sigma^{K}_{2d,m^{*}-1}[x] = \Sigma^{K}_{2d,m}[x] \) and \( \Sigma^{K}_{2d,m^{*}}[x] \cap \Sigma^{K}_{2d,m^{*}-1}[x] = \emptyset \), one has \( S_{m}^{-1}(\Sigma^{K}_{2d,m^{*}}[x]) \cap S_{m}^{-1}(\Sigma^{K}_{2d,m^{*}-1}[x]) = \emptyset \) and \( S_{m}^{-1}(\Sigma^{K}_{2d,m^{*}}[x]) \cup S_{m}^{-1}(\Sigma^{K}_{2d,m^{*}-1}[x]) = S_{m}^{-1}(\Sigma^{K}_{2d,m}[x]) \). Since \( \Sigma^{K}_{2d,m^{*}}[x] \neq \emptyset \), \( x^{2d} \in \Sigma^{K}_{2d,m}[x] \) for \( m \geq 1 \), and \( x^{2d} \notin \tilde{\Sigma}^{K}_{2d,m^{*}}[x] \) for \( m^{*} > 1 \), one has that \( S_{m}^{-1}(\tilde{\Sigma}^{K}_{2d,m^{*}}[x]) \) is a proper subset of \( S_{m}^{-1}(\Sigma^{K}_{2d,m}[x]) \). By Lemma 4, set \( \Sigma^{K}_{2d,m^{*}-1}[x] \) is obtained from \( p = \sum_{i=1}^{m^{*}} w_{i}h_{i}^{2} \) by imposing that either at least one of the \( w_{i} \)'s is zero or the \( h_{1}, \ldots , h_{m} \), are linearly dependent, whence the Zariski closure of \( S_{m}^{-1}(\Sigma^{K}_{2d,m^{*}-1}[x]) \) is a proper variety of \( S_{m}^{-1}(\Sigma^{K}_{2d,m}[x]) \). This implies that \( S_{m}^{-1}(\tilde{\Sigma}^{K}_{2d,m^{*}}[x]) \) is Zariski open.

Proof of (5.2). By (5.1), there are only two cases: either \( \tilde{\Sigma}^{K}_{2d,m}[x] = \emptyset \) or \( S_{m}^{-1}(\tilde{\Sigma}^{K}_{2d,m}[x]) \) is a Zariski open of \( S_{m}^{-1}(\Sigma^{K}_{2d,m}[x]) \). To show that \( m = m^{*} \) it is sufficient to show that

---

*L. Menini: menini@disp.uniroma2.it
†C. Possieri: possieri@ing.uniroma2.it
‡A. Tornambè: tornambe@disp.uniroma2.it
all the points belonging to the line parameterized by $x$ of (7.1) follows from Theorem 4. Moreover, if $x$ is not finite.

Proof. (of Lemma 6) Let $H(\tilde{B}) \in \mathbb{K}^{m,2 \times n,2 d}$ be such that $M_{h2}^{\tilde{h}} = H(\tilde{B})M_{z2}^{z}$, where $M_{h2}^{\tilde{h}} := [\tilde{h}_1^2 \tilde{h}_1 \tilde{h}_2 \ldots \tilde{h}_m^2]^T$.

(P.1) For $n \geq m \geq 2$ and for all $d \in \mathbb{Z}_{\geq 2}$, polynomials $h_1^2, h_1 h_2, h_2^2, \ldots, h_1 h_m, \ldots, h_m^2$ are linearly independent over $\mathbb{K}$ if and only if matrix $H(\tilde{B})$ has full row rank.

(P.2) If matrix $H(\tilde{B}^o)$ has full row rank for a certain $\tilde{B}^o \in \mathbb{K}^{m,2 \times n,2 d} \subseteq \mathbb{R}^{m,2 \times n,2 d}$, then there exists an open neighborhood $B \subseteq \mathbb{R}^{m,2 \times n,2 d}$ of $\tilde{B}^o$ such that $H(\tilde{B})$ has full row rank for all $\tilde{B} \in B$. Let $S \subseteq \mathbb{K}^{m,2 \times n,2 d}$ be the set of all $\tilde{B} \in \mathbb{K}^{m,2 \times n,2 d}$ such that $H(\tilde{B})$ has full row rank. The Zariski closure $\overline{S}$ of $S$ does not coincide with $\mathbb{K}^{m,2 \times n,2 d}$, because, in that case, for any open neighborhood $B \subseteq \mathbb{R}^{m,2 \times n,2 d}$ of $\tilde{B}^o$, there would exist $\tilde{B}^* \in B$ such that $H(\tilde{B}^*)$ has full row rank, being $\mathbb{K}$ dense in $\mathbb{R}$. Hence, if $H(\tilde{B}^o)$ has full row rank for some $\tilde{B}^o \in \mathbb{K}^{m,2 \times n,2 d}$, then it has full row rank for “almost all” $\tilde{B} \in \mathbb{K}^{m,2 \times n,2 d}$.

