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 $p \in \widetilde{\Sigma}^{\mathbb{K}}_{2d,m}[x]$ 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 $\mathbb{K}[x]$. 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 $p \in \widetilde{\Sigma}^{\mathbb{K}}_{2d,m}[x]$. The case $w_i = 0$ is trivial. □

Proof. (of Lemma 5) Proof of (5.1). The proof is trivial if $m = 1$. Let $m \geq 2$. Let $m^* \in \mathbb{Z}$ be such that $m \geq m^* \geq 1$ and $\widetilde{\Sigma}^{\mathbb{K}}_{2d,m^*}[x] \neq \emptyset$. Since $\widetilde{\Sigma}^{\mathbb{K}}_{2d,m^*}[x] \cup \Sigma^{\mathbb{K}}_{2d,m^*-1}[x] = \Sigma^{\mathbb{K}}_{2d,m}[x]$ and $\widetilde{\Sigma}^{\mathbb{K}}_{2d,m^*}[x] \cap \Sigma^{\mathbb{K}}_{2d,m^*-1}[x] = \emptyset$, one has $S_m^{-1}(\widetilde{\Sigma}^{\mathbb{K}}_{2d,m^*}[x]) \cap S_m^{-1}(\Sigma^{\mathbb{K}}_{2d,m^*-1}[x]) = \emptyset$ and $S_m^{-1}(\widetilde{\Sigma}^{\mathbb{K}}_{2d,m^*}[x]) \cup S_m^{-1}(\Sigma^{\mathbb{K}}_{2d,m^*-1}[x]) = S_m^{-1}(\Sigma^{\mathbb{K}}_{2d,m}[x])$. Since $\widetilde{\Sigma}^{\mathbb{K}}_{2d,m^*}[x] \neq \emptyset$, $x_1^{2d} \in \Sigma^{\mathbb{K}}_{2d,m}[x]$ for $m \geq 1$, and $x_1^{2d} \notin \widetilde{\Sigma}^{\mathbb{K}}_{2d,m^*}[x]$ for $m^* > 1$, one has that $S_m^{-1}(\widetilde{\Sigma}^{\mathbb{K}}_{2d,m^*}[x])$ is a proper subset of $S_m^{-1}(\Sigma^{\mathbb{K}}_{2d,m}[x])$. By Lemma 4, set $\Sigma^{\mathbb{K}}_{2d,m^*-1}[x]$ 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 $S_m^{-1}(\Sigma^{\mathbb{K}}_{2d,m^*-1}[x])$ is a proper variety of $S_m^{-1}(\Sigma^{\mathbb{K}}_{2d,m}[x])$. This implies that $S_m^{-1}(\widetilde{\Sigma}^{\mathbb{K}}_{2d,m^*}[x])$ is Zariski open.
Proof of (5.2). By (5.1), there are only two cases: either $\widetilde{\Sigma}^{\mathbb{K}}_{2d,m}[x] = \emptyset$ or $S_m^{-1}(\widetilde{\Sigma}^{\mathbb{K}}_{2d,m}[x])$ is a Zariski open of $S_m^{-1}(\Sigma^{\mathbb{K}}_{2d,m}[x])$. 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

$\widetilde{\Sigma}^{\mathbb{K}}_{2d,m}[x] \neq \emptyset$. Since $n \geq m$, $p = x_1^{2d} + \ldots + x_m^{2d}$ is a sum of m squares that cannot be expressed as a wSOS with a smaller number of squares [2, pag 20] (*i.e.*, $p \in \Sigma^{\mathbb{K}}_{2d,m}[x]$, $p \notin \Sigma^{\mathbb{K}}_{2d,m-1}[x]$), which implies $p \in \widetilde{\Sigma}^{\mathbb{K}}_{2d,m}[x]$. □

