Journal of Algebra 674 (2025) 314–340

Contents lists available at ScienceDirect

Journal of Algebra

journal homepage: www.elsevier.com/locate/jalgebra

Research Paper

Convex hulls of curves in n-space

Claus Scheiderer

Fachbereich Mathematik und Statistik, Universität Konstanz, 78457 Konstanz, Germany

A R T I C L E I N F O

Article history:
Received 10 November 2024
Available online 20 March 2025
Communicated by Franz-Viktor Kuhlmann

Keywords:
Spectrahedral shadows
Convex algebraic geometry
Real algebraic geometry
Real closed fields

A B S T R A C T

Let $K \subseteq \mathbb{R}^n$ be a convex semialgebraic set. The semidefinite extension degree $\operatorname{sxdeg}(K)$ of K is the smallest number d such that K is a linear image of an intersection of finitely many spectrahedra, each of which is described by a linear matrix inequality of size $\le d$. This invariant can be considered to be a measure for the intrinsic complexity of semidefinite optimization over the set K. For an arbitrary semialgebraic set $S \subseteq \mathbb{R}^n$ of dimension one, our main result states that the closed convex hull K of S satisfies $\operatorname{sxdeg}(K) \le 1 + \lfloor \frac{n}{2} \rfloor$. This bound is best possible in several ways. Before, the result was known for $n = 2$, and also for general n in the case when S is a monomial curve.

Introduction

Semidefinite programming (SDP) is the task of optimizing a linear function over the solution set of a linear matrix inequality (LMI)

$$A_0 + \sum_{i=1}^{n} x_i A_i \succeq 0$$

E-mail address: claus.scheiderer@uni-konstanz.de.

https://doi.org/10.1016/j.jalgebra.2025.03.018

where $A_0, \dots, A_n$ are real symmetric matrices of some size and $A \succeq 0$ means that A is positive semidefinite. Under mild conditions, semidefinite programs can be solved in polynomial time, up to any prescribed accuracy. Thanks to its enormous expressive power, semidefinite programming has numerous applications from a wide range of areas. See [1] for detailed background on SDP.

Solution sets of linear matrix inequalities are called spectrahedra. The feasible sets of semidefinite programming are therefore spectrahedra and, more generally, linear images of spectrahedra (aka spectrahedral shadows). The performance of numerical SDP solvers is known to be heavily influenced by the matrix size of the LMI. On the other hand, it is often possible in concrete examples to represent a given convex set K by a combination of several LMIs of small size d. Practical experience shows that this size d is far more critical for the running time than the number of the LMIs. Motivated by these observations, Averkov [1] introduced an invariant of convex semialgebraic sets $K \subseteq \mathbb{R}^n$ that captures this essential bit of the intrinsic complexity of semidefinite optimization over K: The *semidefinite extension degree* of K, denoted $\mathrm{sxdeg}(K)$, is the smallest number d such that K can be written as a linear image of a finite intersection of spectrahedra, all of which are described by LMIs of size $\le d$. So $\mathrm{sxdeg}(K) \le d$ means that K can be represented in the form

$$K \;=\; \bigl\{x \in \mathbb{R}^n \colon \exists\, y \in \mathbb{R}^m \;\, A(x,y) \succeq 0\bigr\}$$

for some m, where $A(x,y) = A_0 + \sum_{i=1}^n x_i A_i + \sum_{j=1}^m y_j B_j$ is a symmetric linear matrix polynomial of block-diagonal structure with all blocks of size at most d. For example, $\mathrm{sxdeg}(K) \le 1$ if and only if K is a polyhedron, and $\mathrm{sxdeg}(K) \le 2$ if and only if K is second-order cone representable. It is this invariant that we are going to study.

Let $n \ge 1$, and let S be an arbitrary semialgebraic set in $\mathbb{R}^n$ of dimension one. Our main result (Theorem 1.3) states that the closed convex hull K of S satisfies $\mathrm{sxdeg}(K) \le 1 + \lfloor \frac{n}{2} \rfloor$. Before, this was known for $n = 2$ [7], and also for general n in the case where S is a curve parametrized by monomials [2]. In the general case, it was known from [5] that $\mathrm{sxdeg}(K)$ is finite, or in other words, that K is a spectrahedral shadow.

The upper bound in Theorem 1.3 is best possible: If $n = 2k$ is even and K is the closed convex hull of the rational normal curve $\{(t, t^2, \dots, t^n) \colon t \in \mathbb{R}\}$ of degree n, then $\mathrm{sxdeg}(K) = 1 + \frac{n}{2}$, as follows from [1, Cor. 2.3]. In this particular case, K happens to be a spectrahedron, and an explicit representation of minimal matrix size $k+1$ is given by the LMI

$$\begin{pmatrix} 1 & x_1 & \cdots & x_k \\ x_1 & x_2 & \cdots & x_{k+1} \\ \vdots & \vdots & & \vdots \\ x_k & x_{k+1} & \cdots & x_{2k} \end{pmatrix} \;\succeq\; 0.$$

Our theorem cannot be extended to convex hulls of sets of dimension greater than one. Indeed, such convex hulls need not be spectrahedral shadows in general. Explicit examples in $\mathbb{R}^n$ are currently known for $n \geq 11$, and can be found in [6] or in [8, Sect. 8.7].

For monomial curves, the proof of our main result in [2] leads to an explicit semidefinite representation of the convex hull. This is not so in the general situation considered here. The basic approach is the same as for monomial curves, but the technical details are getting considerably more involved in the general case. To establish the upper bound for $\mathrm{sxdeg}(K)$ we dualize, meaning that, instead of the convex hull K, we study the convex cone of linear polynomials that are non-negative on S. The main tool for our proof is an algebraic characterization of $\mathrm{sxdeg}(K)$ that uses the concept of *tensor evaluation*. For precise details we refer to 2.7 and Theorem 2.8 below.

In the (explicit) case of monomial curves, a key role was played in [2] by Schur polynomials and by Jacobi's bialternant identity. We would like to point out that the same is true in the general case considered here. Speaking very loosely, the problem can be localized to some extent. Locally around a given point, Schur polynomials provide a lowest degree approximation of the problem. A large part of the effort then consists in showing that this approximation dominates the picture in a sufficiently small neighborhood.

The paper is organized as follows. After stating the main result and its dual version in Section 1, we apply a number of reduction steps in Section 2. Here we also recall the concept of tensor evaluation. Sections 3 and 4 are of preparatory character, dealing respectively with Schur polynomials and with extreme rays in cones of non-negative polynomials. A very rough general outline of the proof is given in Section 5. Sections 6 and 7 set up the technical machinery needed for the proof proper, while the actual proof is given in Section 8.

1. Main result

1.1. Before stating the main theorem we briefly recall a few basic notions from convexity. Let C be a convex cone in a finite-dimensional $\mathbb{R}$-vector space V, meaning that $C \neq \varnothing$, $C + C \subseteq C$ and $aC \subseteq C$ for every real number $a \geq 0$. The cone C is said to be pointed if $C \cap (-C) = \{0\}$. A convex subset $F \neq \varnothing$ of C is a *face* of C if $x, y \in C$ and $x + y \in F$ imply $x, y \in F$. If $0 \neq x \in C$ is such that the half-line $F = \{ax\colon a \geq 0\}$ is a face of C then F is called an *extreme ray* of C. Every closed and pointed convex cone is the Minkowski sum of its extreme rays. For every $x \in C$ there is a unique smallest face of C, denoted F_x, that contains x. We call F_x the *supporting face* of x (in C). See [8, Sect. 8.1] for these facts and for more general background.

Definition 1.2. (See [1]) Let K be a convex semialgebraic set in $\mathbb{R}^n$. The *semidefinite extension degree* $\mathrm{sxdeg}(K)$ of K is the smallest integer $d \geq 0$ such that K has a representation

$$K \;=\; \Big\{x\in\mathbb{R}^n\colon \exists\, y\in\mathbb{R}^m \;\forall\,\nu=1,\dots,r\;\, A_\nu+\sum_{i=1}^n x_iB_{\nu i}+\sum_{j=1}^m y_jC_{\nu j}\succeq 0\Big\}$$

with r, $m\ge 1$ and with A_ν, $B_{\nu i}$, $C_{\nu i}$ real symmetric matrices of the same size $d_\nu\le d$, for all $\nu=1,\dots,r$. We put $\operatorname{sxdeg}(K)=\infty$ if there is no such integer $d\ge 0$.

If K is an affine space then $\operatorname{sxdeg}(K)=0$ (this may be considered part of the definition), otherwise $\operatorname{sxdeg}(K)\ge 1$. It follows directly that $\operatorname{sxdeg}(K)\le 1$ if and only if K is a polyhedron. Moreover it is not hard to see (e.g. [7, Example 1.5]) that $\operatorname{sxdeg}(K)\le 2$ if and only if K is second-order cone representable. The main result of this paper is the following:

Theorem 1.3. *Let $S\subseteq\mathbb{R}^n$ be a semialgebraic set of dimension one, let $K\subseteq\mathbb{R}^n$ be the closed convex hull of S. Then* $\operatorname{sxdeg}(K)\le 1+\lfloor\frac n2\rfloor$.

Here, of course, $\lfloor\frac n2\rfloor$ denotes the largest integer $\le\frac n2$. In particular:

Corollary 1.4. *The closed convex hull of any one-dimensional semialgebraic set in $\mathbb{R}^3$ is second-order cone representable.* □

Let $S\subseteq\mathbb{R}^n$ be a subset, let K be its closed convex hull and let

$$P_S \;=\; \{f\in\mathbb{R}[x]_{\le 1}\colon f|_S\ge 0\},$$

the set of linear polynomials in $x=(x_1,\dots,x_n)$ that are non-negative on S. Recall that the homogenization K^h of K is the closure of $\{(t,tu)\colon u\in K,\ t\ge 0\}$ in $\mathbb{R}\times\mathbb{R}^n$ [8, Prop. 8.1.19]. The set P_S is a closed convex cone in $\mathbb{R}[x]_{\le 1}$, and is linearly isomorphic to the dual convex cone of K^h in a natural way [8, Example 8.1.23]. By [7, Cor. 1.9] we have $\operatorname{sxdeg}(K)=\operatorname{sxdeg}(P_S)$. So Theorem 1.3 follows from the following theorem:

Theorem 1.5. *Let C be an affine algebraic curve over $\mathbb{R}$, let $S\subseteq C(\mathbb{R})$ be a semialgebraic set, and let V be a linear subspace of the affine coordinate ring $\mathbb{R}[C]$ of C with* $\dim(V)=n+1$. *Then the closed convex cone*

$$P_{V,S} \;:=\; \{f\in V\colon f|_S\ge 0\}$$

in V satisfies $\operatorname{sxdeg}(P_{V,S})\le 1+\lfloor\frac n2\rfloor$.

Proof of 1.5 ⇒ 1.3. Assuming Theorem 1.5, let $S\subseteq\mathbb{R}^n$ be a semialgebraic set of dimension one. We may assume that S is not contained in an affine hyperplane of $\mathbb{R}^n$. Let C be the Zariski closure of S and let $V\subseteq\mathbb{R}[C]$ be the image of $\mathbb{R}[x_1,\dots,x_n]_{\le 1}$ in $\mathbb{R}[C]$. Then $\dim(V)=n+1$ and $P_{V,S}=P_S$, and so $\operatorname{sxdeg}(K)=\operatorname{sxdeg}(P_S)=\operatorname{sxdeg}(P_{V,S})$. □

2. First reduction steps

We start by making a couple of first reductions towards a proof of Theorem 1.5. On one hand they concern the curve C and the set S. On the other we are going to reformulate the task of bounding $\mathrm{sxdeg}(K)$ in a way that is more abstract and algebraic, but also more manageable.

2.1. The set S can be assumed to be closed. It is enough to cover S by finitely many semialgebraic sets S_i and to prove the theorem for each of them. Indeed, since $P_{V,S} = \bigcap_i P_{V,S_i}$ we have $\mathrm{sxdeg}(P_{V,S}) \le \max_i \mathrm{sxdeg}(P_{V,S_i})$ [7, Lemma 1.4(d)]. In this way we may assume that the Zariski closure $C \subseteq \mathbb{A}^n$ of S is an irreducible curve, and that S does not have any isolated point. We may in fact assume that the curve C is non-singular, since otherwise we replace C by its normalization C' and $S \subseteq C(\mathbb{R})$ by its preimage in $C'(\mathbb{R})$. Since S does not have isolated points, S is contained in the image of the natural map $C'(\mathbb{R}) \to C(\mathbb{R})$.