(P.3) For $n \geq m, 2 \geq \forall d \in \mathbb{Z}_{\geq 2}$, by (P.1) and (P.2), if there exist $\tilde{h}_1^o, \ldots, \tilde{h}_m^o \in \mathbb{K}|x|_d$ in the reduced echelon form so that $(h_1^o)^2, h_1^o h_2^o, (h_2^o)^2, \ldots, h_1^o h_m^o, \ldots, (h_m^o)^2$ are linearly independent over $\mathbb{K}$, then $\tilde{h}_1^2, \tilde{h}_1 \tilde{h}_2, \tilde{h}_2^2, \ldots, \tilde{h}_1 h_m, \ldots, h_m^2$ are linearly independent for “almost all” $\tilde{h}_1, \ldots, \tilde{h}_m \in \mathbb{K}|x|_d$.

(P.4) Since any $p$ in $\mathbb{K}|x_1, \ldots, x_n|_d$ can be coerced into $\mathbb{K}|x_1, \ldots, x_n, x_{n+1}|_d$, if (P.3) holds for $n = m$, then it holds for any $n \geq m$.

(P.5) Let $n = m, h_i = x_i^{d-1} x_i, i = 1, \ldots, n$. Forms $\tilde{h}_i \tilde{h}_j = x_1^{2(d-1)} x_i x_j, i, j = 1, \ldots, n$ are linearly independent.

Proof. (of Lemma 7) Without loss of generality, let $i = n$. Fix the GRL order $> G$ on $\mathbb{K}|x|$, with $x_1 > G x_2 > G \ldots > G x_n$, and let $p \in \mathbb{K}|x|_d$. First, it is proved that if LM$(p) = x_n^d$, then $p = a x_n^d$, for some constant $a \in \mathbb{K}, a \neq 0$. As a matter of fact, since $p$ is homogeneous, all its terms have the same degree. Thus, assume that LM$(p) = x_n^d$ and, by absurd, that $p$ contains a monomial $x^\beta = x_1^{\beta_1} \ldots x_n^{\beta_n}, \sum_{i=1}^{n} \beta_i = d$, different from $x_n^d$. This yields a contradiction, because if $x_1^{\beta_1} \ldots x_n^{\beta_n} \neq x_n^d, \sum_{i=1}^{n} \beta_i = d$, then $x_1^{\beta_1} \ldots x_n^{\beta_n} > G x_n^d$, whence $x_n^d$ is not the leading monomial of $p$. Therefore, the proof of (7.1) follows from Theorem 4. Moreover, if $x_i^\alpha \in I$, then $x_i \in \sqrt{I}, i = 1, \ldots, n$, which proves (7.2).