Proof. (of Lemma 6) Let $H(\tilde{B}) \in \mathbb{K}^{\ell_{m,2} \times \ell_{n,2d}}$ be such that $M^{\tilde{h}}_{=2} = H(\tilde{B}) M^{x}_{=2d}$, where $M^{\tilde{h}}_{=2} := [\tilde{h}_1^2\ \tilde{h}_1\tilde{h}_2\ \ldots\ \tilde{h}_m^2]^\top$.
(P.1) For $n \geq m \geq 2$ and for all $d \in \mathbb{Z}_{\geq 2}$, polynomials $\tilde{h}_1^2, \tilde{h}_1\tilde{h}_2, \tilde{h}_2^2, \ldots, \tilde{h}_1\tilde{h}_m, \ldots, \tilde{h}_m^2$ 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 $\tilde{B}^o \in \mathbb{K}^{\ell_{m,2} \times \ell_{n,2d}} \subseteq \mathbb{R}^{\ell_{m,2} \times \ell_{n,2d}}$, then there exists an open neighborhood $\mathcal{B} \subseteq \mathbb{R}^{\ell_{m,2} \times \ell_{n,2d}}$ of $\tilde{B}^o$ such that $H(\tilde{B})$ has full row rank for all $\tilde{B} \in \mathcal{B}$. Let $\mathcal{S} \subseteq \mathbb{K}^{\ell_{m,2} \times \ell_{n,2d}}$ be the set of all $\tilde{B} \in \mathbb{K}^{\ell_{m,2} \times \ell_{n,2d}}$ such that $H(\tilde{B})$ has not full row rank. The Zariski closure $\overline{\mathcal{S}}$ of $\mathcal{S}$ does not coincide with $\mathbb{K}^{\ell_{m,2} \times \ell_{n,2d}}$, because, in that case, for any open neighborhood $\mathcal{B} \subseteq \mathbb{R}^{\ell_{m,2} \times \ell_{n,2d}}$ of $\tilde{B}^o$, there would exist $\tilde{B}^\star \in \mathcal{B}$ such that $H(\tilde{B}^\star)$ has not full row rank, being $\mathbb{K}$ dense in $\mathbb{R}$. Hence, if $H(\tilde{B}^o)$ has full row rank for some $\tilde{B}^o \in \mathbb{K}^{\ell_{m,2} \times \ell_{n,2d}}$, then it has full row rank for "almost all" $\tilde{B} \in \mathbb{K}^{\ell_{m,2} \times \ell_{n,2d}}$.
(P.3) For $n \geq m \geq 2$, $\forall d \in \mathbb{Z}_{\geq 2}$, 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 $(\tilde{h}_1^o)^2, \tilde{h}_1^o\tilde{h}_2^o, (\tilde{h}_2^o)^2, \ldots, \tilde{h}_1^o\tilde{h}_m^o, \ldots, (\tilde{h}_m^o)^2$ are linearly independent over $\mathbb{K}$, then $\tilde{h}_1^2, \tilde{h}_1\tilde{h}_2, \tilde{h}_2^2, \ldots, \tilde{h}_1\tilde{h}_m, \ldots, \tilde{h}_m^2$ 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 $n = m$, $\tilde{h}_i = x_1^{d-1} x_i$, $i = 1, \ldots, n$. 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 $>_{\mathrm{G}}$ on $\mathbb{K}[x]$, with $x_1 >_{\mathrm{G}} x_2 >_{\mathrm{G}} \ldots >_{\mathrm{G}} x_n$ and let $p \in \mathbb{K}[x]_{=d}$. First, it is proved that if $\mathrm{LM}(p) = x_n^d$, 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 $\mathrm{LM}(p) = x_n^d$ and, by absurd, that p contains a monomial $x^\beta = x_1^{\beta_1} \cdots x_n^{\beta_n}$, $\sum_{i=1}^n \beta_i = d$, different from x_n^d. This yields a contradiction, because if $x_1^{\beta_1} \cdots x_n^{\beta_n} \neq x_n^d$, $\sum_{i=1}^n \beta_i = d$, then $x_1^{\beta_1} \cdots x_n^{\beta_n} >_{\mathrm{G}} x_n^d$, whence x_n^d is not the leading monomial of p. Therefore, the proof of (7.1) follows from Theorem 4. Moreover, if $x_i^{\mu_i} \in \mathcal{I}$, then $x_i \in \sqrt{\mathcal{I}}$, $i = 1, \ldots, n$, 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 $0 \in \mathbf{V}_{\overline{\mathbb{K}}^n}(\mathcal{I}_{\hat{a}})$. Now, assume that there exists a point $\tilde{x} \in \mathbb{K}^n$, $\tilde{x} \neq 0$, belonging to $\mathbf{V}_{\overline{\mathbb{K}}^n}(\mathcal{I}_{\hat{a}})$; this implies that $p_i(\hat{a}, \tilde{x}) = 0$, $i = 1, \ldots, m$. Therefore, taking into account the homogeneity, by letting $x = \theta\tilde{x}$, $\theta \in \mathbb{K}$, one has $p_i(\hat{a}, \theta\tilde{x}) = \theta p_i(\hat{a}, \tilde{x}) = 0$, $i = 1, \ldots, m$, which shows that all the points belonging to the line parameterized by $x = \theta\tilde{x}$ belong to $\mathbf{V}_{\overline{\mathbb{K}}^n}(\mathcal{I}_{\hat{a}})$, which, therefore, is not finite.