2.2. So let the curve C be irreducible and non-singular. By the previous discussion we assume that S is closed in $C(\mathbb{R})$, and is homeomorphic either to a compact non-degenerate interval or to a closed half-line. In fact it is enough to consider compact intervals. Indeed, assuming that S is homeomorphic to $[0,\infty[$, let $\overline{C}$ be the non-singular projective model of C and let $u \in \overline{C}(\mathbb{R}) \smallsetminus C(\mathbb{R})$ be the point in the closure of S. Choose a point $v \in C(\mathbb{R}) \smallsetminus S$ and let $C' = \overline{C} \smallsetminus \{v\}$. Then C' is an affine curve, and the subset $S' := S \cup \{u\}$ of $C'(\mathbb{R})$ is homeomorphic to $[0,1]$. If $0 \ne p \in \mathbb{R}[C']$ is chosen such that p vanishes in all (real and nonreal) points of $\overline{C} \smallsetminus C$, and if $k \ge 1$ is large enough, the subspace $V' := p^{2k}V$ of the function field $\mathbb{R}(C) = \mathbb{R}(C')$ is contained in $\mathbb{R}[C']$. Multiplication by p^{2k} is a vector space isomorphism $V \to V'$ under which the cone $P_{V,S}$ gets identified with the cone $P_{V',S'}$. So it suffices to consider the latter cone.

Summarizing the reduction steps discussed so far, we have:

Lemma 2.3. *To prove Theorem 1.5, it suffices to consider the case where the curve C is irreducible and non-singular and where the set $S \subseteq C(\mathbb{R})$ is homeomorphic to* $[0,1]$. □

2.4. Let $\xi \in C(\mathbb{R})$ be an $\mathbb{R}$-point. The order of vanishing of a rational function $f \in \mathbb{R}(C)$ in the point ξ will be denoted $\mathrm{ord}_\xi(f)$. A *local orientation* of $C(\mathbb{R})$ at ξ is an equivalence class of local uniformizers at ξ (elements $u \in \mathbb{R}[C]$ with $\mathrm{ord}_\xi(u) = 1$), where u_1 and u_2 are said to be equivalent if $\frac{u_1}{u_2}(\xi) > 0$. Let such a local orientation at ξ be given. By a *closed interval on the positive side* of ξ, we mean a compact connected set $J \subseteq C(\mathbb{R})$ with $\xi \in J$ and $|J| > 1$ such that $u|_J \ge 0$ for some local uniformizer u at ξ that represents the given orientation. Such J has boundary points ξ and $\xi' \ne \xi$, and we'll simply write $J = [\xi, \xi']$ (tacitly assuming the given local orientation to be understood).

With this terminology we may reduce the task of proving Theorem 1.5 still a bit further:

Lemma 2.5. *Let C be an affine curve over $\mathbb{R}$, irreducible and non-singular, and let $V \subseteq \mathbb{R}[C]$ be a linear subspace with $\dim(V) = n+1$. Suppose that, for every $\xi \in C(\mathbb{R})$ and every local orientation of $C(\mathbb{R})$ at ξ, some closed interval $J \subseteq C(\mathbb{R})$ on the positive side of ξ can be found such that $\mathrm{sxdeg}(P_{V,J_1}) \le 1 + \lfloor \frac{n}{2} \rfloor$ holds for every closed interval $J_1 = [\xi, \xi_1]$ contained in J. Then $\mathrm{sxdeg}(P_{V,S}) \le 1 + \lfloor \frac{n}{2} \rfloor$ holds for every semialgebraic set $S \subseteq C(\mathbb{R})$.*

Proof. By Lemma 2.3 we may assume that S is homeomorphic to $[0, 1]$. Then S is covered by finitely many closed intervals $J_i = [\xi_i, \xi_i']$ as in the statement, and so

$$\mathrm{sxdeg}(P_{V,S}) \le \max_i \mathrm{sxdeg}(P_{V,J_i}) \le 1 + \lfloor \frac{n}{2} \rfloor$$

by the remarks in 2.1. □

2.6. Throughout the paper we'll denote the affine coordinate ring of the curve C by $A = \mathbb{R}[C]$. In view of Lemma 2.5, fix a point $\xi \in C(\mathbb{R})$ together with one of the two local orientations at ξ. To verify the condition in this lemma we may replace the curve C by an arbitrary Zariski-open neighborhood of ξ in C. In this way we may assume that there exists an element t in A such that the A-module $\Omega_{A/\mathbb{R}}$ of Kähler differentials is freely generated by dt. After replacing t with $t - t(\xi)$, the element t will be a local uniformizer at ξ, and after multiplication with -1 if necessary, t will represent the given local orientation at ξ. Both ξ and t will be fixed for the rest of the paper. By shrinking C further around ξ if necessary, we can in addition assume that the maximal ideal $\mathfrak{m}_\xi = \{f \in A \colon f(\xi) = 0\}$ in A is principal, generated by t.

2.7. The second reduction step is more abstract in nature. First we need to recall some facts from [7, Sect. 3] about tensor evaluation. Let X be an affine $\mathbb{R}$-variety and let $R \supseteq \mathbb{R}$ be a real closed field. Write $R[X] = \mathbb{R}[X] \otimes R$ (tensor product over $\mathbb{R}$) and let $f \in R[X]$. If $\eta \in X(R)$ is an R-rational point of X (i.e., a homomorphism $\eta \colon \mathbb{R}[X] \to R$), let the *tensor evaluation* $f^{\otimes}(\eta)$ (of f at η) be the image of f under the ring homomorphism

$$R[X] = \mathbb{R}[X] \otimes R \xrightarrow{\eta \otimes \mathrm{id}} R \otimes R.$$

Note that $f(\eta) \in R$ (the usual evaluation of f at η) is the result of applying the product map $R \otimes R \to R$ to $f^{\otimes}(\eta)$.

For M a semialgebraic subset of $X(\mathbb{R})$, let M_R denote the base field extension of M to R (see [8, Sect. 4.1]). This is the subset of $X(R)$ that is described by the same finite system of polynomial inequalities as M. Given $\theta \in R \otimes R$, let $\mathrm{rk}(\theta)$ (the tensor rank of θ) be the minimal number $r \ge 0$ such that $\theta = \sum_{i=1}^{r} a_i \otimes b_i$ for suitable a_i, $b_i \in R$. If θ

is a sum of squares in $R \otimes R$, let $\operatorname{sosx}(\theta)$ be the smallest integer $d \geq 0$ such that there is an identity $\theta = \sum_i \theta_i^2$ with $\operatorname{rk}(\theta_i) \leq d$ for all i. If θ is not a sum of squares we put $\operatorname{sosx}(\theta) = \infty$. To prove our main theorem we are going to apply the following criterion. It is a particular case of [7, Thm. 3.10]:

Theorem 2.8. *Let C, V, S and $P = P_{V,S}$ be as in Theorem 1.5, and let E denote the set of elements in P that span an extreme ray of P. Let $d \geq 1$ be an integer. Then* $\operatorname{sxdeg}(P) \leq d$ *holds if and only if* $\operatorname{sosx} f^{\otimes}(\eta) \leq d$ *for every real closed field $R \supseteq \mathbb{R}$, every $f \in E_R$ and every $\eta \in S_R$.*

2.9. Summarizing, we have reduced the task of proving Theorem 1.5 to the following. Let C be an irreducible and non-singular affine curve over $\mathbb{R}$, let $V \subseteq A = \mathbb{R}[C]$ be a linear subspace of dimension $n+1$ and let a point $\xi \in C(\mathbb{R})$ be given, together with a local orientation of $C(\mathbb{R})$ at ξ. We need to find a closed interval $S \subseteq C(\mathbb{R})$ on the positive side of ξ such that the following holds: Whenever $R \supseteq \mathbb{R}$ is real closed, $\eta \in S_R$ is a point and $f \in V_R = V \otimes R$ is non-negative on S_R and generates an extreme ray in $(P_{V,S})_R = \{g \in V_R \colon g|_{S_R} \geq 0\}$, there is an identity $f^{\otimes}(\eta) = \sum_i \theta_i^2$ in $R \otimes R$ where each θ_i has the form $\theta_i = \sum_{j=1}^{k} a_{ij} \otimes b_{ij}$ with $k = 1 + \lfloor \frac{n}{2} \rfloor$ and suitable $a_{ij}, b_{ij} \in R$.

3. Complements on Schur polynomials

3.1. Let $n \geq 0$, let $x = (x_0, \ldots, x_n)$ be a tuple of $n+1$ variables, and let $\underline{a} = (a_0, \ldots, a_n)$ be a sequence of non-negative integers that is strictly decreasing, i.e. satisfies $a_0 > \cdots > a_n \geq 0$. By $\sigma_{\underline{a}} = \sigma_{\underline{a}}(x)$ we denote the polynomial in the variables x that is defined by the identity

$$\sigma_{\underline{a}}(x_0, \ldots, x_n) \cdot \prod_{0 \leq i < j \leq n} (x_i - x_j) \;=\; \det\Big(\big(x_i^{a_j}\big)_{i,j=0,\ldots,d}\Big). \tag{1}$$

The polynomial $\sigma_{\underline{a}}(x)$ is the Schur polynomial associated with the partition $\lambda = \underline{a} - \delta_n$ where $\delta_n = (n, \ldots, 1, 0)$, and identity (1) is known as Jacobi's bialternant formula (see [9, Sect. 7.15]). Standard notation would be $s_\lambda(x)$, rather than $\sigma_{\underline{a}}(x)$, and would use variables $x_1, \ldots, x_n$ instead of $x_0, \ldots, x_n$. In this paper, however, it is the sequence $\underline{a}$ of length $n+1$, rather than the partition λ, that plays the main role. Therefore we prefer the alternative notation used here.

3.2. The polynomial $\sigma_{\underline{a}}(x)$ is symmetric, and its coefficients are non-negative integers that allow a combinatorial characterization. Let us briefly recall this. Let $Y_{\underline{a}}$ denote the Young diagram of shape $\lambda = \underline{a} - \delta_n$. So $Y_{\underline{a}}$ consists of $n+1$ rows that contain $a_0 - n, a_1 - n + 1, \ldots, a_n$ many entries, respectively, and that are aligned to the left. An admissible filling T of $Y_{\underline{a}}$ assigns to each position in $Y_{\underline{a}}$ an integer from $\{0, \ldots, n\}$, in such a way that the entries are weakly increasing in each row (from left to right) and strictly increasing in each column (from top to bottom). If the entry i is assigned to exactly $\alpha(i)$ positions by the filling T, write $x^T = x_0^{\alpha(0)} \cdots x_n^{\alpha(n)}$. With this notation one has

$$\sigma_{\underline{a}}(x) \;=\; \sum_T x^T,$$

sum over all admissible fillings T of $Y_{\underline{a}}$, see [9, Sect. 7.10].