Proof. (of Lemma 8) Proof of (8.1). Let $\hat{a} \in \mathbb{K}^\ell$ be any specialization of the parameters. First, note that, since the polynomials $p_i(a, x), i = 1, \ldots, m$, are homogeneous for any specialization, one has $p_i(\hat{a}, 0) = 0, i = 1, \ldots, m$, for each $\hat{a} \in \mathbb{K}^\ell$, whence $0 \in V_{\mathbb{K}^n}(I_0)$. Now, assume that there exists a point $\hat{x} \in \mathbb{K}^n, \hat{x} \neq 0$, belonging to $V_{\mathbb{K}^n}(I_0)$; this implies that $p_i(\hat{a}, \hat{x}) = 0, i = 1, \ldots, m$. Therefore, taking into account the homogeneity, by letting $x = \theta \hat{x}, \theta \in \mathbb{K}$, one has $p_i(\hat{a}, \theta \hat{x}) = \theta p_i(\hat{a}, \hat{x}) = 0, i = 1, \ldots, m$, which shows that all the points belonging to the line parameterized by $x = \theta \hat{x}$ belong to $V_{\mathbb{K}^n}(I_0)$, which, therefore, is not finite.
Proof of (8.2). Let \( \hat{a} \in \mathbb{K}^\ell \) be such that the variety \( V_{\mathbb{K}^n}(I_{\hat{a}}) \) of \( \mathbb{K}^n \) is finite. By (8.1), one has \( V_{\mathbb{K}^n}(I_{\hat{a}}) = \{0\} \), whence \( V_{\mathbb{K}^n}(I_{\hat{a}} \cap \mathbb{K}[x_i]) = \{0\} \); \( I_{\hat{a}} \cap \mathbb{K}[x_i] \) is a principal ideal, which is therefore generated by one monic polynomial \( q(x_i) \) in \( x_i \), which satisfies \( q(0) = 0 \), because \( V_{\mathbb{K}^n}(I_{\hat{a}} \cap \mathbb{K}[x_i]) = \{0\} \). Since \( I_{\hat{a}} \cap \mathbb{K}[x_i] \) is homogeneous, the polynomial \( q(x_i) \) must be necessarily homogeneous, whence \( q(x_i) = x_i^{\mu_i}, i = 1, \ldots, n \). If \( I_{\hat{a}} \cap \mathbb{K}[x_i] = \langle \emptyset \rangle \), then \( V_{\mathbb{K}^n}(I_{\hat{a}}) \) is not finite, whereas if \( I_{\hat{a}} \cap \mathbb{K}[x_i] = \langle x_i^{\mu_i} \rangle, \mu_i \geq 1 \), then \( x_i \in V_{\mathbb{K}^n}(I_{\hat{a}}) \) implies \( x_i = 0 \), for \( i = 1, \ldots, n \).

Proof of (8.3). By assumption, \( \mathcal{I} \cap \mathbb{K}[a] = \langle \emptyset \rangle \), whence

\[
\mathcal{I} \cap \mathbb{K}[a, x_i] = \langle q_{i,1}(a)x_i^{\mu_{i,1}}, \ldots, q_{i,M_i}(a)x_i^{\mu_{i,M_i}} \rangle,
\]

where at least one of the polynomials \( q_{i,j}(a) \) is not zero at the specialization \( a = \hat{a}^\circ \), because otherwise \( V_{\mathbb{K}^n}(I_{\hat{a}^\circ}) \) would not be finite. Hence, \( V_{\mathbb{K}^n}(I_{\hat{a}} \cap \mathbb{K}[x_i]) \) is finite, for all \( \hat{a} \) that do not belong to the variety of the ideal \( \langle q_{i,1}, \ldots, q_{i,M_i} \rangle \) of \( \mathbb{K}[a] \), i.e., for “almost all” \( \hat{a} \in \mathbb{K}^\ell \). The finiteness of \( V_{\mathbb{K}^n}(I_{\hat{a}} \cap \mathbb{K}[x_i]) \cap \cdots \cap V_{\mathbb{K}^n}(I_{\hat{a}} \cap \mathbb{K}[x_n]) \) implies the finiteness of \( V_{\mathbb{K}^n}(I_{\hat{a}}) \), because \( V_{\mathbb{K}^n}(I_{\hat{a}}) = \bigcup V_{\mathbb{K}^n}(I_{\hat{a}} \cap \mathbb{K}[x]) \subseteq V_{\mathbb{K}^n}(I_{\hat{a}} \cap \mathbb{K}[x_1] \cup \cdots \cup \mathbb{K}[x_n]) \subseteq V_{\mathbb{K}^n}(I_{\hat{a}} \cap \mathbb{K}[x_1]) \cap \cdots \cap V_{\mathbb{K}^n}(I_{\hat{a}} \cap \mathbb{K}[x_n]). \)

