Rev. Mat. Iberoam. **31** (2015), no. 1, 291–302
DOI 10.4171/RMI/834

Interpolation of ideals

Martín Avendano and Jorge Ortigas-Galindo

Abstract. Let $\mathbb{K}$ denote an algebraically closed field. We study the relation between an ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ and its cross sections $I_\alpha = I + \langle x_1 - \alpha \rangle$. In particular, we study under what conditions I can be recovered from the set $I_S = \{(\alpha, I_\alpha) : \alpha \in S\}$ with $S \subseteq \mathbb{K}$. For instance, we show that an ideal $I = \bigcap_i Q_i$, where Q_i is primary and $Q_i \cap \mathbb{K}[x_1] = \{0\}$, is uniquely determined by I_S when $|S| = \infty$. Moreover, there exists a function $B(\delta, n)$ such that, if I is generated by polynomials of degree at most δ, then I is uniquely determined by I_S when $|S| \geq B(\delta, n)$. If I is also known to be principal, the reconstruction can be made when $|S| \geq 2\delta$, and in this case, we prove that the bound is sharp.

1. Introduction

Throughout this paper $\mathbb{K}$ will be an algebraically closed field. The main result regarding univariate polynomial interpolation states that for any given $d+1$ points $\{(\alpha_i, \beta_i) \in \mathbb{K}^2 \colon i = 1, \ldots, d+1\}$ there exists a unique polynomial $p \in \mathbb{K}[x]$ of degree less than or equal to d such that $f(\alpha_i) = \beta_i$ for $i = 1, \ldots, d+1$. The uniqueness part of this statement says that a planar algebraic curve $\mathcal{C} = \{(x, y) \in \mathbb{K}^2 \colon y = p(x)\}$ of degree at most d is uniquely determined by its intersection with $d+1$ parallel lines $\{x = \alpha_i\}$. In this paper we study generalizations of this fact to higher dimensions, i.e., we study under what conditions it is possible to recover an algebraic variety $V \subseteq \mathbb{K}^n$ from its intersection with parallel hyperplanes. We also consider the algebraic counterpart of the problem, i.e., under what conditions it is possible to recover an ideal $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ from some cross sections $I + \langle x_1 - \alpha \rangle$. Our first result studies the simplest situation, when all the cross sections are known:

Theorem 1.1. *Let $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ be an ideal. Then:*

(a) $\sqrt{I} = \bigcap_{\alpha \in \mathbb{K}} \sqrt{I + \langle x_1 - \alpha \rangle}$.

Mathematics Subject Classification (2010): 14Q15, 13P99.
Keywords: Polynomial interpolation, ideals, complexity.

(b) $I = \bigcap_{\alpha\in\mathbb{K}} \bigcap_{k\geq 1} I + \langle x_1 - \alpha\rangle^k$.

For radical ideals $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$, Theorem 1.1 (a) implies that $I = \bigcap_{\alpha\in\mathbb{K}} I + \langle x_1 - \alpha\rangle$, since

$$I \subseteq \bigcap_{\alpha\in\mathbb{K}} I + \langle x_1 - \alpha\rangle = \bigcap_{\alpha\in\mathbb{K}} \sqrt{I} + \langle x_1 - \alpha\rangle \subseteq \tag{1.1}$$
$$\subseteq \bigcap_{\alpha\in\mathbb{K}} \sqrt{I + \langle x_1 - \alpha\rangle} \overset{1.1(a)}{=} \sqrt{I} = I.$$

However, this reconstruction formula is not valid for general ideals. For example $I = \langle xy\rangle$ and $J = \langle x^2 y\rangle$ are distinct ideals of $\mathbb{K}[x, y]$ that have exactly the same cross sections $I + \langle x - \alpha\rangle = J + \langle x - \alpha\rangle$ for all $\alpha \in \mathbb{K}$. Theorem 1.1 (b) shows that this problem can be avoided by including powers of the ideals $\langle x_1 - \alpha\rangle$. Informally speaking, these powers account for the multiplicities hidden in I that are not visible geometrically in $V(I)$.