Lemma 3.3. *Let $\underline{a} \neq \underline{b}$ be strictly decreasing sequences of non-negative integers, both of length $n+1$, and assume that $b_i \geq a_i$ for $i = 0, \ldots, n$. Then every monomial of $\sigma_{\underline{b}}(x)$ is properly divisible by some monomial of $\sigma_{\underline{a}}(x)$.*

Proof. It suffices to check this in the case when there is an index k with $b_k = a_k + 1$ and $b_i = a_i$ for all $i \neq k$. Given an admissible filling T of $Y_{\underline{b}}$, corresponding to a monomial x^β of $\sigma_{\underline{b}}(x)$, we may simply delete the last entry of T in row k. This gives an admissible filling of $Y_{\underline{a}}$ whose corresponding monomial divides x^β. $\square$

Lemma 3.4. *Let $\underline{a} = (a_0, \ldots, a_n)$ be a strictly decreasing sequence of non-negative integers, and let $\underline{b} = (b_0, \ldots, b_r)$ be a subsequence of $\underline{a}$ (i.e., there are $0 \leq i(0) < \cdots < i(r) \leq n$ with $b_\nu = a_{i(\nu)}$ for $\nu = 0, \ldots, r$). Then every monomial of $\sigma_{\underline{b}}(x_0, \ldots, x_r)$ is divisible by a monomial of $\sigma_{\underline{a}}(x_0, \ldots, x_r, 1, \ldots, 1)$.*

Proof. It suffices to prove this in the case $r = n - 1$. Write $x = (x_0, \ldots, x_n)$ and $x' = (x_0, \ldots, x_{n-1})$. Let $Y_{\underline{a}}$ and $Y_{\underline{b}}$ be the Young diagrams of $\underline{a}$ and $\underline{b}$, respectively, and let $k \in \{0, \ldots, n\}$ be the index for which a_k is missing in $\underline{b}$. The bottom $n - k$ rows of $Y_{\underline{a}}$ and of $Y_{\underline{b}}$ have the same lengths, while the top k rows of $Y_{\underline{a}}$ are each shorter by one than the corresponding rows of $Y_{\underline{b}}$. Given an admissible filling T of $Y_{\underline{b}}$, corresponding to a monomial x'^{β} of $\sigma_{\underline{b}}(x')$, construct an admissible filling of $Y_{\underline{a}}$ in the following way. First delete the last entry in each of the top k rows of T. Then, for i from 0 to $n-1$, put the remaining entries of row i of T into row i of $Y_{\underline{a}}$, starting from the left in each row. Finally, put the entry n into those boxes of $Y_{\underline{a}}$ that are still unfilled. The filling of $Y_{\underline{a}}$ constructed in this way is admissible and corresponds to a monomial x^α of $\sigma_{\underline{a}}(x)$ which, after substitution $x_n = 1$, divides x'^{β}. $\square$

The following lemma will be needed in Section 6:

Lemma 3.5. *Let B be a commutative ring, let $p_0, \ldots, p_n \in B[[t]]$ be formal power series and let $0 \leq r \leq n$. Let M be a matrix of size $(n+1) \times (n+1)$ with coefficients in $B[[x_0, \ldots, x_r]]$ whose i-th row is*

$$\big(p_0(x_i),\; \ldots,\; p_n(x_i)\big)$$

for $i = 0, \ldots, r$, and whose lower $n - r$ rows have coefficients in B.

(a) *There is a (unique) power series* $g \in B[[x_0, \dots, x_r]]$ *such that*

$$\det(M) \;=\; g \cdot \prod_{0 \le i < j \le r} (x_i - x_j).$$

(b) *If the vanishing orders* $m_i = \mathrm{ord}_t(p_i)$ $(i = 0, \dots, n)$ *satisfy* $m_0 > \cdots > m_n$*, the series* g *lies in the ideal of* $B[[x_0, \dots, x_r]]$ *that is generated by the monomials of* $\sigma_{\underline{m}}(x_0, \dots, x_r, 1, \dots, 1)$*, where* $\underline{m} = (m_0, \dots, m_n)$*.*

Proof. The factor g is unique since $x_i - x_j$ is not a zero divisor in the power series ring, for $i < j$. Assertion (a) is clear since the determinant vanishes after substitution $x_j := x_i$. Using the Leibniz formula, it suffices for (b) to consider the case where each p_i is a monomial $p_i = t^{a_i}$ with $a_i \ge m_i$. So assume $p_i = t^{a_i}$ with $a_i \ge m_i$ for all i. Expanding the determinant by its lower $n - r$ rows, we see that $\det(M)$ is a B-linear combination (usually infinite) of $(r+1) \times (r+1)$-determinants

$$\det \begin{pmatrix} x_0^{b_0} & \cdots & x_0^{b_r} \\ \vdots & & \vdots \\ x_r^{b_0} & \cdots & x_r^{b_r} \end{pmatrix} \tag{2}$$

where $\underline{b} = (b_0, \dots, b_r)$ is a subsequence of $\underline{a} = (a_0, \dots, a_n)$. Say $b_i = a_{\nu(i)}$ with $0 \le \nu(0) < \cdots < \nu(r) \le n$, let $\underline{m}' = (m_{\nu(0)}, \dots, m_{\nu(r)})$ and let $\underline{b}' = (b'_0, \dots, b'_r)$ be the descending permutation of $\underline{b}$. We may assume that $b_i \ne b_j$ for $i \ne j$, then (2) is equal to $\pm\sigma_{\underline{b}'}(x_0, \dots, x_r) \cdot \prod_{0 \le i < j \le r}(x_i - x_j)$. It is easily checked that $b'_i \ge m'_i = m_{\nu(i)}$ holds for $i = 0, \dots, r$. Therefore every monomial in $\sigma_{\underline{b}'}(x_0, \dots, x_r)$ is divisible by some monomial in $\sigma_{\underline{m}'}(x_0, \dots, x_r)$, by Lemma 3.3, and hence by a monomial in $\sigma_{\underline{m}}(x_0, \dots, x_r, 1, \dots, 1)$ (Lemma 3.4). So the proof is complete. □

4. Extreme rays

4.1. Let C be an affine algebraic curve over $\mathbb{R}$ that is irreducible and non-singular. As before we write $A = \mathbb{R}[C]$ for the affine coordinate ring of C. We assume that $C(\mathbb{R}) \ne \varnothing$, so $C(\mathbb{R})$ is topologically a union of finitely many loops (1-spheres) and copies of the affine line $\mathbb{R}$. Let V be a linear subspace of A of dimension $n + 1 < \infty$, with basis $p_0, \dots, p_n$. For the following fix a compact semialgebraic subset $S \ne \varnothing$ of $C(\mathbb{R})$ without isolated points. We are going to study the convex cone $P = P_{V,S}$ in V consisting of all $f \in V$ that are non-negative on S. Clearly, the cone P is closed and pointed.

Definition 4.2. Given an element $f \in V$, put

$$V_f \;=\; \{g \in V \colon \forall\, \xi \in S \;\, \mathrm{ord}_\xi(g) \ge \mathrm{ord}_\xi(f)\}.$$

So V_f is the linear space consisting of all $g \in V$ with at least the same zeros in S as f, taking multiplicities into account.

Proposition 4.3. *Let $S \neq \varnothing$ be a compact semialgebraic set in $C(\mathbb{R})$ without isolated points, and let $0 \neq f \in P = P_{V,S}$.*

(a) *$V_f = F_f - F_f$, the linear span of the supporting face F_f of f in P.*
(b) *In particular, if f spans an extreme ray of P then $V_f = \mathbb{R}f$.*

Proof. It suffices to prove (a). For this let B be the ring of all rational functions on C that have no pole in any point of S. Considering A as a subring of B we have $V_f = V \cap fB$. The supporting face of f in P is $F_f = \{p \in P\colon f - p \in P\}$. If p, $q \in P$ satisfy $f = p + q$, then clearly p, $q \in V_f$, showing that $F_f \subseteq V_f$. To prove that V_f is spanned by F_f, we show that there exists an open neighborhood Ω of the origin in V_f such that $f + \Omega \subseteq F_f$. Let $W = \{g \in B\colon fg \in V_f\}$, then the linear map $W \to V_f$, $g \mapsto fg$ is an isomomorphism. Let $||\cdot||_S$ denote the supremum norm on S. Then $\Omega' = \{g \in W\colon ||g||_S < 1\}$ is an open neighborhood of the origin in W, and so $f\Omega'$ is a neighborhood of 0 in V_f. Since for every $g \in \Omega'$ we have $f(1 \pm g) \in P$, it follows that $f(1 + \Omega') \subseteq F_f$, completing the proof. □

As a consequence, note that every extreme ray of P is determined (inside V) by its zeros in S, listed with multiplicities. Since prescribing one zero means one linear condition on elements of V, we also conclude:

Corollary 4.4. *If $f \in P$ spans an extreme ray of P, then f has at least n zeros in S, counted with multiplicities.* □

We remark that the results of this section remain true *verbatim* if the ground field is an arbitrary real closed field R, instead of the field of real numbers. Of course one has to replace "convex" by "R-convex", the corresponding notion over R (cf. [8, Cor. 1.6.18]).

If f spans an extreme ray of P, we'll later use Proposition 4.3 to obtain a determinantal identity for f, at least in the case where f has exactly n zeros in S. See Proposition 7.8 and Section 8.

5. Outline of the proof

We now give a very coarse outline for the proof of Theorem 1.5 (following the reductions made in 2.9) and for the rest of this paper. Given the point $\xi \in C(\mathbb{R})$, the linear system V in $A = \mathbb{R}[C]$ has a basis $p_0, \dots, p_n$ such that the sequence $\underline{m} = (m_0, \dots, m_n)$ of vanishing orders $m_i = \mathrm{ord}_\xi(p_i)$ is strictly decreasing. If S is a closed interval on the positive side of ξ, and if S is sufficiently small, a general extremal member f of $(P_{V,S})_R$ (for $R \supseteq \mathbb{R}$ any real closed field) will have precisely n zeros in S_R, and these zeros determine f up to scaling. If we fix the number r of different zeros $\xi_1, \dots, \xi_r$ and the tuple $\underline{b} = (b_1, \dots, b_r)$ of their (even) multiplicities, there exists a Nash function (analytic and algebraic) $G(x_0, x_1, \dots, x_r)$, defined on a neighborhood of $(\xi, \dots, \xi)$ in $C(\mathbb{R})^{r+1}$, such that f is given as

$$f(x) \;=\; G(x,\xi_1,\dots,\xi_r)\cdot\prod_{j=1}^{r}\bigl(t(x)-t(\xi_j)\bigr)^{b_j} \tag{3}$$

in a neighborhood of $x=\xi$. Writing G as a (convergent) power series in $(t_0,\dots,t_r)$, the lowest degree terms of G are given by a Schur polynomial

$$\sigma_{\underline{m}}(t_0,t_1,\dots,t_1,\dots,t_r,\dots,t_r), \tag{4}$$

up to a scalar factor. "Morally", the tensor evaluation $f^{\otimes}(\eta)$ should be the image of

$$G(\eta,\xi_1,\dots,\xi_r)\cdot\prod_{j=1}^{r}\bigl(t(\eta)-t(\xi_j)\bigr)^{b_j} \tag{5}$$

under a ring homomorphism $\mathbb{R}\langle x_0,\dots,x_r\rangle\to R\otimes R$ that maps x_0 to $t(\eta)\otimes 1$ and x_j to $1\otimes t(\xi_j)$ for $j=1,\dots,r$. (Here $\mathbb{R}\langle\cdots\rangle$ denotes the ring of algebraic (Nash) power series.) The desired sosx-invariant $k=1+\lfloor\frac{n}{2}\rfloor$ should then come out from (5) correctly, after some further discussion.

When C is a monomial curve, parametrized by a tuple $(x^{m_0},\dots,x^{m_n})$ of monomials, this approach works and was essentially carried out in [2]. In fact, the cofactor G agrees with the Schur polynomial (4) in this case. So for monomial curves, there is no need to use power series.

In the general case, however, there is one major problem, apart from a number of detail questions that have been suppressed: A ring homomorphism $\mathbb{R}\langle x_0,\dots,x_r\rangle\to R\otimes R$ as above *simply does not exist.* The approach via (Nash) power series is too coarse. Instead it is necessary to work in an $(n+1)$-fold tensor product $A^{\otimes(n+1)}$ over $\mathbb{R}$, to have the algebraic dependence between the arguments built into the setup. The backdrop is that there won't be a product decomposition (3) any more. The vanishing ideal in $A^{\otimes(n+1)}$ of the generalized diagonal is not principal unless the curve is rational, and so one has to work with suitable ideal generators and with a corresponding decomposition. Arriving at a proper substitute for a product decomposition (5) is a major technical step that will be carried out in the next two sections. The actual proof of the main theorem will then be given in Section 8.

6. Representing the determinant, I

In this section and the next we are working on a non-singular affine algebraic curve. Essentially, the base field won't play a role, so we just assume that k is a field of characteristic zero. Let C be an integral affine curve over k that is non-singular, with affine coordinate ring $A=k[C]$. If $\xi\in C(k)$ is a k-rational point, the maximal ideal of A corresponding to ξ is denoted $\mathfrak{m}_\xi$.