Proof. (of Lemma 9) Proof of (9.1). Let \( \mathcal{I} = \{ \frac{\partial p}{\partial x} \} \) and, for any \( i = 1, \ldots, n \), let \( G_{\mathcal{I}} \) be the rGb of \( \mathcal{I} \), w.r.t. the GRL order \( \triangleright_G \), with \( a_1 \triangleright_G \cdots \triangleright_G a_\ell \triangleright_G x_j \triangleright_G x_i, \forall j \neq i \). Clearly, the quotient ring \( \mathbb{K}[a, x]/\mathcal{I} \) is not finite dimensional; let \( B \) be its monomial basis, w.r.t. the above monomial order. Now, since \( B \) is the set of all monomials \( a^{\beta}x^\gamma \notin \langle LT(\mathcal{I}) \rangle \), but \( LT(\mathcal{I}) \) is finitely generated, there exists \( \mu_i \in \mathbb{Z}_{\geq 1} \) such that \( a^\beta x_i^{\mu_i} \in LT(\mathcal{I}) \), because \( V_{\mathbb{K}^n}(I_{\hat{a}}) = \{0\} \), for \( \hat{a} = \hat{a}^\circ \). Therefore, for each \( i = 1, \ldots, n \), there exists an element of \( G_{\mathcal{I}} \) of the form \( q_i(a)x_i^{\mu_i} \), where \( q_i \in \mathbb{K}[a] \). Fix any \( \hat{a} \notin V_{\mathbb{K}^n}(\langle q_1, \ldots, q_n \rangle) \); for the GRL order \( \triangleright_G \) in \( \mathbb{K}[x_1, \ldots, x_n] \), with \( x_j \triangleright_G x_i, \forall j \neq i \), is used for the computation of the rGb \( G_{\mathcal{I}_{\hat{a}}} \) of \( I_{\hat{a}} \), then one has \( x_i^{\mu_i} \in G_{\mathcal{I}_{\hat{a}}} \), with \( \mu_i \in \mathbb{Z}_{\geq 1} \), which proves (by Lemma 7) that \( V_{\mathbb{K}^n}(I_{\hat{a}}) = \{0\} \) and that \( \langle \frac{\partial p}{\partial x} \rangle \) is primary, for “almost all” \( \hat{a} \in \mathbb{K}^\ell \).

The proof of (9.2) follows from (9.1).

Proof. (of Lemma 10) By Lemma 5, for “almost all” \( p \in \Sigma_{\mathbb{K}2d,m}[x] \), one has \( p \in \Sigma_{\mathbb{K}2d,m}[x] \). Letting \( h = [h_1 \ldots h_m]^\top \in \mathbb{K}^m[x]_{=d} \), one can write \( p = h^\top Wh \), where \( W = \text{diag}(w_1, \ldots, w_m) \), \( \text{det}(W) \neq 0 \). By (2), each form \( h_i \in \mathbb{K}[x]_{=d} \), \( i = 1, \ldots, m \), can be taken as a specialization \( \Phi_n,d(\hat{a}^\circ, x) \) of \( \Phi_n,d(a^\circ, x) \). Hence, each form \( p \in \Sigma_{\mathbb{K}2d,m}[x] \) can be taken as a specialization \( p(\hat{a}^\circ, x) \) of \( p(a^\circ, x) = \sum_{i=1}^m w_i \Phi_n,d(a^\circ, x), \) where \( a^\circ := [(a^1)^\top \cdots (a^m)^\top] w_1 \cdots w_m \). Consider the ideals \( \langle \frac{\partial p(a^\circ, x)}{\partial x} \rangle \) and \( \langle h^\top (a^\circ, x) \rangle \) of \( \mathbb{K}[a^\circ, x] \), where

\[
\hat{h}(a^\circ, x) := [\Phi_n,d(a^1, x) \ldots \Phi_n,d(a^m, x)]^\top.
\]