Our second result corresponds with the situation where infinitely many cross sections are known, i.e., the problem of recovering an ideal I from the set $I_S = \{(\alpha, I + \langle x_1 - \alpha\rangle) \colon \alpha \in S\}$, where $S \subseteq \mathbb{K}$ is infinite. In this case, only varieties with no irreducible component included in a hyperplane $\{x_1 = \alpha\}$ can be reconstructed. These varieties, as we show in section 2, correspond exactly with those given by ideals in good position according to the following definition.

Definition 1.2. Let $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ be an ideal. We say that I is in good position geometrically (with respect to the variable x_1) if $\sqrt{I} = \bigcap_{i=1}^r P_i$ for some prime ideals P_i such that $P_i \cap \mathbb{K}[x_1] = \{0\}$. Similarly, we say that I is in good position algebraically (with respect to x_1) if $I = \bigcap_{i=1}^r Q_i$ for some primary ideals Q_i such that $Q_i \cap \mathbb{K}[x_1] = \{0\}$.

Any ideal whose variety has no zero-dimensional component can be rotated with a suitable linear change of variables in such a way that the resulting ideal is in good position geometrically. Similarly, ideals with no embedded zero-dimensional component can be put in good position algebraically through a linear change of coordinates.

Theorem 1.3. *Let $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ be an ideal and let $S \subseteq \mathbb{K}$ be an infinite set. Then:*

(a) *I is in good position geometrically with respect to $x_1 \Rightarrow \sqrt{I} = \bigcap_{\alpha\in S} \sqrt{I + \langle x_1 - \alpha\rangle}$.*

(b) *I is in good position algebraically with respect to $x_1 \Rightarrow I = \bigcap_{\alpha\in S} I + \langle x_1 - \alpha\rangle$.*

For radical ideals $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ in good position geometrically, we can show that $I = \bigcap_{\alpha\in S} I + \langle x_1 - \alpha\rangle$ for any infinite set $S \subseteq \mathbb{K}$, using an argument similar

to that yielding (1.1):

$$I \subseteq \bigcap_{\alpha\in S} I + \langle x_1 - \alpha\rangle = \bigcap_{\alpha\in S} \sqrt{I} + \langle x_1 - \alpha\rangle \subseteq \tag{1.2}$$
$$\subseteq \bigcap_{\alpha\in S} \sqrt{I + \langle x_1 - \alpha\rangle} \overset{1.3(a)}{=} \sqrt{I} = I.$$

Finally, our third result studies the possibility of reconstructing a variety (or an ideal) from finitely many cross sections.

Theorem 1.4. *Let $I = \langle f_1, \dots, f_r\rangle \subseteq \mathbb{K}[x_1, \dots, x_n]$ be an ideal, let $S \subseteq \mathbb{K}$ be a finite set, and let $f \in \mathbb{K}[x_1, \dots, x_n]$ satisfy $\deg(f) \le d$. Let $\delta = \max\{\deg(f_i) : i = 1, \dots, r\}$.*

(a) *I is in good position geometrically with respect to x_1 and $|S| > (d+1)\deg(V(I))$. Then*
$$f \in \sqrt{I} \iff f \in \sqrt{I + \langle x_1 - \alpha\rangle}\ \forall\, \alpha \in S,$$
where $\deg(V(I))$ is the maximum of the degrees of the irreducible components of $V(I)$.

(b) *I is in good position algebraically with respect to x_1 and*
$$|S| > \left(\left(d + 2(\delta r)^{2^{n-1}}\right)^n + 1\right)\max\{d, \delta\},$$
then
$$f \in I \iff f \in I + \langle x_1 - \alpha\rangle\ \forall\, \alpha \in S.$$