6.1. We consider $A\otimes A=A\otimes_k A$ as an A-algebra via the second tensor component, i.e. write $a(b\otimes c):=a\otimes(bc)$ for a, b, $c\in A$. Let $\mu\colon A\otimes A\to A$ be the product map, let $I = \ker(\mu)$. For $p \in A$ let $\delta(p) := p \otimes 1 - 1 \otimes p$, an element of I. The A-module I/I^2 is naturally isomorphic to the module $\Omega_{A/k}$ of Kähler differentials of A over k, via $\Omega_{A/k} \xrightarrow{\sim} I/I^2$, $dp \mapsto \delta(p) + I^2$ ($p \in A$). Note that I is the vanishing ideal of the diagonal $\Delta_C \subseteq C \times C$, and is an invertible prime ideal of $A \otimes A$.

Lemma 6.2. *The ideal I of $A \otimes A$ is generated by the elements $\delta(p)$ ($p \in A$).*

Proof. If $\alpha = \sum_i a_i \otimes b_i$ lies in I then $\alpha = \sum_i b_i \delta(a_i)$. This proves the lemma (and shows that I is generated by the $\delta(p)$ even as an A-submodule of $A \otimes A$). □

Lemma 6.3. *For $g \in A$ and $\eta \in C(k)$, the following are equivalent:*

(i) $\mathrm{ord}_\eta(g - g(\eta)) = 1$;
(ii) *dg generates the sheaf $\Omega_{C/k}$ on C, locally at η;*
(iii) *$\delta(g)$ generates the ideal I of $A \otimes A$, locally at (η, η).*

Proof. (i) and (ii) are equivalent since the stalk of the sheaf $\Omega_{C/k}$ at η is $\mathfrak{m}_\eta/\mathfrak{m}_\eta^2$, and since dg corresponds to the coset of $g - g(\eta)$ in $\mathfrak{m}_\eta/\mathfrak{m}_\eta^2$ under this isomorphism. Also (iii) $\Rightarrow$ (ii) is clear since $\Omega_{A/k} \cong I/I^2$ via the isomorphism $dg \mapsto \delta(g) + I^2$. Conversely assume (ii) that $\Omega_{C/k}$ is generated by dg locally at η. Replacing C by a suitable neighborhood of η, we may assume that dg generates the A-module $\Omega_{A/k}$. Let M be the maximal ideal of $A \otimes A$ corresponding to (η, η). Then $I \subseteq M$, and $\delta(p) \in \frac{dp}{dg}\delta(g) + I^2 \subseteq \langle \delta(g) \rangle + MI$ holds for every $p \in A$. Since I is generated by the elements $\delta(p)$ ($p \in A$), it follows that $I = \langle \delta(g) \rangle + MI$. So the Nakayama lemma implies $I(A \otimes A)_M = \delta(g)(A \otimes A)_M$. □

6.4. Now we need quite a bit of notation. Fix an integer $n \geq 1$ and put $A_n = A^{\otimes(n+1)} = A \otimes \cdots \otimes A$, the $(n+1)$-fold tensor product over k. The tensor components of A_n will be labeled with $i = 0, \dots, n$. For $0 \leq i \leq n$ let $\varphi_i \colon A \to A_n$ be the i-th canonical embedding, i.e. $\varphi_i(a) = 1 \otimes \cdots \otimes a \otimes \cdots \otimes 1$ with a at position i. For $0 \leq i < j \leq n$ and $a \in A$ write $\delta_{ij}(a) = \varphi_i(a) - \varphi_j(a)$. Moreover let $\mu_{ij} \colon A_n \to A_n$ be the homomorphism that multiplies the i-th and the j-th tensor component and puts the result at position i, while putting 1 at position j. In other words,

$$\mu_{ij}(a_0 \otimes \cdots \otimes a_n) \;=\; b_0 \otimes \cdots \otimes b_n$$

where $b_i = a_i a_j$, $b_j = 1$ and $b_\nu = a_\nu$ for $\nu \in \{0, \dots, n\} \smallsetminus \{i, j\}$. The ideal $I_{ij} = \ker(\mu_{ij})$ is an invertible prime ideal of A_n. Let the ideal $\mathcal{I}$ in A_n be defined by

$$\mathcal{I} \;:=\; \bigcap_{0 \leq i < j \leq n} I_{ij} \;=\; \prod_{0 \leq i < j \leq n} I_{ij} \tag{6}$$

Intersection and ideal product coincide since the I_{ij} are pairwise different invertible prime ideals, and since the local rings of A_n are factorial. In particular we see that

$\mathcal{I}$ is again an invertible ideal of A_n, which corresponds to the generalized diagonal $\bigcup_{i<j}\{(x_0,\dots,x_n)\colon x_i = x_j\}$ in C^{n+1}.

Lemma 6.5. *For $w \in A$ let $\delta_w \in A_n$ be defined by*

$$\delta_w = \prod_{0\le i<j\le n} \delta_{ij}(w).$$

Fixing an arbitrary point $\xi \in C(k)$, the ideal $\mathcal{I}$ of A_n is generated by all elements δ_w where $w \in A$ satisfies $\mathrm{ord}_\xi(w) = 1$.

Proof. It suffices to prove the lemma locally, in a Zariski neighborhood of $\underline{\eta} = (\eta_0,\dots,\eta_n)$ for any given tuple $\underline{\eta} \in C(k)^{n+1}$. Fix $\underline{\eta}$ and let $(p_{ij})_{0\le i<j\le n}$ be a family of elements of A. Then $\mathcal{I}$ is generated by the product $\prod_{0\le i<j\le n}\delta_{ij}(p_{ij})$ locally at $\underline{\eta}$, provided that the following two conditions hold for each pair $i<j$ of indices:

(1) $p_{ij}(\eta_i) \ne p_{ij}(\eta_j)$ if $\eta_i \ne \eta_j$;
(2) $\mathrm{ord}_{\eta_i}(p_{ij} - p_{ij}(\eta_i)) = 1$ if $\eta_i = \eta_j$.

This follows by applying Lemma 6.3 to I_{ij}, for each pair $i<j$. To prove the lemma, it therefore suffices to show: Given a finite number $\xi_0,\dots,\xi_r$ of pairwise different points in $C(k)$, there exists $w \in A$ with $w(\xi_i) \ne w(\xi_j)$ for $i \ne j$, with $\mathrm{ord}_{\xi_i}(w - w(\xi_i)) = 1$ for every i, and with $\mathrm{ord}_\xi(w) = 1$. Using the Chinese remainder theorem, it is clear that this condition is satisfied. □

6.6. From now on we are going to impose some additional assumptions on the curve C. Once and for all, we fix a k-point $\xi \in C(k)$ on C and let $\mathfrak{m}_\xi$ denote the maximal ideal of A corresponding to ξ. Moreover we assume that there is an element $t \in A$ such that

(A1) $\mathfrak{m}_\xi = At$ (the principal ideal generated by t in A),
(A2) the A-module $\Omega_{A/k}$ is (freely) generated by dt,

compare 2.6. We'll also fix t for the rest of the section. If $p \in A$, let $p' = \frac{dp}{dt} \in A$ be defined by $dp = p'\,dt$. This is well-defined by (A2).

6.7. Since the ring A_n is noetherian, Lemma 6.5 implies that there exists a finite subset Λ of A such that the ideal $\mathcal{I}$ is generated by the δ_w ($w \in \Lambda$), and such that $\mathrm{ord}_\xi(w-t) > 1$ (in particular, $\mathrm{ord}_\xi(w) = 1$ and $w'(\xi) = 1$) holds for every $w \in \Lambda$.

We need a few simple observations. The following lemma is easily verified:

Lemma 6.8. *Let V be a linear subspace of A with $\dim(V) = n+1$. Then the set $\{\mathrm{ord}_\xi(p)\colon 0 \ne p \in V\}$ has cardinality $n+1$.* □

Given a subspace $V \subseteq A$ of dimension $n+1$ we write $\underline{m}_\xi(V) = (m_0, \dots, m_n)$ if $m_0 > \cdots > m_n$ and there exist elements $p_i \in V$ with $\mathrm{ord}_\xi(p_i) = m_i$ $(i = 0, \dots, n)$. Note that any such tuple $\underline{p} = (p_0, \dots, p_n)$ is a k-basis of V. Given tuples $\underline{a} = (a_0, \dots, a_n)$, $\underline{b} = (b_0, \dots, b_n)$ of integers, write $\underline{a} \ge \underline{b}$ if $a_i \ge b_i$ for $i = 0, \dots, n$, and write $\underline{a} > \underline{b}$ if $\underline{a} \ge \underline{b}$ and $\underline{a} \ne \underline{b}$.

Lemma 6.9. *Let $q_0, \dots, q_n$ be a k-basis of V, write $a_i = \mathrm{ord}_\xi(q_i)$ $(i = 0, \dots, n)$ and assume $a_0 \ge \cdots \ge a_n$. Then $\underline{m}_\xi(V) \ge (a_0, \dots, a_n)$.*

Proof. If the a_i are pairwise different there is nothing to show. Otherwise let i be the largest index with $a_i = a_{i+1}$. There is (unique) $c \in k^*$ with $\mathrm{ord}_\xi(q_i + cq_{i+1}) > \mathrm{ord}_\xi(q_i)$. Put $a'_i = \mathrm{ord}_\xi(q_i + cq_{i+1})$ and $a'_\nu = a_\nu$ for $\nu \ne i$. If $(\tilde{a}_0, \dots, \tilde{a}_n)$ is the weakly descending permutation of $(a'_0, \dots, a'_n)$ then $(\tilde{a}_0, \dots, \tilde{a}_n) \ge (a_0, \dots, a_n)$ holds. So the lemma follows by descending induction on i. □

Lemma 6.10. *Let $\underline{m}_\xi(V) = (m_0, \dots, m_n)$, and let $\underline{q} = (q_0, \dots, q_n)$ be a linearly independent sequence in A such that $\mathrm{ord}_\xi(q_i) \ge m_i$ for $i = 0, \dots, n$, with strict inequality for at least one index i. Then $W = \mathrm{span}(\underline{q})$ satisfies $\underline{m}_\xi(W) > \underline{m}_\xi(V)$.*

Proof. Let $a_i = \mathrm{ord}_\xi(q_i)$. The assertion is clear from Lemma 6.9 if $\underline{a} = (a_0, \dots, a_n)$ is weakly decreasing. Otherwise there are indices $i < j$ with $a_i < a_j$. Swap a_i and a_j in $\underline{a}$, then the new sequence $\underline{a}' = (a'_0, \dots, a'_n)$ satisfies the hypothesis in the lemma as well. After finitely many steps we have therefore reduced to Lemma 6.9. □

6.11. For the discussion to follow, fix a linear subspace $V \subseteq A$ of dimension $n+1$. Write $\underline{m} = \underline{m}_\xi(V) = (m_0, \dots, m_n)$ and let $\underline{p} = (p_0, \dots, p_n)$ be a basis of V with $\mathrm{ord}_\xi(p_i) = m_i$ $(i = 0, \dots, n)$. Consider the matrix

$$M = M(\underline{p}) = \big(\varphi_i(p_j)\big)_{0 \le i,j \le n} \tag{7}$$

of size $(n+1) \times (n+1)$ with entries in A_n, together with its determinant

$$F = F(\underline{p}) = \det M(\underline{p}) \in A_n. \tag{8}$$

Note that $\mu_{ij}(F) = 0$ for any pair of indices $0 \le i < j \le n$, since rows i and j of the matrix $\mu_{ij}(M)$ coincide. Therefore F lies in the ideal $\mathcal{I} = \bigcap_{i<j} I_{ij}$. Note also that, up to a nonzero scalar factor in k, the determinant $F = F(\underline{p})$ depends only on V, and not on the choice of the basis $\underline{p}$.