Since these two ideals are homogeneous for “almost all” specializations \( a^\circ \in \mathbb{K}(\ell_{n,d+1}) \), the quotient ideal \( \langle \frac{\partial p(a^\circ, x)}{\partial x} \rangle \) is homogeneous for “almost all” specializations \( a^\circ \in \mathbb{K}(\ell_{n,d+1}) \). Consider the specialization \( \hat{a}^\circ \in \mathbb{K}(\ell_{n,d+1}) \) such that \( \Phi_n,d(\hat{a}^\circ, x) = \sum_{j=1}^n x_j^{\hat{d}_j} \), and \( \hat{w}_i = 1, i = 1, \ldots, m \). It can be easily verified that, for such
a specialization, the ideal \( ((\partial p(\hat{a}_{w,e})/\partial x) : (h^T(\hat{a}_{w,e}, x))) \) equals \( \langle x_1^{d-1}, \ldots, x_n^{d-1} \rangle \), and hence \( V_{\mathbb{K}^n}(\langle \partial p(\hat{a}_{w,e})/\partial x \rangle : \langle h^T(\hat{a}_{w,e}, x) \rangle) = \{0\} \). Therefore, by Lemma (8.3), the variety
\[
V_{\mathbb{K}^n}(\langle \partial p(\hat{a}_{w,e})/\partial x \rangle : \langle h^T(\hat{a}_{w,e}, x) \rangle)
\]
is finite for “almost all” \( a_{w,e} \in \mathbb{K}^{(\ell_n + 1)m} \) and hence for “almost all” \( p \in \Sigma_{2d,m}^\mathbb{K}[x] \). Hence, by (8.2) of Lemma 8, there exists \( N \in \mathbb{Z}_{\geq 1} \) such that \( x_n^N \in \langle \langle \partial p(\hat{a}_{w,e})/\partial x \rangle : \langle h^T(\hat{a}_{w,e}, x) \rangle \rangle \), for “almost all” \( a_{w,e} \in \mathbb{K}^{(\ell_n + 1)m} \), and hence \( x_n^N \in \langle \langle \partial p/\partial x \rangle : \langle h^T \rangle \rangle \), for “almost all” \( p \in \Sigma_{2d,m}^\mathbb{K}[x] \). This implies \( x_n^N h_i \in \langle \frac{\partial p}{\partial y} \rangle, \ i = 1, \ldots, m \). Therefore, for “almost all” \( p \in \Sigma_{2d,m}^\mathbb{K}[x] \), one has \( \langle h^T \rangle \subseteq \langle \langle \partial p/\partial x \rangle : \langle x_n^N \rangle \rangle = \langle \langle \frac{\partial p}{\partial x} \rangle : \langle x_n^\infty \rangle \rangle \).

**Proof.** (of Lemma 11) Consider \( Q = \langle \Phi_{n,d}(a^1, x), \ldots, \Phi_{n,d}(a^m, x), 1 - y x_n \rangle \) of \( \mathbb{K}[a_e, x, y] \), where \( y \) is an auxiliary variable.

(F.1) If \( Q \cap \mathbb{K}[a_e] \neq \langle 0 \rangle \), then \( x_n \in \sqrt{J_{a_e}}, \forall \hat{a}_e \notin V(\mathbb{Q} \cap \mathbb{K}[a_e]) \), whence for “almost all” \( \hat{a}_e \in \mathbb{K}^{m_{\ell_n,d}} \).

(F.2) If \( Q \cap \mathbb{K}[a_e] = \langle 0 \rangle \), then \( x_n \notin \sqrt{J_{a_e}} \) for “almost all” \( \hat{a}_e \in \mathbb{K}^{m_{\ell_n,d}} \).

To prove (F.1), note that, for any specialization \( \hat{a}_e \notin V(\mathbb{Q} \cap \mathbb{K}[a_e]) \), one has \( \mathbb{Q}_{\hat{a}_e} = \langle 1 \rangle \), and therefore Theorem 1 implies \( x_n \in \sqrt{J_{a_e}} \). The condition \( \mathbb{Q} \cap \mathbb{K}[a_e] \neq \langle 0 \rangle \) implies that the variety \( V(\mathbb{Q} \cap \mathbb{K}[a_e]) \) of \( \mathbb{K}^{m_{\ell_n,d}} \) does not coincide with the whole \( \mathbb{K}^{m_{\ell_n,d}} \). To prove (F.2), let \( S \subseteq \mathbb{K}^\ell \) be the set of all specializations \( \hat{a}_e \) such that \( \mathbb{Q}_{\hat{a}_e} = \langle 1 \rangle \); its Zariski closure \( \overline{S} \) cannot coincide with the whole \( \mathbb{K}^{m_{\ell_n,d}} \), because \( \mathbb{Q} \cap \mathbb{K}[a_e] = \langle 0 \rangle \), whence \( x_n \notin \sqrt{J_{a_e}} \), for all \( \hat{a}_e \in \mathbb{K}^{m_{\ell_n,d}} \setminus \overline{S} \), where \( \mathbb{K}^{m_{\ell_n,d}} \setminus \overline{S} \) is Zariski open.