The conclusion of Theorem 1.4 (b) can be written as

$$I \cap \{f \,:\, \deg(f) \le d\} = \bigcap_{\alpha\in S} (I + \langle x_1 - \alpha\rangle) \cap \{f \,:\, \deg(f) \le d\},$$

where $S \subseteq \mathbb{K}$ has at least $\left(\left(d + 2(\delta r)^{2^{n-1}}\right)^n + 1\right)\max\{d, \delta\} + 1$ elements. In this formulation, both sides of the equality are $\mathbb{K}$-vector spaces of dimension at most $\binom{d+n}{n}$, and in the case where $d = \delta$, they include the generators of I. In particular, it is possible to compute generators of I as the basis of the $\mathbb{K}$-vector space $\bigcap_{\alpha\in S}(I + \langle x_1 - \alpha\rangle) \cap \{f \,:\, \deg(f) \le \delta\}$ when

$$|S| > \left(\left(\delta + 2\left(\delta\tbinom{\delta+n}{n}\right)^{2^{n-1}}\right)^n + 1\right)\delta. \tag{1.3}$$

The same conclusion is achieved with the simpler bound $|S| \ge (\delta + n)^{(n+1)^2 2^n}$, that overestimates bound (1.3) while keeping its order of magnitude. It should be noted that, when the number n of variables is fixed, the bound depends polynomially on δ.

Theorem 1.4 can be used to reduce the problem of ideal membership [8] (for ideals with no zero-dimensional components) to several instances of the same problem with one variable less. The idea is to make first a linear change of coordinates to put the ideal in good position, and then use the theorem to reduce the problem to a large enough number of cross sections. In the geometric case, one can easily check

whether a polynomial f of degree d vanishes on a given algebraic variety V, by simply testing if f vanishes on $(d+1)\deg(V)$ cross sections of V.

In [2], the authors prove that the ideal $I(V)$ of a smooth irreducible variety V is generated by polynomials of degree at most $\deg(V)$. They also provide a probabilistic method for computing those generators. Theorem 1.4 (a) can be used as an alternative procedure to compute the generators of $I(V)$, by iteratively reducing the number of variables and the dimension of V, until there is obtained a zero-dimensional variety, to which we can apply [1] or [6]. At each iteration we change the problem by $(\deg(V)+1)^2$ problems in one variable less.

In the case of principal ideals, we obtained a much better bound, as shown in the following theorem.

Theorem 1.5. *Let $I = \langle f\rangle \subseteq \mathbb{K}[x_1,\dots,x_n]$ be a principal ideal generated by a nonzero polynomial of degree at most d. Assume that $f \notin \mathbb{K}[x_1]$. Let $I_k = I + \langle x_1 - \alpha_k\rangle$ for $k = 1,\dots,2d$, where $\alpha_1,\dots,\alpha_{2d} \in \mathbb{K}$ are pairwise distinct. Then the ideal I can be reconstructed uniquely from the pairs (α_k, I_k).*

Note that the information that I is principal has to be known a priori. In Example 4.2 we exhibit two principal ideals $I, J \subseteq \mathbb{C}[x,y]$, generated by polynomials of degree d, and $2d-1$ points $\alpha_1,\dots,\alpha_{2d-1} \in \mathbb{C}$, such that $I+\langle x-\alpha_i\rangle = J+\langle x-\alpha_i\rangle$ for all $i = 1,\dots,2d-1$. This shows that the bound of Theorem 1.5 cannot be improved.

2. Interpolation of ideals and algebraic varieties

Proposition 2.1. *Let $I \subseteq \mathbb{K}[x_1,\dots,x_n]$ be a radical ideal. Then*

$$I = \bigcap_{\alpha\in\mathbb{K}} I + \langle x_1 - \alpha\rangle.$$

Proof. The forward inclusion ($\subseteq$) is trivial. The backwards inclusion ($\supseteq$) is proved in the following way. Let $f \in \bigcap_{\alpha\in\mathbb{K}} I + \langle x_1-\alpha\rangle$ and $p = (p_1,\dots,p_n) \in V(I)$. Since $f \in I + \langle x_1 - p_1\rangle$, there are $g \in I$ and $q \in \mathbb{K}[x_1,\dots,x_n]$ such that $f = g + (x_1-p_1)q$. Therefore $f(p) = g(p) + (p_1-p_1)q(p) = 0$. This implies that $f \in I(V(I)) = \sqrt{I} = I$. □

The same technique can be used to prove Theorem 1.1 (a), which is slightly stronger than Proposition 2.1, since the ideal $\sqrt{I + \langle x_1-\alpha\rangle}$ contains the ideal $I + \langle x_1-\alpha\rangle$ for all $\alpha \in \mathbb{K}$.