6.12. For $0 \le i \le n$ write $t_i = \varphi_i(t)$ where $t \in A$ is the element fixed in 6.6. Let $J = \langle t_0, \dots, t_n \rangle$, the ideal generated by $t_0, \dots, t_n$ in A_n. By hypothesis (A1), this is the maximal ideal of A_n corresponding to the point $(\xi, \dots, \xi)$ on the diagonal. From 3.1 recall the definition of the Schur polynomial $\sigma_{\underline{m}}(x_0, \dots, x_n)$. By $J(\underline{m})$ we denote the ideal in

A_n that is generated by those monomials $\underline{t}^\alpha = t_0^{\alpha_0} \cdots t_n^{\alpha_n}$ that occur in $\sigma_{\underline{m}}(t_0, \dots, t_n)$ with a nonzero coefficient. Our goal in this section is to arrive at a specific identity for $F = \det(M)$ (Corollary 6.20). The first step is to show:

Proposition 6.13. *$F = F(\underline{p})$ is contained in the ideal product $\mathcal{I} \cdot J(\underline{m})$ (taken in the ring A_n).*

Proof. It suffices to prove the proposition after extension of the base field. We therefore assume that k is algebraically closed (this is just to simplify language and notation). It suffices to argue in the local ring of any given tuple $\underline{\eta} = (\eta_0, \dots, \eta_n) \in C(k)^{n+1}$. Let $\mathcal{O}_{\underline{\eta}} = \mathcal{O}_{C^{n+1},\underline{\eta}}$ be the local ring at $\underline{\eta}$ and let $\widehat{\mathcal{O}}_{\underline{\eta}}$ be its completion. The ring extension $\mathcal{O}_{\underline{\eta}} \subseteq \widehat{\mathcal{O}}_{\underline{\eta}}$ is faithfully flat [4, §8]. This implies that $\mathfrak{a}\widehat{\mathcal{O}}_{\underline{\eta}} \cap \mathcal{O}_{\underline{\eta}} = \mathfrak{a}$ holds for every ideal $\mathfrak{a}$ of $\mathcal{O}_{\underline{\eta}}$ ([4, §7]). To prove $F \in \mathcal{I}J(\underline{m})\mathcal{O}_{\underline{\eta}}$, it suffices therefore to show $F \in \mathcal{I}J(\underline{m})\widehat{\mathcal{O}}_{\underline{\eta}}$.

After a suitable permutation of the components, we may assume that $\eta_0 = \cdots = \eta_r = \xi$ (the point on C fixed in 6.6) and $\eta_i \neq \xi$ for $i = r+1, \dots, n$. Locally at $\underline{\eta}$, the ideal $\mathcal{I}$ is generated by

$$\prod_{i<j \text{ with } \eta_i = \eta_j} \delta_{ij}(t),$$

according to Lemma 6.3 (this uses hypothesis (A2) from 6.6). On the other hand, the element $t \in A$ is a unit in $\mathcal{O}_{C,\xi'}$ for every $\xi' \neq \xi$ in $C(k)$, by hypothesis (A1) in 6.6. Locally at $\underline{\eta}$, this implies that the ideal $J(\underline{m})$ is generated by all monomials $t_0^{e_0} \cdots t_r^{e_r}$ that occur in $\sigma_{\underline{m}}(t_0, \dots, t_r, 1, \dots, 1)$. Proposition 6.13 therefore follows from a repeated application of Lemma 3.5: First apply the lemma to rows $0, \dots, r$ of $M = M(\underline{p})$. Thereby we extract the factor $\prod_{0 \le i < j \le r} \delta_{ij}(t)$ and get a cofactor that is contained in $J(\underline{m})$. Then apply 3.5 successively to the groups of rows whose indices lie in $\{i \colon \eta_i = \omega\}$, for each of the remaining components ω of $\underline{\eta}$. This completes the proof of the lemma: If $i < j$ are indices with $i, j > r$, the factor $\delta_{ij}(t) = t_i - t_j$ is not a zero divisor modulo $J(\underline{m})$ since $J(\underline{m})$ is generated by monomials in $t_0, \dots, t_r$. Therefore $\delta_{ij}(t)G \in J(\underline{m})$ implies $G \in J(\underline{m})$ for $G \in \mathcal{O}$. □

In more explicit terms, Proposition 6.13 states:

Corollary 6.14. *Under the assumptions made in 6.11, there exists an identity*

$$F(\underline{p}) = \sum_{w \in \Lambda} g_w \delta_w \tag{9}$$

in A_n with $g_w \in J(\underline{m})$ for every $w \in \Lambda$. □

Example 6.15. To illustrate the proof of Proposition 6.13 with a concrete example, let $n = 4$ and $\underline{m} = (5, 4, 3, 2, 0)$. So $\underline{p} = (p_0, \dots, p_4)$ is a tuple in A with $\mathrm{ord}_\xi(p_i) = m_i$ for $i = 0, \dots, 4$. The Schur polynomial is

$$\sigma_{\underline{m}}(x) \;=\; x_0x_1x_2x_3 + x_0x_1x_2x_4 + x_0x_1x_3x_4 + x_0x_2x_3x_4 + x_1x_2x_3x_4,$$

the fourth elementary symmetric polynomial in $x_0, \dots, x_4$. Let $\omega \neq \xi$ be a point in $C(k)$. By way of example, let us show that $F = F(\underline{p})$ lies in $\mathcal{I}J(\underline{m})$ locally at $\underline{\eta} = (\xi, \xi, \xi, \omega, \omega) \in C(k)^5$. Let $u = t - t(\omega)$, a local parameter at ω, let $\mathcal{O} = \mathcal{O}_{C^5, \underline{\eta}}$ and let $\widehat{\mathcal{O}}$ be the completion of $\mathcal{O}$. Then $\widehat{\mathcal{O}}$ is identified with the formal power series ring $k[[t_0, t_1, t_2, u_3, u_4]]$. In $\mathcal{O}$, the ideal $J(\underline{m})$ is generated by t_0t_1, t_0t_2, t_1t_2 since t_3, t_4 are units at $\underline{\eta}$. Since $\mathcal{I}$ is generated by $\delta_{01}(t)\delta_{02}(t)\delta_{12}(t)\delta_{34}(t)$ at $\underline{\eta}$, we have to show

$$F \;\in\; (t_0 - t_1)(t_0 - t_2)(t_1 - t_2)(t_3 - t_4) \cdot \langle t_0, t_1, t_2 \rangle$$

in $\widehat{\mathcal{O}}$. By Lemma 3.5(b), F is divisible by $\delta_{01}(t)\delta_{02}(t)\delta_{12}(t)$, and the cofactor G is a power series, each of whose monomials is divisible by a monomial of $\sigma_{\underline{m}}(t_0, t_1, t_2, 1, 1)$. In other words $G \in J(\underline{m})$. On the other hand, F is divisible by $\delta_{34}(u) = t_3 - t_4$ as well (again by 3.5), say $F = (t_3 - t_4)H$. And $G \in J(\underline{m}) = \langle t_0t_1, t_0t_2, t_1t_2 \rangle$ implies $H \in J(\underline{m})$ as well, which completes what we wanted to prove.

6.16. In a second step we are going to refine identity (9). As before, consider a k-basis $\underline{p} = (p_0, \dots, p_n)$ of V with $\mathrm{ord}_\xi(p_i) = m_i$, where $(m_0, \dots, m_n) = \underline{m}_\xi(V) = \underline{m}$. To get rid of inessential constants we scale the p_i in such a way that $\mathrm{ord}_\xi(p_i - t^{m_i}) > m_i$ for $i = 0, \dots, n$. By the normalization made in 6.7, this also implies $\mathrm{ord}_\xi(p_i - w^{m_i}) > m_i$ $(i = 0, \dots, n)$ for every $w \in \Lambda$.

Lemma 6.17. *Let $\underline{q} = (q_0, \dots, q_n)$ be a second tuple in A, and assume that $\mathrm{ord}_\xi(q_i) \geq m_i$ holds for all i, with strict inequality for at least one index i. Then $F(\underline{q}) \in JJ(\underline{m}) \cdot \mathcal{I}$.*

Proof. If $\underline{q}$ is k-linearly dependent there is nothing to show. Otherwise let $W = \mathrm{span}(\underline{q})$ and put $\underline{a} = \underline{m}_\xi(W)$. By Lemma 6.10 we have $\underline{a} > \underline{m}$ and therefore $J(\underline{a}) \subseteq JJ(\underline{m})$ (cf. Lemma 3.3). Applying Proposition 6.13 to W and the sequence $\underline{q}$ gives $F(\underline{q}) \in J(\underline{a})\mathcal{I} \subseteq JJ(\underline{m})\mathcal{I}$, thereby proving the assertion. □

Lemma 6.18. *For each $w \in \Lambda$ we may refine (9) to an identity*

$$F(\underline{p}) \;=\; \sigma_{\underline{m}}(t_0, \dots, t_n)\delta_w + \sum_{v \in \Lambda} g_v \delta_v,$$

where the g_v are elements lying in $JJ(\underline{m})$ for every $v \in \Lambda$.

Proof. Fix $w \in \Lambda$. Then $p_i = w^{m_i} + q_i$ holds with $\mathrm{ord}_\xi(q_i) > m_i$ $(i = 0, \dots, n)$, by the normalization made in 6.16. By multilinearity of the determinant, this implies

$$F(\underline{p}) \;=\; F(w^{m_0}, \dots, w^{m_n}) + \sum_\nu F(\tilde{q}_{\nu 0}, \dots, \tilde{q}_{\nu n})$$

(sum over $2^{n+1}-1$ indices ν) where $\tilde{q}_{\nu i} \in \{w^{m_i}, q_i\}$, and where for each index ν there exists at least one index i with $\tilde{q}_{\nu i} = q_i$. Lemma 6.17 shows that $F(\tilde{q}_{\nu 0}, \dots, \tilde{q}_{\nu n}) \in JJ(\underline{m})\mathcal{I}$ for each ν. This proves the lemma since

$$F(w_0^{m_0}, \dots, w_n^{m_n}) \;=\; \sigma_{\underline{m}}(w_0, \dots, w_n) \cdot \delta_0$$

(bialternant formula (1)) and since

$$\sigma_{\underline{m}}(w_0, \dots, w_n) \;\equiv\; \sigma_{\underline{m}}(t_0, \dots, t_n) \pmod{JJ(\underline{m})}$$

by the assumption made in 6.7. □

Proposition 6.19. *There is an identity* $F(\underline{p}) = \sum_{w\in\Lambda} g_w \delta_w$ *such that* g_w *lies in* $\frac{1}{|\Lambda|}\sigma_{\underline{m}}(t_0, \dots, t_n) + JJ(\underline{m})$ *for every* $w \in \Lambda$.

Proof. For each $w \in \Lambda$ fix an identity

$$F(\underline{p}) \;=\; \sigma_{\underline{m}}(t_0, \dots, t_n)\delta_w + \sum_{v\in\Lambda} g_{wv}\delta_v$$

with $g_{wv} \in JJ(\underline{m})$ for all $v \in \Lambda$, see Lemma 6.18. Adding all these identities and dividing by $|\Lambda|$ gives an identity as asserted. □

Alternatively we may phrase Proposition 6.19 as follows:

Corollary 6.20. *There is an identity*

$$F(\underline{p}) \;=\; \frac{1}{|\Lambda|}\sum_{w\in\Lambda}\sum_{\alpha} t_0^{\alpha_0}\cdots t_n^{\alpha_n}(1+g_{w,\alpha})\cdot\delta_w \tag{10}$$

where the inner sum is taken over all monomials x^α *occurring in* $\sigma_{\underline{m}}(x)$, *and where* $g_{w,\alpha} \in J$ *for all* w *and* α. □

7. Representing the determinant, II

We keep the hypotheses made in 6.6. So C is an irreducible and non-singular affine curve over a field k of characteristic 0, and $\xi \in C(k)$ is a fixed point. The element $t \in A = k[C]$ is a local uniformizer at ξ, and the A-module $\Omega_{C/k}$ is freely generated by dt. For $p \in A$ we keep the notation $p' = \frac{dp}{dt}$, and write $p^{(i)} = \frac{d}{dt}p^{(i-1)}$ $(i \geq 1)$ for the iterated $\frac{d}{dt}$-derivatives.