Proof of (11.1). If \( m = n \), then \( Q \cap \mathbb{K}[a_e] \) is a principal ideal; it is generated by one polynomial \( q(a_e) \) (i.e., \( Q \cap \mathbb{K}[a_e] = \langle q(a_e) \rangle \)), which is the resultant
\[
\text{Res}(\Phi_{n,d}(a^1, x), \ldots, \Phi_{n,d}(a^n, x))
\]
of the \( n \) polynomials \( \Phi_{n,d}(a^1, x), \ldots, \Phi_{n,d}(a^n, x) \), w.r.t. \( x \) (see [3, Ch 3, § 2]). By Theorem 2.3 of [3, pag 86], such a resultant vanishes if and only if the system of the \( n \) equations \( \Phi_{n,d}(a^1, x) = 0, \ldots, \Phi_{n,d}(a^n, x) = 0 \) has a non-zero solution in \( x \) over the algebraic closure \( \overline{\mathbb{K}} \), and is a non-zero polynomial in the coefficients \( a^1, \ldots, a^n \). Hence, if \( q(\hat{a}_e) \neq 0 \), then the system \( \Phi_{n,d}(\hat{a}^1, x) = 0, \ldots, \Phi_{n,d}(\hat{a}^n, x) = 0 \) admits only the trivial solution \( x = 0 \), i.e., \( V(\mathcal{J}_{\hat{a}_e}) = \{0\} \) and hence \( V(\mathbb{Q}_{\hat{a}_e}) = \emptyset \). This means that \( \mathcal{J}_{\hat{a}_e} = \langle 1 \rangle \), for all \( \hat{a}_e \) such that \( q(\hat{a}_e) \neq 0 \). Therefore, \( Q \cap \mathbb{K}[a_e] \neq \langle 0 \rangle \), whence (F.1) implies that \( x_n \in \sqrt{J_{a_e}} \), for “almost all” \( \hat{a}_e \in \mathbb{K}^{m_{\ell_n,d}} \).

If \( n \leq m \), then the resultant of the first \( n \) polynomials (as well as of any other \( n \)-plet of such polynomials), \( \text{Res}(\Phi_{n,d}(a^1, x), \ldots, \Phi_{n,d}(a^n, x)) \), belongs to \( Q \cap \mathbb{K}[a_e] \), whence \( Q \cap \mathbb{K}[a_e] \neq \langle 0 \rangle \); (F.1) implies that \( x_n \in \sqrt{J_{a_e}} \), for “almost all” \( \hat{a}_e \in \mathbb{K}^{m_{\ell_n,d}} \).

Proof of (11.2). If \( n > m \), then the resultant of the set of \( n \) polynomials obtained from \( \{\Phi_{n,d}(a^1, x), \ldots, \Phi_{n,d}(a^m, x)\} \) by adding \( n - m \) zero polynomials, is the zero polynomial, whence \( Q \cap \mathbb{K}[a_e] \) is the zero ideal \( \langle 0 \rangle \); hence, (F.2) implies that \( x_n \notin \sqrt{J_{a_e}} \), for “almost all” \( \hat{a}_e \in \mathbb{K}^{m_{\ell_n,d}} \).

**Proof.** (of Lemma 12) If \( n \leq m \), then \( \sqrt{J} \) is “generically” maximal, since \( \sqrt{J} = \langle x_1, \ldots, x_n \rangle \) “generically”, thus proving the lemma in the case \( n \leq m \). Let \( n > m \).
For any $\hat{a}_e \in \mathbb{K}^{m_{\ell,n,d}}$, let $\hat{h}_i(x^1, x^2) = \Phi_{n,d}(\hat{a}_1, x), \ldots, \hat{h}_m(x^1, x^2) = \Phi_{n,d}(\hat{a}_m, x)$, where $x = [(x^1)^\top (x^2)^\top]^\top, x^1 = [x_1 \ldots x_m]^\top$ and $x^2 = [x_{m+1} \ldots x_n]^\top$. For “almost all” $\hat{a}_e \in \mathbb{K}^{m_{\ell,n,d}}$, apart from a reordering of the entries of $x$, $\{x_1, \ldots, x_m\}$ constitute a maximal independent set w.r.t. $J_{\hat{a}_e} = \{h_1, \ldots, h_m\}$, i.e., $J_{\hat{a}_e} \cap \mathbb{K}[x_1, \ldots, x_{m-1}, x_m] = \emptyset$ and $J_{\hat{a}_e} \cap \mathbb{K}[x_1, \ldots, x_{m-1}] \neq \emptyset$. Let $J_{\hat{a}_e} = \{g_1, \ldots, g_s\}$ be the rGb of $J_{\hat{a}_e}$, w.r.t. the Lex order with $x_i > 1, x_j, i \in \{1, \ldots, m\}$ and $j \in \{m+1, \ldots, n\}$. Coerce the polynomials $g_i$ into $\mathbb{K}[x^2][x^1]$ and compute $k_{g_1,\ldots,g_s} = \sum_{i=1}^s \text{LC}(g_i)$, which belongs to $\mathbb{K}[x^2]$. Now, coercing $k_{g_1,\ldots,g_s}$ into $\mathbb{K}[x]$, consider the saturation ($J_{\hat{a}_e} : \langle k_{g_1,\ldots,g_s} \rangle$). By [4], $J_{\hat{a}_e}$ is primary if and only if $(J_{\hat{a}_e} : \langle k_{g_1,\ldots,g_s} \rangle) = J_{\hat{a}_e}$. Clearly, if $(J_{\hat{a}_e} : \langle k_{g_1,\ldots,g_s} \rangle) = J_{\hat{a}_e}$ for some specialization $\hat{a}_e$, then $(J_{\hat{a}_e} : \langle k_{g_1,\ldots,g_s} \rangle) = J_{\hat{a}_e}$, for “almost all” specializations $\hat{a}_e$. To complete the proof, it is enough to find one of such $\hat{a}_e$. Take $\hat{h}_i = (x_1 + x_{m+1} + \ldots + x_n)^d, \ldots, \hat{h}_m = (x_1 + x_{m+1} + \ldots + x_n)^d$, the lemma is proven by (1.3) of Lemma 1.