Proof of (8.2). Let $\hat{a} \in \mathbb{K}^\ell$ be such that the variety $\mathbf{V}_{\overline{\mathbb{K}}^n}(\mathcal{I}_{\hat{a}})$ of $\overline{\mathbb{K}}^n$ is finite. By (8.1), one has $\mathbf{V}_{\mathbb{K}^n}(\mathcal{I}_{\hat{a}}) = \{0\}$, whence $\mathbf{V}_{\overline{\mathbb{K}}}(\mathcal{I}_{\hat{a}} \cap \mathbb{K}[x_i]) = \{0\}$; $\mathcal{I}_{\hat{a}} \cap \mathbb{K}[x_i]$ is a principal ideal, which is therefore generated by one monic polynomial $q(x_i)$ in x_i, which satisfies $q(0) = 0$, because $\mathbf{V}_{\overline{\mathbb{K}}}(\mathcal{I}_{\hat{a}} \cap \mathbb{K}[x_i]) = \{0\}$. Since $\mathcal{I}_{\hat{a}} \cap \mathbb{K}[x_i]$ is homogeneous, the polynomial $q(x_i)$ must be necessarily homogeneous, whence $q(x_i) = x_i^{\mu_i}$, $i = 1, \ldots, n$. If $\mathcal{I}_{\hat{a}} \cap \mathbb{K}[x_i] = \langle \emptyset \rangle$, then $\mathbf{V}_{\mathbb{K}^n}(\mathcal{I}_{\hat{a}})$ is not finite, whereas if $\mathcal{I}_{\hat{a}} \cap \mathbb{K}[x_i] = \langle x_i^{\mu_i} \rangle, \mu_i \geq 1$, then $x \in \mathbf{V}_{\mathbb{K}^n}(\mathcal{I}_{\hat{a}})$ 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 $a = \hat{a}^o$, because otherwise $\mathbf{V}_{\overline{\mathbb{K}}^n}(\mathcal{I}_{\hat{a}^o})$ would not be finite. Hence, $\mathbf{V}_{\overline{\mathbb{K}}}(\mathcal{I}_{\hat{a}} \cap \mathbb{K}[x_i])$ 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 $\mathbf{V}_{\overline{\mathbb{K}}}(\mathcal{I}_{\hat{a}} \cap \mathbb{K}[x_1]) \cap \ldots \cap \mathbf{V}_{\overline{\mathbb{K}}}(\mathcal{I}_{\hat{a}} \cap \mathbb{K}[x_n])$ implies the finiteness of $\mathbf{V}_{\mathbb{K}^n}(\mathcal{I}_{\hat{a}})$, because $\mathbf{V}_{\mathbb{K}^n}(\mathcal{I}_{\hat{a}}) = \mathbf{V}_{\mathbb{K}^n}(\mathcal{I}_{\hat{a}} \cap \mathbb{K}[x]) \subseteq \mathbf{V}_{\mathbb{K}^n}(\mathcal{I}_{\hat{a}} \cap (\mathbb{K}[x_1] \cup \ldots \cup \mathbb{K}[x_n])) \subseteq \mathbf{V}_{\mathbb{K}^n}((\mathcal{I}_{\hat{a}} \cap \mathbb{K}[x_1]) \cup \ldots \cup (\mathcal{I}_{\hat{a}} \cap \mathbb{K}[x_n])) \subseteq \mathbf{V}_{\mathbb{K}^n}(\mathcal{I}_{\hat{a}} \cap \mathbb{K}[x_1]) \cap \ldots \cap \mathbf{V}_{\mathbb{K}^n}(\mathcal{I}_{\hat{a}} \cap \mathbb{K}[x_n])$. □