Recall that $A \otimes A$ is regarded as an A-module via the second tensor component, and that $I \subseteq A \otimes A$ denotes the kernel of the product map $\mu\colon A \otimes A \to A$. The ideal I is generated by the $\delta(p) = p \otimes 1 - 1 \otimes p$ $(p \in A)$. For $r \geq 1$ let I^r denote the r-th ideal power of I. Note that $\alpha\beta \equiv \mu(\alpha)\beta \pmod{I^{r+1}}$ holds for $\alpha \in A \otimes A$ and $\beta \in I^r$.

Lemma 7.1. *For $f \in A$ and every integer $r \geq 1$, the congruence*

$$\delta(f) \equiv f' \cdot \delta(t) + \frac{1}{2!} f'' \cdot \delta(t)^2 + \cdots + \frac{1}{r!} f^{(r)} \cdot \delta(t)^r \pmod{I^{r+1}} \tag{11}$$

holds in $A \otimes A$.

Proof. Let $\Omega = \Omega_{A/k}$. The isomorphism $\Omega \xrightarrow{\sim} I/I^2$, $df \mapsto \delta(f) + I^2$ of A-modules induces isomorphisms $\mathrm{Sym}^d_A(\Omega) \to I^d/I^{d+1}$ for all $d \geq 0$, since the curve C is smooth ([3] 17.12.4, 16.9.4). Since Ω is freely generated by dt, this implies that there exist unique elements $g_1, \ldots, g_r \in A$ such that

$$\delta(f) \equiv g_1 \cdot \delta(t) + \cdots + g_r \cdot \delta(t)^r \pmod{I^{r+1}} \tag{12}$$

holds in $A \otimes A$. Given an arbitrary point $\eta \in C(k)$, consider the homomorphism $\phi_\eta \colon A \otimes A \to A$ defined by $\phi_\eta(p \otimes q) = p \cdot q(\eta)$. Then $\phi_\eta(I) = \mathfrak{m}_\eta$, so applying ϕ_η to (12) gives

$$f - f(\eta) \equiv g_1(\eta) \cdot (t - t(\eta)) + \cdots + g_r(\eta) \cdot (t - t(\eta))^r \pmod{\mathfrak{m}_\eta^{r+1}}.$$

Since $t - t(\eta)$ is a uniformizing element at η (Lemma 6.3) it follows that $g_i(\eta) = \frac{1}{i!} f^{(i)}(\eta)$ for $i = 1, \ldots, r$. This proves the lemma. □

Lemma 7.2. *For every $r \geq 1$ there exists a (unique) well-defined A-linear map $D^{(r)} \colon I^r \to A$ that satisfies $D^{(r)}(I^{r+1}) = 0$ and sends $\delta(p_1) \cdots \delta(p_r)$ to $p_1' \cdots p_r'$, for any $p_1, \ldots, p_r \in A$. This map satisfies $D^{(r)}(\alpha\beta) = \mu(\alpha) D^{(r)}(\beta)$ for $\alpha \in A \otimes A$ and $\beta \in I^r$.*

Proof. The graded A-algebra $\bigoplus_{r \geq 0} I^r/I^{r+1}$ is the symmetric algebra over the A-module I/I^2, see the previous proof. Since I/I^2 is freely generated by $dt = \delta(t) + I^2$, there is a unique homomorphism of A-algebras $D \colon \bigoplus_{r \geq 0} I^r/I^{r+1} \to A$ with $D(dt) = 1$. Let $D^{(r)} \colon I^r \to A$ be the induced A-linear map for $r \geq 0$, so $D^{(r)}(\beta) = D(\beta + I^{r+1})$ for $\beta \in I^r$. We claim that $D^{(r)}$ has the above properties. For $a, b \in A$ one has $D^{(r)}((a \otimes b)\beta) = ab \cdot D^{(r)}(\beta)$ by A-linearity, since $a \otimes b \equiv 1 \otimes ab \pmod{I}$. For $p \in A$ we have $dp = p'\, dt$ by definition of p', which means $\delta(p) \equiv p' \delta(t) \pmod{I}$. This implies $D^{(1)}(\delta(p)) = p'$. Consequently, $D^{(r)}$ maps $\delta(p_1) \cdots \delta(p_r)$ to $p_1' \cdots p_r'$ ($r \geq 1$) since D is a ring homomorphism. □

7.3. In the tensor product $A_n = A^{\otimes(n+1)}$ we may perform the operations $D^{(r)}$ on any fixed pair $i < j$ of indices. Recall that I_{ij} denotes the kernel of $\mu_{ij} \colon A_n \to A_n$ and is generated by the $\delta_{ij}(a)$ ($a \in A$) as an ideal in A_n. For $0 \leq i < j \leq n$ let

$$D^{(r)}_{ij} \colon I^r_{ij} \to A_n$$

be the additive map that satisfies

$$D_{ij}^{(r)}\big(\alpha\,\delta_{ij}(a_1)\cdots\delta_{ij}(a_r)\big) \;=\; \mu_{ij}(\alpha)\cdot\varphi_i(a_1'\cdots a_r') \tag{13}$$

for $a_1,\dots,a_r \in A$ and $\alpha \in A_n$. The unique existence of a map with these properties follows directly from 7.2. For any $p \in A$ and any $r \geq 1$, note that

$$D_{ij}^{(r)}\left(\delta_{ij}(p) - \sum_{\nu=1}^{r-1}\frac{\varphi_j(p^{(\nu)})}{\nu!}\delta_{ij}(t)^\nu\right) \;=\; \frac{1}{r!}\varphi_i(p^{(r)}), \tag{14}$$

by Lemma 7.1.

7.4. As in Section 6, let $\underline{p} = (p_0,\dots,p_n)$ be a fixed $(n+1)$-tuple of elements in A, and consider the matrix $M = M(\underline{p}) = \big(\varphi_i(p_j)\big)_{0\leq i,j\leq n}$ over A_n, see 6.11. If $k \geq 0$, write $\underline{p}^{(k)} = (p_0^{(k)},\dots,p_n^{(k)})$ for the tuple of k-th $\frac{d}{dt}$-derivatives. Fix an integer $1 \leq b \leq n+1$ and a block B of b consecutive numbers in $\{0,\dots,n\}$; for simplicity we take $B = \{0,\dots,b-1\}$. In the following we describe a transformation of the matrix M to a new matrix $\mathcal{T}_B M$, to which we'll refer as the *Taylor process on* B.

Start with the matrix M and let $z_i(M) = \varphi_i(\underline{p})$ denote the i-th row of M ($i = 0,\dots,n$). Replacing $z_1(M)$ with $z_1(M) - z_0(M)$, this new row lies entrywise in I_{01}, so we can apply $D_{01}^{(1)}$ to it. Leaving the other rows unchanged, this gives the new matrix M' with rows

$$\varphi_0(\underline{p}),\ -\varphi_0(\underline{p}'),\ \varphi_2(\underline{p}),\ \dots,\ \varphi_n(\underline{p}).$$

Since the determinant is multilinear with respect to the rows, the determinant of M' satisfies

$$\det(M') \;=\; D_{01}^{(1)}(\det M)$$

by (13). Next replace $z_2(M') = \varphi_2(\underline{p})$ with

$$z_2(M') - z_0(M') - \delta_{02}(t)z_1(M') \;=\; \varphi_2(\underline{p}) - \varphi_0(\underline{p}) - (t_2 - t_0)\varphi_0(\underline{p}').$$

Entrywise, this row lies in I_{02}^2 and is congruent to $\frac{1}{2}\varphi_0(\underline{p}'')\delta_{02}(t)^2$ modulo I_{03}^3, both by Lemma 7.1. Apply $D_{02}^{(2)}$ to this row, to get the new matrix M'' with rows

$$\varphi_0(\underline{p}),\ -\varphi_0(\underline{p}'),\ \frac{1}{2}\varphi_0(\underline{p}''),\ \varphi_3(\underline{p}),\ \dots,\ \varphi_n(\underline{p}),$$

whose determinant satisfies

$$\det(M'') \;=\; D_{02}^{(2)}(\det M') \;=\; D_{02}^{(2)} \circ D_{01}^{(1)}(\det M). \tag{15}$$

Keep proceeding in this way, successively working down the rows in the block B. After $b-1$ steps we have arrived at a matrix $\mathcal{T}_B M = M^{(b-1)}$ with rows

$$\varphi_0(\underline{p}),\ -\varphi_0(\underline{p}'),\ \ldots,\ \frac{(-1)^{b-1}}{(b-1)!}\varphi_0(\underline{p}^{(b-1)}),\ \varphi_b(\underline{p}),\ \ldots,\ \varphi_n(\underline{p}) \tag{16}$$

whose determinant satisfies

$$\det(\mathcal{T}_B M) \;=\; D^{(b-1)}_{0,b-1}\circ\cdots\circ D^{(1)}_{01}(\det M). \tag{17}$$

7.5. Fix an identity $\det(M)=\sum_{w\in\Lambda} g_w\delta_w$ for the determinant of M, with $g_w\in J(\underline{m})$ (Corollary 6.14). How does the Taylor process just described act on the terms of this identity? Write $\mathcal{D}_B := D^{(b)}_{0b}\circ\cdots\circ D^{(1)}_{01}$ for the composite operator (it is defined on $\bigcap_{j=1}^b I_{0j}$), and let $\boldsymbol{\mu}_B=\mu_{0b}\circ\cdots\circ\mu_{01}\colon A_n\to A_n$ denote the ring homomorphism

$$\boldsymbol{\mu}_B\big(a_0\otimes\cdots\otimes a_n\big) \;=\; (a_0\cdots a_{b-1})\otimes\underbrace{1\otimes\cdots\otimes 1}_{b-1\text{ times}}\otimes a_b\otimes\cdots\otimes a_n.$$

Then $\mathcal{D}_B(g\delta_w)=\boldsymbol{\mu}_B(g)\mathcal{D}_B(\delta_w)$ for $g\in A_n$ and $w\in A$, where

$$\mathcal{D}_B(\delta_w) \;=\; \varphi_0(w')^{b(b-1)/2}\cdot\prod_{b\le j\le n}\delta_{0j}(w)^b\cdot\prod_{b\le i<j\le n}\delta_{ij}(w). \tag{18}$$

Note that the entries of the matrix $\mathcal{T}_B M = M^{(b-1)}$ (and its determinant) lie in the subring

$$A\otimes\underbrace{k\otimes\cdots\otimes k}_{b-1\text{ times}}\otimes\underbrace{A\otimes\cdots\otimes A}_{n-b+1\text{ times}}$$

of A_n.