Proof of Theorem 1.1 (a). The forward inclusion ($\subseteq$) is trivial. The backwards inclusion ($\supseteq$) is proved in the following way. Let $f \in \bigcap_{\alpha\in\mathbb{K}} \sqrt{I + \langle x_1-\alpha\rangle}$ and $p = (p_1,\dots,p_n) \in V(I)$. There exists $k \geq 1$ such that $f^k \in I + \langle x_1 - p_1\rangle$. This means that f^k can be written as $f^k = g + (x_1-p_1)q$ for some $g \in I$ and $q \in \mathbb{K}[x_1,\dots,x_n]$. Evaluating at the point p, we get $f^k(p) = g(p) + (p_1-p_1)q(p) = 0$, and then $f(p) = 0$. This implies that $f \in I(V(I)) = \sqrt{I}$. □

The two proofs given above also follow from the fact that $V(I+J) = V(I) \cap V(J)$ for any ideals $I, J \in \mathbb{K}[x_1, \ldots, x_n]$ and the easy fact that if a function is zero on all the cross sections of a variety then it is zero over the whole variety.

Lemma 2.2. *Let $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ be an ideal and let $f, g \in \mathbb{K}[x_1]$ with $\gcd(f, g) = 1$. Then*

$$(I + \langle f \rangle) \cap (I + \langle g \rangle) = I + \langle fg \rangle.$$

Proof. The backwards inclusion ($\supseteq$) is trivial. The forward inclusion ($\subseteq$) is proved in the following way. Take $h \in (I + \langle f \rangle) \cap (I + \langle g \rangle)$. We can write $h = h_1 + ff' = h_2 + gg'$ with $h_1, h_2 \in I$ and $f', g' \in \mathbb{K}[x_1, \ldots, x_n]$. Let $a, b \in \mathbb{K}[x_1]$ be polynomials such that $af + bg = 1$. Since $ff' = h_2 - h_1 + gg'$, then $aff' = a(h_2 - h_1) + agg'$, and also $f' = a(h_2 - h_1) + g(ag' + bf')$. This implies that $ff' \in I + \langle fg \rangle$, and since $h_1 \in I$, we conclude that $h = h_1 + ff' \in I + \langle fg \rangle$. □

Lemma 2.2 allows us to rewrite the conclusion of Proposition 2.1 as

$$I \subseteq \mathbb{K}[x_1, \ldots, x_n] \text{ radical } \Longrightarrow I = \bigcap_{\substack{p \in \mathbb{K}[x_1] \setminus \{0\} \\ \text{squarefree}}} I + \langle p \rangle.$$

Proposition 2.1 does not work for general ideals. For instance, the ideal $I = \langle x_1^2 x_2 \rangle$ and $J = \langle x_1 x_2 \rangle$ satisfy $I + \langle x_1 - \alpha \rangle = J + \langle x_1 - \alpha \rangle$ for all $\alpha \in \mathbb{K}$, but $I \neq J$. Theorem 1.1 (b) shows that this problem can be avoided by considering arbitrarily large powers of $x_1 - \alpha$.