Proof. (of Lemma 9) Proof of (9.1). Let $\mathcal{I} = \langle \frac{\partial p}{\partial x} \rangle$ and, for any $i \in \{1, \ldots, n\}$, let $\mathcal{G}_{\mathcal{I}}$ be the rGb of $\mathcal{I}$, w.r.t. the GRL order $>_{\mathrm{G}}$, with $a_1 >_{\mathrm{G}} \ldots >_{\mathrm{G}} a_\ell >_{\mathrm{G}} x_j >_{\mathrm{G}} x_i$, $\forall j \neq i$. Clearly, the quotient ring $\mathbb{K}[a, x]/\mathcal{I}$ is not finite dimensional; let $\mathcal{B}$ be its monomial basis, w.r.t. the above monomial order. Now, since $\mathcal{B}$ is the set of all monomials $a^\beta x^\gamma \notin \langle \mathrm{LT}(\mathcal{I}) \rangle$, but $\langle \mathrm{LT}(\mathcal{I}) \rangle$ is finitely generated, there exists $\mu_i \in \mathbb{Z}_{\geq 1}$ such that $a^\beta x_i^{\mu_i} \in \mathrm{LT}(\mathcal{I})$, because $\mathbf{V}_{\mathbb{K}^n}(\mathcal{I}_{\hat{a}}) = \{0\}$, for $\hat{a} = \hat{a}^o$. Therefore, for each $i = 1, \ldots, n$, there exists an element of $\mathcal{G}_{\mathcal{I}}$ of the form $q_i(a) x_i^{\mu_i}$, where $q_i \in \mathbb{K}[a]$. Fix any $\hat{a} \notin \mathbf{V}_{\mathbb{K}^\ell}(\langle q_1, \ldots, q_n \rangle)$; for each $i \in \{1, \ldots, n\}$, if the GRL order $>_{\mathrm{G}}$ in $\mathbb{K}[x_1, \ldots, x_n]$, with $x_j >_{\mathrm{G}} x_i$, $\forall j \neq i$, is used for the computation of the rGb $\mathcal{G}_{\mathcal{I}_{\hat{a}}}$ of $\mathcal{I}_{\hat{a}}$, then one has $x_i^{\mu_i} \in \mathcal{G}_{\mathcal{I}_{\hat{a}}}$, with $\mu_i \in \mathbb{Z}_{\geq 1}$, which proves (by Lemma 7) that $\mathbf{V}_{\mathbb{K}^n}(\mathcal{I}_{\hat{a}}) = \{0\}$ and that $\langle \frac{\partial p_{\hat{a}}}{\partial x} \rangle$ 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 $p \in \widetilde{\Sigma}^{\mathbb{K}}_{2d,m}[x]$. Letting $h = [h_1 \ \ldots \ h_m]^\top \in \mathbb{K}^m[x]_{=d}$, one can write $p = h^\top W h$, where $W = \mathrm{diag}(w_1, \ldots, w_m)$, $\det(W) \neq 0$. By (2), each form $h_i \in \mathbb{K}[x]_{=d}$, $i = 1, \ldots, m$, can be taken as a specialization $\Phi_{n,d}(\hat{a}^i, x)$ of $\Phi_{n,d}(a^i, x)$. Hence, each form $p \in \Sigma^{\mathbb{K}}_{2d,m}[x]$ can be taken as a specialization $p(\hat{a}_{w,e}, x)$ of $p(a_{w,e}, x) = \sum_{i=1}^m w_i \Phi^2_{n,d}(a^i, x)$, where $a_{w,e} := [(a^1)^\top \ \ldots \ (a^m)^\top \ w_1 \ \ldots \ w_m]^\top$. Consider the ideals $\langle \frac{\partial p(a_{w,e}, x)}{\partial x} \rangle$ and $\langle h^\top(a_{w,e}, x) \rangle$ of $\mathbb{K}[a_{w,e}, x]$, where