7.6. As a final step we apply the Taylor process 7.4 to several disjoint blocks of rows of the matrix $M=M(\underline{p})$, as follows. We assume that the rows $0,\ldots,n$ of the matrix have been grouped into blocks $B_0,\ldots,B_r$ of consecutive rows, with B_ν consisting of b_ν many rows for $\nu=0,\ldots,r$. More formally, let $\underline{b}=(b_0,\ldots,b_r)$ be a tuple of integers $b_i\ge 1$ with $n+1=\sum_{i=0}^r b_i$, and let $B_0=\{0,\ldots,b_0-1\}$, $B_1=\{b_0,\ldots,b_0+b_1-1\}$ etc, up to $B_r=\{n-b_r+1,\ldots,n\}$. For each of the blocks $B_0,\ldots,B_r$ perform the Taylor process 7.4 on the rows of this block. In the end we have arrived at a matrix $T=T_{\underline{b}}(\underline{p})$ whose coefficients lie in the subring

$$\big(A\otimes\underbrace{k\otimes\cdots\otimes k}_{(b_0-1)\text{ times}}\big)\otimes\cdots\otimes\big(A\otimes\underbrace{k\otimes\cdots\otimes k}_{(b_r-1)\text{ times}}\big)$$

of A_n. Dropping the inessential tensor components we consider T to have coefficients in $A_r=A^{\otimes(r+1)}$. With this convention, the rows of T are

$$\varphi_0(\underline{p}),\ \ldots,\ \varphi_0(\underline{p}^{(b_0-1)}),\ \ldots,\ \varphi_r(\underline{p}),\ \ldots,\ \varphi_r(\underline{p}^{(b_r-1)}) \tag{19}$$

up to nonzero scalar factors in k, see 7.4. In order to describe the effect of the multiple Taylor process on the determinant, let $\boldsymbol{\mu} = \boldsymbol{\mu}_{\underline{b}}\colon A_n \to A_r$ denote the ring homomorphism that puts the product of the tensor components in block B_ν at position ν, for $\nu = 0, \dots, r$:

$$\boldsymbol{\mu}(a_0 \otimes \cdots \otimes a_n) \;=\; \Big(\prod_{i \in B_0} a_i\Big) \otimes \cdots \otimes \Big(\prod_{i \in B_r} a_i\Big). \tag{20}$$

Writing $\mathcal{D} = \mathcal{D}_{B_r} \circ \cdots \circ \mathcal{D}_{B_0}$ we have $\mathcal{D}(g\delta_w) = \boldsymbol{\mu}(g)\mathcal{D}(\delta_w)$ for $g \in A_n$ and $w \in \Lambda$, where

$$\mathcal{D}(\delta_w) \;=\; \prod_{i=0}^{r} \varphi_i(w')^{b_i(b_i-1)/2} \cdot \prod_{0 \le i < j \le r} \delta_{ij}(w)^{b_i b_j}. \tag{21}$$

If we start with an identity

$$\det(M) \;=\; \frac{1}{|\Lambda|} \sum_{w,\alpha} t_0^{\alpha_0} \cdots t_n^{\alpha_n} (1 + g_{w,\alpha}) \cdot \delta_w \tag{22}$$

as in Corollary 6.20, we therefore get

$$\det T_{\underline{b}}(\underline{p}) \;=\; \frac{1}{|\Lambda|} \sum_{w,\alpha} t_0^{\alpha(B_0)} \cdots t_r^{\alpha(B_r)} \cdot (1 + \boldsymbol{\mu}(g_{w,\alpha})) \cdot \mathcal{D}(\delta_w) \tag{23}$$

with $\alpha(B_\nu) = \sum_{j \in B_\nu} \alpha_j$ for $\nu = 0, \dots, r$.

In summary, the previous discussion gives the following result:

Theorem 7.7. *Let $b_0, \dots, b_r \ge 1$ with $\sum_{i=0}^{r} b_i = n+1$, and consider the $(n+1) \times (n+1)$ matrix $T_{\underline{b}}(\underline{p})$ over A_r with rows*

$$\varphi_0(\underline{p}),\; \dots,\; \varphi_0(\underline{p}^{(b_0-1)}),\; \dots,\; \varphi_r(\underline{p}),\; \dots,\; \varphi_r(\underline{p}^{(b_r-1)}). \tag{24}$$

Its determinant $\det T_{\underline{b}}(\underline{p})$ can be written

$$\sum_{w,\alpha} \Big(\boldsymbol{\mu}(t^\alpha) \cdot (1 + h_{w,\alpha}) \cdot \prod_{0 \le i \le r} \varphi_i(w')^{b_i(b_i-1)/2} \cdot \prod_{0 \le i < j \le r} \delta_{ij}(w)^{b_i b_j} \Big), \tag{25}$$

up to a scaling factor in k^*. Here the $h_{w,\alpha}$ lie in $\langle t_0, \dots, t_r \rangle$, and the sum is over $w \in \Lambda$ and those multiindices $\alpha = (\alpha_0, \dots, \alpha_n)$ for which x^α occurs in the Schur polynomial $\sigma_{\underline{m}}(x_0, \dots, x_n)$. □

Given a k-algebra $\mathcal{A}$ together with k-homomorphisms $\psi_i\colon A \to \mathcal{A}$ $(i = 0, \dots, r)$, we may specialize the matrix $T_{\underline{b}}(\underline{p})$ over A_r to a matrix over $\mathcal{A}$ via

$$\psi\colon A_r \to \mathcal{A}, \quad a_0 \otimes \cdots \otimes a_r \mapsto \psi_0(a_0) \cdots \psi_r(a_r).$$

Several specializations of this sort will play a role in the sequel. We begin with the following one:

Proposition 7.8. *Let $p_0, \dots, p_n$ be a basis of the vector space $V \subseteq A$, let $\underline{\eta} = (\eta_1, \dots, \eta_r)$ be a tuple of r pairwise different points in $C(k)$, and let $\underline{b} = (b_1, \dots, b_r)$ be an r-tuple of positive integers with $\sum_{i=1}^r b_i = n$. The following conditions are equivalent:*

(i) *The matrix*

$$Z_{\underline{b}}(\underline{p}, \underline{\eta}) = \begin{pmatrix} p_0 & \cdots & p_n \\ p_0(\eta_1) & \cdots & p_n(\eta_1) \\ \vdots & & \vdots \\ p_0^{(b_1-1)}(\eta_1) & \cdots & p_n^{(b_1-1)}(\eta_1) \\ \vdots & & \vdots \\ p_0(\eta_r) & \cdots & p_n(\eta_r) \\ \vdots & & \vdots \\ p_0^{(b_r-1)}(\eta_r) & \cdots & p_n^{(b_r-1)}(\eta_r) \end{pmatrix} \tag{26}$$

(of size $(n+1) \times (n+1)$ and with coefficients in A) has non-zero determinant;

(ii) *the subspace $V_0 := \bigcap_{i=1}^r \{f \in V : \operatorname{ord}_{\eta_i}(f) \ge b_i\}$ of V has dimension one.*

When (i) and (ii) hold, the regular function $\det Z_{\underline{b}}(\underline{p}, \underline{\eta})$ on C (is non-zero and) lies in V_0.

Proof. Put $Z := Z_{\underline{b}}(\underline{p}, \underline{\eta})$. Regardless of condition (i), the subspace V_0 in (ii) has $\dim(V_0) \ge 1$ since V_0 is described by n linear conditions on f. Let Z_0 be the matrix that is obtained from Z by deleting the top row. Then Z_0 is the matrix of the linear map $\phi\colon V \to k^n$,

$$p \mapsto \left(p(\eta_1), \dots, p^{(b_1-1)}(\eta_1), \dots, p(\eta_r), \dots, p^{(b_r-1)}(\eta_r)\right)$$

with respect to the basis $p_0, \dots, p_n$ of V. By definition, V_0 is the kernel of ϕ. The determinant $\det(Z)$ is an element of V which is non-zero if, and only if, at least one of the $n \times n$-minors of Z_0 does not vanish. This is equivalent to ϕ being surjective, and hence also to condition (ii). To see the last assertion note that, for any $k \ge 0$, the k-th derivative $\frac{d^k}{dt^k} \det(Z)$ of $\det(Z)$ is obtained by replacing the top row of Z with $(p_0^{(k)}, \dots, p_n^{(k)})$. Therefore, the vanishing order of $\det(Z)$ at η_i is at least b_i, for every $i = 1, \dots, r$. □

In the next section we are going to specialize the matrix $T_{\underline{b}}(\underline{p})$ in several other ways, to complete the proof of the main theorem.

8. Proof of the main theorem

8.1. After the extensive preparations in the previous sections we can now give the proof of the main theorem. Assume that an affine algebraic curve C over $\mathbb{R}$ is given that is non-singular and irreducible, together with an $\mathbb{R}$-linear subspace V of $A = \mathbb{R}[C]$ of dimension $n+1$. Moreover let $\xi \in C(\mathbb{R})$ be a fixed real point of C, together with a local orientation of the curve $C(\mathbb{R})$ at ξ. We assume that $t \in A$ represents the given orientation and is such that $\Omega_{A/\mathbb{R}}$ is freely generated by dt, and such that $\mathfrak{m}_\xi = At$ (conditions (A1) and (A2) from 6.6). We need to prove the following (see 2.5, 2.9):

(∗) There exists a closed interval $S = [\xi, \xi']$ in $C(\mathbb{R})$ on the positive side of ξ for which the following is true: For every real closed field $R \supseteq \mathbb{R}$, every element $f \in V_R = V \otimes R$ with $f \ge 0$ on $S_R \subseteq C(R)$ and every $\xi_0 \in S_R$, the tensor evaluation (see 2.7) of f at ξ_0 satisfies

$$\operatorname{sosx} f^{\otimes}(\xi_0) \;\le\; 1 + \lfloor \frac{n}{2} \rfloor.$$

It suffices in fact to show this for every f that spans an extreme ray of the cone $(P_{V,S})_R = \{g \in V_R \colon g \ge 0 \text{ on } S_R\}$.

See 2.4 for the meaning of interval in this context.

8.2. We may assume that ξ is not a base point of V, i.e., that there is $p \in V$ with $p(\xi) \ne 0$. Indeed, let $e = \min\{\operatorname{ord}_\xi(p) \colon p \in V\}$. Then $V = t^e V_1$ where $V_1 = \{t^{-e} p \colon p \in V\}$ is contained in A since $\mathfrak{m}_\xi = At$. Now ξ isn't a base point of V_1 any more, and multiplication by t^e is a linear isomorphism $V_1 \to V$ that identifies $P_{V_1,S}$ with $P_{V,S}$ for every interval $S \subseteq C(\mathbb{R})$ on which t is non-negative. So we may replace V with V_1.

8.3. As in Sections 6 and 7 let $\underline{m} = \underline{m}_\xi(V)$, and let $\underline{p} = (p_0, \dots, p_n)$ be an $\mathbb{R}$-basis of V with $\operatorname{ord}_\xi(p_i) = m_i$ $(i = 0, \dots, n)$. To find an interval S as in 8.1, form the matrix $M = M(\underline{p})$ over $A_n = A^{\otimes(n+1)}$ as in 6.11. Let $\sigma_{\underline{m}}(x_0, \dots, x_n)$ be the Schur polynomial associated with the sequence $\underline{m} = (m_0, \dots, m_n)$, see 3.1, and fix a finite set $\Lambda \subseteq A$ of elements w as in 6.7. The ideal $\mathcal{I}$ in A_n is generated by the δ_w $(w \in \Lambda)$, and each $w \in \Lambda$ satisfies $\operatorname{ord}_\xi(w) = 1$ and $\frac{dw}{dt}(\xi) = 1$. Then, according to Corollary 6.20, there is an identity

$$\det M(\underline{p}) \;=\; \frac{1}{|\Lambda|} \sum_{w,\alpha} t_0^{\alpha_0} \cdots t_n^{\alpha_n} (1 + g_{w,\alpha}) \cdot \delta_w \tag{27}$$

in A_n as in (10). In particular, the element $g_{w,\alpha}$ lies in $J = \langle t_0, \dots, t_n \rangle$ for every pair w, α. (Recall that the sum is over $w \in \Lambda$ and the monomials x^α in $\sigma_{\underline{m}}(x)$.)

From now on fix one such identity (27). Considering the finitely many elements $g_{w,\alpha} \in J \subseteq A_n$ as polynomial functions on $C^{n+1} = C \times \cdots \times C$, they all vanish in the diagonal point $(\xi,\dots,\xi)$. So there exists an open neighborhood Q of ξ in $C(\mathbb{R})$ with the property that $1+g_{w,\alpha}(\eta_0,\dots,\eta_n)>0$ for all $\eta_0,\dots,\eta_n\in Q$ and all w,α. Choose the non-degenerate interval $S=[\xi,\xi']$ in such a way that S contains the positive side of ξ, and such that the following hold:

(S0) V has no base point in S,
(S1) $S\subseteq Q$,
(S2) $t\ge 0$ on S,
(S3) $w'=\frac{dw}{dt}\ge 0$ on S (and hence also $w\ge 0$ on S), for every $w\in\Lambda$.

Clearly it is possible to find such an interval S, given that ξ is not a base point of V (see 8.2). We claim that $(*)$ in 8.1 is satisfied for such S.