Proof of Theorem 1.1 (b). Let $\mathcal{P}$ denote the set of nonzero polynomials in $\mathbb{K}[x_1]$. By Lemma 2.2 it is enough to show that $I = \bigcap_{p \in \mathcal{P}} I + \langle p \rangle$. We show first that the we can reduce the proof to the case where I is a primary ideal. Indeed, if $I = Q_1 \cap \cdots \cap Q_r$ with Q_i primary ideals, then

$$\begin{aligned} I &\subseteq \bigcap_{p \in \mathcal{P}} I + \langle p \rangle = \bigcap_{p \in \mathcal{P}} ((Q_1 \cap \cdots \cap Q_r) + \langle p \rangle) \\ &\subseteq \bigcap_{p \in \mathcal{P}} ((Q_1 + \langle p \rangle) \cap \cdots \cap (Q_r + \langle p \rangle)) = \bigcap_{i=1}^{r} \bigcap_{p \in \mathcal{P}} (Q_i + \langle p \rangle) = \bigcap_{i=1}^{r} Q_i = I. \end{aligned}$$

If there is a nonzero polynomial q in I pure in x_1, then it is clear that

$$I \subseteq \bigcap_{p \in \mathcal{P}} I + \langle p \rangle \subseteq I + \langle q \rangle = I.$$

This reduces the proof to the case of primary ideals I such that $I \cap \mathbb{K}[x_1] = \{0\}$.

Take I a primary ideal with $I \cap \mathbb{K}[X_1] = 0$. Let $f \in I + \langle p \rangle$. For all $p \in \mathcal{P}$ we can write $f = f_p + pg_p$ with $f_p \in I$ and $g_p \in \mathbb{K}[x_1, \ldots, x_n]$. Now we compare the two representations of f with subindices p and pq for $p, q \in \mathcal{P}$. We have that $f = f_p + pg_p = f_{pq} + pqg_{pq}$. This implies that $p(g_p - qg_{pq}) \in I$ and, since $p \notin \sqrt{I}$, we get $g_p - qg_{pq} \in I$, and also that $g_p \in I + \langle q \rangle$. Write $J = \bigcap_{p \in \mathcal{P}} I + \langle p \rangle$. The

previous discussion proves that $J \subseteq \bigcap_{p\in\mathcal{P}}(I + \langle p\rangle J)$, and since the other inclusion is trivial, we obtain

$$J = \bigcap_{p\in\mathcal{P}} (I + \langle p\rangle J)\,. \tag{2.1}$$

Now we localize (2.1) at the maximal ideal $\mathcal{M} = \langle x_1 - \alpha_1, \ldots, x_n - \alpha_n\rangle \in \mathbb{K}[x_1, \ldots, x_n]$. We obtain

$$J_{\mathcal{M}} = \Big(\bigcap_{p\in\mathcal{P}} (I + \langle p\rangle J)\Big)_{\mathcal{M}} \subseteq \bigcap_{p\in\mathcal{P}} (I + \langle p\rangle J)_{\mathcal{M}} \subseteq \bigcap_{p\in\mathcal{P}} (I_{\mathcal{M}} + \langle p\rangle J_{\mathcal{M}}) \subseteq J_{\mathcal{M}}.$$

Now we have $J_{\mathcal{M}} = \bigcap_{p\in\mathcal{P}} I_{\mathcal{M}} + \langle p\rangle J_{\mathcal{M}}$ as $\mathbb{K}[x_1, \ldots, x_n]_{\mathcal{M}}$-modules. This intersection can be rewritten as

$$J_{\mathcal{M}} = \Big(\bigcap_{\substack{p\in\mathcal{P}\\ p(\alpha_1)=0}} I_{\mathcal{M}} + \langle p\rangle J_{\mathcal{M}}\Big) \cap \Big(\bigcap_{\substack{p\in\mathcal{P}\\ p(\alpha_1)\neq 0}} I_{\mathcal{M}} + \langle p\rangle J_{\mathcal{M}}\Big) = J' \cap J''\,.$$