$$h(a_{w,e}, x) := [\Phi_{n,d}(a^1, x) \ \ldots \ \Phi_{n,d}(a^m, x)]^\top.$$

Since these two ideals are homogeneous for "almost all" specializations $a_{w,e} \in \mathbb{K}^{(\ell_{n,d}+1)m}$, the quotient ideal $(\langle \frac{\partial p(a_{w,e}, x)}{\partial x} \rangle : \langle h^\top(a_{w,e}, x) \rangle)$ is homogeneous for "almost all" specializations $a_{w,e} \in \mathbb{K}^{(\ell_{n,d}+1)m}$. Consider the specialization $\hat{a}_{w,e} \in \mathbb{K}^{(\ell_{n,d}+1)m}$ such that $\Phi_{n,d}(\hat{a}^i, x) = \sum_{j=1}^n x_j^d$, and $\hat{w}_i = 1$, $i = 1, \ldots, m$. It can be easily verified that, for such

a specialization, the ideal $(\langle\frac{\partial p(\hat{a}_{w,e},x)}{\partial x}\rangle : \langle h^\top(\hat{a}_{w,e},x)\rangle)$ equals $\langle x_1^{d-1},\ldots,x_n^{d-1}\rangle$, and hence $\mathbf{V}_{\overline{\mathbb{K}}^n}(\langle\frac{\partial p(\hat{a}_{w,e},x)}{\partial x}\rangle : \langle h^\top(\hat{a}_{w,e},x)\rangle) = \{0\}$. Therefore, by Lemma (8.3), the variety

$$\mathbf{V}_{\overline{\mathbb{K}}^n}(\langle\frac{\partial p(a_{w,e},x)}{\partial x}\rangle : \langle h^\top(a_{w,e},x)\rangle)$$

is finite for "almost all" $a_{w,e} \in \mathbb{K}^{(\ell_{n,d}+1)m}$ and hence for "almost all" $p \in \Sigma^{\mathbb{K}}_{2d,m}[x]$. Hence, by (8.2) of Lemma 8, there exists $N \in \mathbb{Z}_{\geq 1}$ such that $x_n^N \in (\langle\frac{\partial p(\hat{a}_{w,e},x)}{\partial x}\rangle : \langle h^\top(\hat{a}_{w,e},x)\rangle)$, for "almost all" $a_{w,e} \in \mathbb{K}^{(\ell_{n,d}+1)m}$, and hence $x_n^N \in (\langle\frac{\partial p}{\partial x}\rangle : \langle h^\top\rangle)$, for "almost all" $p \in \Sigma^{\mathbb{K}}_{2d,m}[x]$. This implies $x_n^N h_i \in \langle\frac{\partial p}{\partial x}\rangle$, $i = 1,\ldots,m$. Therefore, for "almost all" $p \in \Sigma^{\mathbb{K}}_{2d,m}[x]$, one has $\langle h^\top\rangle \subseteq (\langle\frac{\partial p}{\partial x}\rangle : \langle x_n^N\rangle) = (\langle\frac{\partial p}{\partial x}\rangle : \langle x_n^\infty\rangle)$. □