8.4. Let $R\supseteq\mathbb{R}$ be a real closed field extension, let $f\in V_R$ with $f\ge 0$ on S_R and assume that f spans an extreme ray of $(P_{V,S})_R$. If $f(\xi)=0$ we may pass from V to the linear system $V_0=\{p\in V\colon p(\xi)=0\}$. Then $\dim(V)=n<n+1$ since ξ is not a base point of V, and by induction we may assume this case already to be covered. Argueing similarly in case $f(\xi')=0$, we may therefore assume that $f(\xi)>0$ and $f(\xi')>0$. This implies that the number of zeros of f in S_R is even, counting with multiplicities. By Corollary 4.4, this number is at least n. We claim that it is equal to n (and therefore, that n is even). To see this, consider the following lemma:

Lemma 8.5. *With S as in 8.3, assume that $\xi_0,\dots,\xi_r\in S_R$ are pairwise different and also different from ξ. Let integers $b_0,\dots,b_r\ge 1$ with $\sum_{i=0}^r b_i=n+1$ be given. Then the determinant of the matrix*

$$\begin{pmatrix} p_0(\xi_0) & \cdots & p_n(\xi_0)\\ \vdots & & \vdots\\ p_0^{(b_0-1)}(\xi_0) & \cdots & p_n^{(b_0-1)}(\xi_0)\\ \vdots & & \vdots\\ p_0(\xi_r) & \cdots & p_n(\xi_r)\\ \vdots & & \vdots\\ p_0^{(b_r-1)}(\xi_r) & \cdots & p_n^{(b_r-1)}(\xi_r)\end{pmatrix} \tag{28}$$

is a nonzero element of R.

Proof. On the interval S, each $w\in\Lambda$ is strictly increasing as a function of t, by hypothesis (S3) in (27). So we may label the ξ_i in such a way that

$$w(\xi_0)\;>\;w(\xi_1)\;>\;\cdots\;>\;w(\xi_r)$$

for each $w \in \Lambda$. Consider the matrix $T_{\underline{b}}(\underline{p})$ over A_r from Theorem 7.7, with parameters $\underline{b} = (b_0, \dots, b_r)$ as given above. The matrix (28) is the image of $T_{\underline{b}}(\underline{p})$ under the ring homomorphism

$$A_r \to R, \quad a_0 \otimes \cdots \otimes a_r \mapsto \prod_{i=0}^{r} a_i(\xi_i) \tag{29}$$

Hence the determinant of (28) is the image of the sum (25) under this ring homomorphism. But from conditions (S0)–(S3) it follows that every factor in a typical summand

$$\boldsymbol{\mu}(t^\alpha) \cdot (1 + h_{w,\alpha}) \cdot \prod_i \varphi_i(w')^{b_i(b_i-1)/2} \cdot \prod_{i<j} \delta_{ij}(w)^{b_i b_j}$$

of (25) maps to a *strictly positive* number in R under (29). This proves the lemma. □

Proposition 8.6. *f as in 8.4 has precisely n zeros ($\neq \xi, \xi'$) in S_R, counting with multiplicities. In particular, n is even.*

Proof. Assume to the contrary that f has at least $n+1$ zeros in S_R (different from ξ, ξ'). Then there are $\xi_0, \dots, \xi_r \in S_R$, pairwise different, together with integers $b_0, \dots, b_r \geq 1$ such that $\mathrm{ord}_{\xi_i}(f) \geq b_i \geq 1$ for $i = 0, \dots, r$ and $\sum_{i=0}^{r} b_i = n + 1$. By Lemma 8.5, the determinant of the matrix (28) is nonzero. Choose an arbitrary element $q \in A$ that is linearly independent from $p_0, \dots, p_n$. Consider the extended tuple $\underline{\tilde{p}} = (q, p_0, \dots, p_n)$ and form the matrix of size $(n+2) \times (n+2)$ over A with rows

$$\underline{\tilde{p}},\ \underline{\tilde{p}}(\xi_0), \dots, \underline{\tilde{p}}^{(b_0-1)}(\xi_0),\ \dots,\ \underline{\tilde{p}}(\xi_r), \dots, \underline{\tilde{p}}^{(b_r-1)}(\xi_r)$$

Deletion of row 0 and column 0 in this matrix gives back the matrix (28), whose determinant is $\neq 0$. By Proposition 7.8, therefore, the unique element (up to scaling) in $V_R \oplus Rq = \mathrm{span}(\underline{\tilde{p}})_R$ with at least the given zeros is this determinant, and it is not contained in V_R. But by assumption, $f \in V_R$ is another nonzero element with at least these zeros, contradicting uniqueness and thereby proving Proposition 8.6. □

8.7. Let f span an extreme ray in $(P_{V,S})_R$, with f as in 8.4. As was just proved, n is even and f has precisely n zeros in S_R. Let these be $\xi_1, \dots, \xi_r$, pairwise different, with respective (even) multiplicities $b_1, \dots, b_r \geq 2$, so $\sum_{i=1}^{r} b_i = n$. Write $\underline{b} = (b_1, \dots, b_r)$ and $\underline{\xi} = (\xi_1, \dots, \xi_r)$ and form the matrix $Z = Z_{\underline{b}}(\underline{p}, \underline{\xi})$ over $A_R = A \otimes R$ as in (26), with rows

$$\underline{p},\ \underline{p}(\xi_1),\ \dots,\ \underline{p}^{(b_1-1)}(\xi_1),\ \dots,\ \underline{p}(\xi_r),\ \dots,\ \underline{p}^{(b_r-1)}(\xi_r).$$

The determinant $\det(Z)$ is an element of V_R with at least the same zeros in S_R as f. Choose any $\xi_0 \in S_R$ that is not in $\{\xi, \xi_1, \dots, \xi_r\}$. Then $\det(Z)$, evaluated at ξ_0, is nonzero by Lemma 8.5, showing in particular that $\det(Z)$ is not identically zero. By

Proposition 7.8, therefore, $f = c\cdot\det(Z)$ with some nonzero scalar $c \in R$. For calculating sosx $f^{\otimes}(\xi_0)$ with $\xi_0 \in S_R$, we may assume $f = \det(Z)$.

Consider the matrix $T = T_{(1,\underline{b})}(\underline{p})$ with $(1,\underline{b}) := (1, b_1, \dots, b_r)$, see (19). So the blocks for the Taylor process are

$$B_0 = \{0\},\ B_1 = \{1, \dots, b_1\},\ B_2 = \{b_1 + 1, \dots, b_1 + b_2\} \text{ etc}, \tag{30}$$

and T is the $(n + 1) \times (n + 1)$ matrix over A_r with rows

$$\varphi_0(\underline{p}),\ \varphi_1(\underline{p}),\ \dots,\ \varphi_1(\underline{p}^{(b_1-1)}),\ \dots,\ \varphi_r(\underline{p}),\ \dots,\ \varphi_r(\underline{p}^{(b_r-1)}),$$

up to nonzero scalar factors in $\mathbb{R}$. The matrix Z arises from T by applying the homomorphism

$$A_r \mapsto A \otimes R, \quad a_0 \otimes \cdots \otimes a_r \ \mapsto\ a_0 \otimes \big(a_1(\xi_1) \cdots a_r(\xi_r)\big). \tag{31}$$

By definition, the tensor evaluation of f in $\xi_0 \in S_R$ is the image of $f = \det(Z) \in A \otimes R$ under

$$A \otimes R \to R \otimes R, \quad q \otimes a \mapsto q(\xi_0) \otimes a. \tag{32}$$

So altogether, $f^{\otimes}(\xi_0)$ is the image of $\det(T) \in A_r$ under the ring homomorphism $A_r \to R \otimes R$,

$$a_0 \otimes \cdots \otimes a_n \ \mapsto a_0(\xi_0) \otimes \big(a_1(\xi_1) \cdots a_r(\xi_r)\big). \tag{33}$$

8.8. Theorem 7.7 gives an expression (25) for $\det(T)$, from which we get $f^{\otimes}(\xi_0)$ by applying the homomorphism (33) to the summands. Taking a typical summand

$$\boldsymbol{\mu}(t^\alpha) \cdot (1 + h_{w,\alpha}) \cdot \prod_{0\le i\le r} \varphi_i(w')^{b_i(b_i-1)/2} \cdot \prod_{0\le i<j\le r} \delta_{ij}(w)^{b_i b_j} \tag{34}$$

in (25), let us discuss its image under (33), factor by factor:

- $\boldsymbol{\mu}(t^\alpha) = \boldsymbol{\mu}(t_0^{\alpha_0} \cdots t_n^{\alpha_n})$ is mapped to

  $$t(\xi_0)^{\alpha_0} \otimes \Big(t(\xi_1)^{\alpha(B_1)} \cdots t(\xi_r)^{\alpha(B_r)}\Big)$$

  (with $B_1, \dots, B_r$ as in (30) and $\alpha(B_\nu) = \sum_{i\in B_\nu} \alpha_i$). By (S2) in 8.3, this is a tensor in $R \otimes R$ of the form $a_1 \otimes a_2$ with $a_1,\ a_2 \ge 0$.
- Let $\mathcal{O}$ be the convex hull of $\mathbb{R}$ in R, a valuation ring of R with residue field $\mathbb{R}$. Let moreover $\omega \mapsto \overline{\omega}$ denote the natural residue map $\mathcal{O} \otimes \mathcal{O} \to \mathbb{R}$. The factor $1 + h_{w,\alpha}$ in (25) is mapped to an element $\omega \in \mathcal{O} \otimes \mathcal{O}$ for which $\overline{\omega} > 0$ in $\mathbb{R}$, by (S1) in 8.3. Such ω satisfies $\text{sosx}(\omega) = 1$, according to [7, Prop. 3.5].

- $\varphi_i(w')$ is mapped to $w'(\xi_0)\otimes 1$ (for $i=0$) or to $1\otimes w'(\xi_i)$ (for $1\le i\le r$), respectively. In either case, $w'(\xi_i)\ge 0$ by (S3) in 8.3.
- For $1\le i<j\le r$, $\delta_{ij}(w)^{b_ib_j}$ is mapped to an element $1\otimes a$ with $a>0$, since b_ib_j is even.
- *The critical factor is* $\prod_{j=1}^r \delta_{0j}(w)^{b_j}$. Under (33) it is mapped to

$$\prod_{j=1}^{r}\Big(w(\xi_0)\otimes 1-1\otimes w(\xi_j)\Big)^{b_j}. \tag{35}$$

  Since $b_1,\dots,b_r$ are even numbers with $\sum_{j=1}^r b_j=n$, this is the square of a product of $\frac{n}{2}$ factors, each of the form $w(\xi_0)\otimes 1-1\otimes c_i$ with $c_i\in R$ ($i=1,\dots,\frac{n}{2}$). Therefore, (35) is equal to $(a_0\otimes b_0+\cdots+a_{n/2}\otimes b_{n/2})^2$ with $a_\nu,\,b_\nu\in R$. In particular, the tensor (35) has sosx $\le 1+\frac{n}{2}$.

All factors in the preceding list, except for the last, have sosx ≤ 1. Their product therefore has sosx $\le 1+\frac{n}{2}$, see [7, Lemma 3.4(c)]. Since this holds for every summand w,α, it follows that

$$\operatorname{sosx} f^{\otimes}(\xi_0)\ \le\ 1+\frac{n}{2},$$

which finally completes the proof of the main theorem. □

Data availability

No data was used for the research described in the article.

References

[1] G. Averkov, Optimal size of linear matrix inequalities in semidefinite approaches to polynomial optimization, SIAM J. Appl. Algebra Geom. 3 (2019) 128–151.
[2] G. Averkov, C. Scheiderer, Convex hulls of monomial curves, and a sparse positivstellensatz, Math. Program., Ser. A 209 (2025) 113–131, https://doi.org/10.1007/s10107-024-02060-9.
[3] A. Grothendieck, Éléments de géométrie algébrique IV, Quatrième partie, Publ. Math. IHÉS 32 (1967) 5–361.
[4] H. Matsumura, Commutative Ring Theory, Cambridge University Press, Cambridge, 1987.
[5] C. Scheiderer, Semidefinite representation for convex hulls of real algebraic curves, SIAM J. Appl. Algebra Geom. 2 (2018) 1–25.
[6] C. Scheiderer, Spectrahedral shadows, SIAM J. Appl. Algebra Geom. 2 (2018) 26–44.
[7] C. Scheiderer, Second-order cone representation for convex sets in the plane, SIAM J. Appl. Algebra Geom. 5 (2021) 114–139.
[8] C. Scheiderer, A Course in Real Algebraic Geometry. Positivity and Sums of Squares, Graduate Texts in Mathematics, vol. 303, Springer Nature, Cham, 2024.
[9] R. Stanley, Enumerative Combinatorics, vol. 2, Cambridge Studies in Advanced Mathematics, vol. 62, 2011.