For any $p \in \mathcal{P}$ such that $p(\alpha_1) \neq 0$, we have that $\langle p\rangle = \langle 1\rangle$ in $\mathbb{K}[x_1, \ldots, x_n]_{\mathcal{M}}$ and consequently $I_{\mathcal{M}} + \langle p\rangle J_{\mathcal{M}} = J_{\mathcal{M}}$. Therefore $J'' = J_{\mathcal{M}}$. For any $p \in \mathcal{P}$ with $p(\alpha_1) = 0$, we have that $\langle p\rangle \subseteq \langle x_1 - \alpha_1\rangle$, and therefore $J' \subseteq I_{\mathcal{M}} + \langle x_1 - \alpha_1\rangle J_{\mathcal{M}}$. All together, this shows that $J_{\mathcal{M}} = J' \cap J'' \subseteq I_{\mathcal{M}} + \langle x_1 - \alpha_1\rangle$, and by Nakayama's lemma, $J_{\mathcal{M}} = I_{\mathcal{M}}$. Since this is true for any maximal ideal $\mathcal{M}$, it follows from the global-local principle that $I = J$. □

Theorem 1.1 (b) is the algebraic counterpart of the more geometrically intuitive Proposition 2.1 and Theorem 1.1 (a). These results show that ideal reconstruction is possible if we are given all the cross sections. Indeed, it is possible to recover ideals (with no vertically embedded components) with infinitely many sections, as we show below. The extra assumption is necessary, as shown by the ideals $I = \langle (x+y)^2, (x+y)x\rangle = \langle x+y\rangle \cap \langle x, y\rangle$ and $J = \langle x+y\rangle$ which satisfy $I + \langle x-\alpha\rangle = J + \langle x-\alpha\rangle = \langle x+y, x-\alpha\rangle$ for all $\alpha \neq 0$, but are not equal. The problem in this example comes from the embedded component $\{(0,0)\}$ of I, corresponding to the primary ideal $\langle x, y\rangle$, that is invisible to all the vertical planes $\{x = \alpha\}$ with $\alpha \neq 0$.

Lemma 2.3. *Let $A(t) \in \mathbb{K}[t]^{N\times M}$ and $b(t) \in \mathbb{K}[t]^{N\times 1}$.*

1. *If $(A(t)|b(t))$ is incompatible in $\mathbb{K}(t)$ then $(A(\alpha)|b(\alpha))$ is compatible in $\mathbb{K}$ for only finitely many $\alpha \in \mathbb{K}$.*
2. *If $(A(t)|b(t))$ is compatible in $\mathbb{K}(t)$ then $(A(\alpha)|b(\alpha))$ is compatible in $\mathbb{K}$ for all but finitely many $\alpha \in \mathbb{K}$.*
3. *Assume that $\deg(A_{ij}), \deg(b_i) \leq d$ for all $1 \leq i \leq N$ and $1 \leq j \leq M$. Let $S \subseteq \mathbb{K}$ with $|S| > d\max\{N, M+1\}$. Then $(A(t)|b(t))$ is compatible if and only if $(A(\alpha)|b(\alpha))$ is compatible for all $\alpha \in S$.*

Proof. The rank of any matrix with coefficients in $\mathbb{K}[t]$ is the size of the largest submatrix with nonzero determinant. Since the determinant of that submatrix is a polynomial in t, its evaluation at α is nonzero for almost every $\alpha \in \mathbb{K}$. The first two statements follow immediately from that remark and the fact that a system $(A|b)$

is compatible if and only if $\operatorname{rank}(A|b) = \operatorname{rank}(A)$. For the last item, note that the degree of the determinant of any square submatrix of $(A(t)|b(t))$ has degree at most $d\max\{N, M+1\}$. □

Theorem 2.4. *Let $I = \langle f_1, \dots, f_r\rangle \subseteq \mathbb{K}[x_1, \dots, x_n]$ be an ideal with $\deg(f_i) \leq \delta$ for $i = 1, \dots, r$, and let $f \in I$. Then there exists $g_1, \dots, g_r \in \mathbb{K}[x_1, \dots, x_n]$ such that $f = g_1 f_1 + \cdots + f_r g_r$ and $\deg(g_i) \leq \deg(f) + 2(r\delta)^{2^{n-1}}$.*

Proof. See the application of Theorem 3 in [4]. □

Lemma 2.5. *Let $I \subseteq \mathbb{K}[x_1, \dots, x_n]$ be a primary ideal with $I \cap \mathbb{K}[x_1] = \{0\}$. Then*

$$(I + \langle x_1 - t\rangle) \cap \mathbb{K}[x_1, \dots, x_n] = I\,,$$

where $I + \langle x_1 - t\rangle$ is regarded as an ideal of $\mathbb{K}(t)[x_1, \dots, x_n]$.