Proof. (of Lemma 11) Consider $\mathcal{Q} = \langle \Phi_{n,d}(a^1,x),\ldots,\Phi_{n,d}(a^m,x), 1-yx_n\rangle$ of $\mathbb{K}[a_e,x,y]$, where y is an auxiliary variable.
(F.1) If $\mathcal{Q}\cap\mathbb{K}[a_e] \neq \langle\emptyset\rangle$, then $x_n \in \sqrt{\mathcal{J}_{\hat{a}_e}}$, $\forall \hat{a}_e \notin \mathbf{V}(\mathcal{Q}\cap\mathbb{K}[a_e])$, whence for "almost all" $\hat{a}_e \in \mathbb{K}^{m\,\ell_{n,d}}$.
(F.2) If $\mathcal{Q}\cap\mathbb{K}[a_e] = \langle\emptyset\rangle$, then $x_n \notin \sqrt{\mathcal{J}_{\hat{a}_e}}$ for "almost all" $\hat{a}_e \in \mathbb{K}^{m\,\ell_{n,d}}$.
To prove (F.1), note that, for any specialization $\hat{a}_e \notin \mathbf{V}(\mathcal{Q}\cap\mathbb{K}[a_e])$, one has $\mathcal{Q}_{\hat{a}_e} = \langle 1\rangle$, and therefore Theorem 1 implies $x_n \in \sqrt{\mathcal{J}_{\hat{a}_e}}$. The condition $\mathcal{Q}\cap\mathbb{K}[a_e] \neq \langle\emptyset\rangle$ implies that the variety $\mathbf{V}(\mathcal{Q}\cap\mathbb{K}[a_e])$ of $\mathbb{K}^{m\,\ell_{n,d}}$ does not coincide with the whole $\mathbb{K}^{m\,\ell_{n,d}}$. To prove (F.2), let $\mathcal{S} \subseteq \mathbb{K}^\ell$ be the set of all specializations $\hat{a}_e$ such that $\mathcal{Q}_{\hat{a}_e} = \langle 1\rangle$; its Zariski closure $\overline{\mathcal{S}}$ cannot coincide with the whole $\mathbb{K}^{m\,\ell_{n,d}}$, because $\mathcal{Q}\cap\mathbb{K}[a_e] = \langle\emptyset\rangle$, whence $x_n \notin \sqrt{\mathcal{J}_{\hat{a}_e}}$, for all $\hat{a}_e \in \mathbb{K}^{m\,\ell_{n,d}}\backslash\overline{\mathcal{S}}$, where $\mathbb{K}^{m\,\ell_{n,d}}\backslash\overline{\mathcal{S}}$ is Zariski open.
Proof of (11.1). If $m = n$, then $\mathcal{Q}\cap\mathbb{K}[a_e]$ is a principal ideal; it is generated by one polynomial $q(a_e)$ (*i.e.*, $\mathcal{Q}\cap\mathbb{K}[a_e] = \langle q(a_e)\rangle$), which is the resultant