**Proof.** (of Lemma 13) First, take $n = m$ and let $h(a_e, x) = [h_1(a_1, x) \ldots h_n(a^n, x)]^\top$, where $a_e = [(a^1)^\top \ldots (a^n)^\top]^\top$. For any specialization $\hat{a}_e \in \mathbb{K}^{m_{\ell,n,d}}$ of $a_e$, let $h$ be the corresponding specialization of $h$. As well known [5], the $n$ polynomials $\hat{h}_i$ in the $n$ unknowns $x$ are algebraically independent if and only if $\text{det}(\frac{\partial h}{\partial x}) = 0$ in $\mathbb{K}[a_e, x]$ and can be rewritten as $\text{det}(\frac{\partial h}{\partial x}) = q_1(a_e)x^{\alpha_1} + q_2(a_e)x^{\alpha_2} + \ldots$, where $q_i(a_e), i = 1, 2, \ldots$, are non-zero polynomials and the $\alpha^i$s are multi-indices of the same length $|\alpha^i| = |\alpha^j|$. Let $Q = \langle q_1(a_e), q_2(a_e), \ldots \rangle$ be an ideal of $\mathbb{K}[a_e]$; $\text{det}(\frac{\partial h}{\partial x}) = 0$ in $\mathbb{K}[x]$ if and only if $\hat{a}_e \in \mathbb{V}(Q)$, thus proving the theorem, since $\mathbb{V}(Q) \neq \mathbb{K}^{m_{\ell,n,d}}$. Similarly, for $n > m$.

**Proof.** (of Lemma 14) By the proof of Theorem 5, each $p \in \Sigma_{2d,m}^\mathbb{K}[x]$ can be taken as a specialization $p_{a_e^*}(x) = p(a_e^*, x)$ of $p(a_e^*, x) = \sum_{i=1}^{m^*} w_i h_i^2(a_i, x)$, where $a_e^* = [(a^1)^\top \ldots (a^n)^\top w_1 \ldots w_{m^*}]^\top$, and, for “almost all” $a_e^* \in \mathbb{K}^{(\ell_0 + 1)d}m^*$, the variety $\mathbb{V}(\Sigma_{2d,m}^\mathbb{K})(\frac{\partial p(a_e^*, x)}{\partial x} : \langle h^\top(a_e^*, x) \rangle)$ is finite. This implies the existence of $q \in \mathbb{K}[a_e^*]$ such that $q(a_e^*)x_n^{m^*} \in \Sigma_{2d,m}^\mathbb{K}(\frac{\partial p(a_e^*, x)}{\partial x} : \langle h^\top(a_e^*, x) \rangle) \cap \mathbb{K}[a_e^*, x_n]$. Hence, for each $\hat{a}_e^* \in \mathbb{K}^{(\ell_0 + 1)d^*}$ such that $q(\hat{a}_e^*) \neq 0$, one has $(\frac{\partial p(\hat{a}_e^*, x)}{\partial x} : \langle x_n^{m^*} \rangle) = (h^\top)$.

**References**