Proof. The backwards inclusion ($\supseteq$) is trivial. The forward inclusion ($\subseteq$) is proved in the following way. Assume that $I = \langle f_1, \dots, f_r\rangle$ with $f_i \in \mathbb{K}[x_1, \dots, x_n]$. Take $f \in \mathbb{K}[x_1, \dots, x_n]$ and suppose that it can be written as $f = f_1 g_1 + \cdots + f_r g_r + (x_1 - t)g$, with $g_i \in \mathbb{K}(t)[x_1, \dots, x_n]$. Clearing denominators by multiplying by $\omega(t) \in \mathbb{K}[t]$ gives $\omega(t)f = f_1\bar{g_1} + \cdots + f_r\bar{g_r} + (x_1 - t)\bar{g}$, where $\bar{g_1}, \dots, \bar{g_r}, \bar{g} \in \mathbb{K}[t, x_1, \dots, x_n]$. Since $f_1, \dots, f_r, f$ do not involve the variable t, substituting $t = x_1$ gives $\omega(x_1)f \in I$. Moreover, $\omega(x_1) \notin \sqrt{I}$ because $I \cap \mathbb{K}[x_1] = 0$. Since I is primary, we conclude that $f \in I$. □

We start with a simplified version of Theorem 1.3 (b) for primary ideals.

Theorem 2.6. *Let $I \subseteq \mathbb{K}[x_1, \dots, x_n]$ be a primary ideal with $I \cap \mathbb{K}[x_1] = \{0\}$ and let $S \subseteq \mathbb{K}$ be an infinite set. Then*

$$I = \bigcap_{\alpha \in S} I + \langle x_1 - \alpha\rangle.$$

Proof. Assume that $I = \langle f_1, \dots, f_r\rangle$, with $f_i \in \mathbb{K}[x_1, \dots, x_n]$, and consider $f \in \mathbb{K}[x_1, \dots, x_n]$. Define $C = \deg(f) + 2((r+1)\delta)^{2^{n-1}}$, where

$$\delta = \max\{1, \deg(f_1), \dots, \deg(f_r)\}.$$

For a given $\alpha \in \mathbb{K}$, we have that $f \in I + \langle x_1 - \alpha\rangle$ if and only if there exist $g_1, \dots, g_r, g \in \mathbb{K}[x_1, \dots, x_n]$ with degrees at most C such that $f = f_1 g_1 + \cdots + f_r g_r + (x_1 - \alpha)g$, by Theorem 2.4. This is a linear system of equations with coefficients that depend polynomially on α. By Lemma 2.3, if this system is compatible for infinitely many α, then it is compatible in $\mathbb{K}(\alpha)$, where α is regarded as an indeterminate. Conversely, if the system is incompatible for infinitely many values of α, then it is also incompatible in $\mathbb{K}(\alpha)$. All together this says that

$$f \in \bigcap_{\alpha \in S} I + \langle x_1 - \alpha\rangle \iff f \in I + \langle x_1 - t\rangle \subseteq \mathbb{K}(t)[x_1, \dots, x_r].$$

We conclude the proof by using Lemma 2.5. □

At this point we have all the tools needed to show the main result of this section.