$$\mathrm{Res}(\Phi_{n,d}(a^1,x),\ldots,\Phi_{n,d}(a^n,x))$$

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.*, $\mathbf{V}(\mathcal{J}_{\hat{a}_e}) = \{0\}$ and hence $\mathbf{V}(\mathcal{Q}_{\hat{a}_e}) = \emptyset$. 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, $\mathcal{Q}\cap\mathbb{K}[a_e] \neq \langle\emptyset\rangle$, whence (F.1) implies that $x_n \in \sqrt{\mathcal{J}_{\hat{a}_e}}$, 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), $\mathrm{Res}(\Phi_{n,d}(a^1,x),\ldots,\Phi_{n,d}(a^n,x))$, belongs to $\mathcal{Q}\cap\mathbb{K}[a_e]$, whence $\mathcal{Q}\cap\mathbb{K}[a_e] \neq \langle\emptyset\rangle$; (F.1) implies that $x_n \in \sqrt{\mathcal{J}_{\hat{a}_e}}$, 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 $\mathcal{Q}\cap\mathbb{K}[a_e]$ is the zero ideal $\langle\emptyset\rangle$; hence, (F.2) implies that $x_n \notin \sqrt{\mathcal{J}_{\hat{a}_e}}$, for "almost all" $\hat{a}_e \in \mathbb{K}^{m\ell_{n,d}}$. □

Proof. (of Lemma 12) If $n \leq m$, then $\sqrt{\mathcal{J}}$ is "generically" maximal, since $\sqrt{\mathcal{J}} = \langle x_1,\ldots,x_n\rangle$ "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 $\hat{h}_1(x^1, x^2) = \Phi_{n,d}(\hat{a}^1, x), \ldots, \hat{h}_m(x^1, x^2) = \Phi_{n,d}(\hat{a}^m, x)$, 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. $\mathcal{J}_{\hat{a}_e} = \langle \hat{h}_1, \ldots, \hat{h}_m \rangle$, *i.e.*, $\mathcal{J}_{\hat{a}_e} \cap \mathbb{K}[x_1, \ldots, x_{m-1}, x_m] = \langle \emptyset \rangle$ and $\mathcal{J}_{\hat{a}_e} \cap \mathbb{K}[x_1, \ldots, x_{m-1}] \neq \langle \emptyset \rangle$. Let $\mathcal{G}_{\mathcal{J}_{\hat{a}_e}} = \{g_1, \ldots, g_s\}$ be the rGb of $\mathcal{J}_{\hat{a}_e}$, w.r.t. the Lex order with $x_i >_{\mathrm{L}} x_j$, $i \in \{1, \ldots, m\}$ and $j \in \{m+1, \ldots, n\}$. Coerce the polynomials g_i into $\mathbb{K}[x^2][x^1]$ and compute $k_{g_1,\ldots,g_s} = \sum_{i=1}^{s} \mathrm{LC}(g_i)$, which belongs to $\mathbb{K}[x^2]$. Now, coercing $k_{g_1,\ldots,g_s}$ into $\mathbb{K}[x]$, consider the saturation $(\mathcal{J}_{\hat{a}_e} : \langle k^{\infty}_{g_1,\ldots,g_s} \rangle)$. By [4], $\mathcal{J}_{\hat{a}_e}$ is primary if and only if $(\mathcal{J}_{\hat{a}_e} : \langle k^{\infty}_{g_1,\ldots,g_s} \rangle) = \mathcal{J}_{\hat{a}_e}$. Clearly, if $(\mathcal{J}_{\hat{a}^o_e} : \langle k^{\infty}_{g_1,\ldots,g_s} \rangle) = \mathcal{J}_{\hat{a}^o_e}$ for some specialization $\hat{a}^o_e$, then $(\mathcal{J}_{\hat{a}_e} : \langle k^{\infty}_{g_1,\ldots,g_s} \rangle) = \mathcal{J}_{\hat{a}_e}$, for "almost all" specializations $\hat{a}_e$. To complete the proof, it is enough to find one of such $\hat{a}^o_e$. Take $\hat{h}^o_1 = (x_1 + x_{m+1} + \ldots + x_n)^d, \ldots, \hat{h}^o_m = (x_m + x_{m+1} + \ldots + x_n)^d$; 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 $a_e = [(a^1)^\top \ldots (a^m)^\top]^\top$. For any specialization $\hat{a}_e \in \mathbb{K}^{m\,\ell_{n,d}}$ of a_e, let $\hat{h}$ be the corresponding specialization of h. As well known [5], the n polynomials $\hat{h}_i$ in the n unknowns x_i are algebraically independent if and only if $\det(\frac{\partial \hat{h}}{\partial x}) = 0$ in $\mathbb{K}[x]$; $\det(\frac{\partial h}{\partial x}) \neq 0$ in $\mathbb{K}[a_e, x]$ and can be rewritten as $\det(\frac{\partial h}{\partial x}) = q_1(a_e)x^{\alpha^1} + q_2(a_e)x^{\alpha^2} + \ldots$, where $q_i(a_e)$, $i = 1, 2, \ldots$, are non-zero polynomials and the α^i's are multi-indices of the same length $|\alpha^i| = |\alpha^j|$. Let $\mathcal{Q} = \langle q_1(a_e), q_2(a_e), \ldots \rangle$ be an ideal of $\mathbb{K}[a_e]$; $\det(\frac{\partial \hat{h}}{\partial x}) = 0$ in $\mathbb{K}[x]$ if and only if $\hat{a}_e \in \mathbf{V}(\mathcal{Q})$, thus proving the theorem, since $\mathbf{V}(\mathcal{Q}) \neq \mathbb{K}^{m\ell_{n,d}}$. Similarly, for $n > m$. □

Proof. (of Lemma 14) By the proof of Theorem 5, each $p \in \widetilde{\Sigma}^{\mathbb{K}}_{2d,m^*}[x]$ can be taken as a specialization $p_{\hat{a}^*_e}(x) = p(\hat{a}^*_e, x)$ of $p(a^*_e, x) = \sum_{i=1}^{m^*} w_i h_i^2(a^i, x)$, where

$$a^*_e = [(a^1)^\top \ldots (a^{m^*})^\top\, w_1 \ldots w_{m^*}]^\top,$$

and, for "almost all" $a^*_e \in \mathbb{K}^{(\ell_{n,d}+1)m^*}$, the variety $\mathbf{V}_{\overline{\mathbb{K}}^n}(\langle \frac{\partial p(a^*_e,x)}{\partial x} \rangle : \langle h^\top(a^*_e, x) \rangle)$ is finite. This implies the existence of $q \in \mathbb{K}[a^*_e]$ such that $q(a^*_e)x_n^{N^*} \in (\langle \frac{\partial p(a^*_e,x)}{\partial x} \rangle : \langle h^\top(a^*_e, x) \rangle) \cap \mathbb{K}[a^*_e, x_n]$. Hence, for each $\hat{a}^*_e \in \mathbb{K}^{(\ell_{n,d}+1)m^*}$ such that $q(\hat{a}^*_e) \neq 0$, one has $(\langle \frac{\partial p(\hat{a}^*_e,x)}{\partial x} \rangle : \langle x_n^{N^*} \rangle) = \langle h^\top \rangle$. □

References

[1] L. Menini, C. Possieri, and A. Tornambe, "Algebraic certificates of (semi)definiteness for polynomials over fields containing the rationals," *IEEE Trans. Autom. Control*, 2018.

[2] A. R. Rajwade, *Squares*, vol. 171. Cambridge Univ. Press, 1993.

[3] D. Cox, J. Little, and D. O'Shea, *Using algebraic geometry*. Springer Verlag, 1998.

[4] P. Gianni, B. Trager, and G. Zacharias, "Gröbner bases and primary decomposition of polynomial ideals," *J. of Symb. Computation*, vol. 6, no. 2, pp. 149–167, 1988.

[5] P. J. Olver, *Applications of Lie groups to differential equations*, vol. 107 of *Graduate Texts in Mathematics*. Springer, 1986.