Proof of Theorem 1.3 (b). The forward inclusion ($\subseteq$) is trivial. The backwards inclusion ($\supseteq$) is proved in the following way. Assume that $I = \bigcap_{i=1}^{r} Q_i$ with Q_i primary and $Q_i \cap \mathbb{K}[x_1] = \{0\}$. We have that

$$\bigcap_{\alpha\in S} I + \langle x_1 - \alpha\rangle = \bigcap_{\alpha\in S}\Big[\Big(\bigcap_{i=1}^{r} Q_i\Big) + \langle x_1-\alpha\rangle\Big]$$
$$\subseteq \bigcap_{\alpha\in S}\bigcap_{i=1}^{r}(Q_i + \langle x_1-\alpha\rangle) = \bigcap_{i=1}^{r}\bigcap_{\alpha\in S}(Q_i + \langle x_1-\alpha\rangle).$$

By Theorem 2.6, the last term of the previous chain of inclusions equals $\bigcap_{i=1}^{r} Q_i = I$. □

Theorem 2.7. *Let $I = \langle f_1,\dots,f_r\rangle \subseteq \mathbb{K}[x_1,\dots,x_n]$ be an ideal with $\deg(f_i) \le \delta$ for $i = 1,\dots,r$, and let $f \in \sqrt{I}$ with $\deg(f) \le \delta$. Then there exist $g_1,\dots,g_r,g \in \mathbb{K}[t,x_1,\dots,x_n]$ such that $1 = g_1f_1 + \cdots + f_rg_r + (1-tf)g$, with $\deg(g_i)$ and $\deg(g)$ no greater than $\max\{3,\delta+1\}^{n+1}$.*

Proof. See Theorem 1.5 in [7]. See also [3], Theorem 1.1 in [5], or Theorem 1 in [9] for alternative proofs. □

A conclusion similar to that of Theorem 2.7 can be obtained from Theorem 2.4, but with a worse bound. Although any finite bound would have been enough to show the following theorem, we included it here since it gives an idea of the computational complexity of the linear algebra problem involved in the proof.

Proof of Theorem 1.3 (a). The forward inclusion ($\subseteq$) is trivial. The backwards inclusion ($\supseteq$) is proved in the following way. Assume that $I = \langle f_1,\dots,f_r\rangle$ with $f_i \in \mathbb{K}[x_1,\dots,x_n]$. Take $f \in \bigcap_{\alpha\in S}\sqrt{I + \langle x_1-\alpha\rangle}$ and let

$$\delta = \max\{\deg(f),\ \deg_{i=1,\dots,r}(f_i)\}.$$

Define $C = \max\{3,\delta+1\}^{n+1}$, the constant of Theorem 2.7. For all $\alpha \in S$, the linear system $1 = f_1g_1 + \cdots + f_rg_r + (x_1-\alpha)h + (1-tf)g$ with $\deg(g),\deg(h),\deg(g_i) \le C$ is compatible in $\mathbb{K}$, i.e., there are $g_1,\dots,g_r,g,h \in \mathbb{K}[x_1,\dots,x_n]$, that depend on α, such that $1 = f_1g_1 + \cdots + f_rg_r + (x_1-\alpha)h + (1-tf)g$. By Lemma 2.3, the system is also compatible over $\mathbb{K}(\alpha)$, where α is regarded as an indeterminate. This means that, in the expression above, $g_1,\dots,g_r,h,g$ can be taken in $\mathbb{K}(\alpha)[t,x_1,\dots,x_n]$. Multiplying by $\omega(\alpha)$ in order to clear denominators, we get

$$\omega(\alpha) = f_1\bar{g}_1 + \cdots + g_r\bar{g}_r + (x_1-t)\bar{h} + (1-tf)\bar{g}\,,$$

where $\bar{g}_1,\dots,\bar{g}_r,\bar{h},\bar{g} \in \mathbb{K}[\alpha,t,x_1,\dots,x_n]$. Substituting $\alpha = x_1$, we get

$$\omega(x_1) = f_1\tilde{g}_1 + \cdots + f_r\tilde{g}_r + (1-tf)\tilde{g}\,,$$

where $\tilde{g}_1,\dots,\tilde{g}_r,\tilde{g} \in \mathbb{K}[t,x_1,\dots,x_n]$. Finally, substituting $t = 1/f$ and removing denominators by multiplying by a large enough power of f, we obtain $f^N\omega(x_1) \in I$. Since $\sqrt{I} = P_1 \cap \cdots \cap P_s$ with P_i prime and $P_i \cap \mathbb{K}[x_1] = 0$, we have that $\omega(x_1) \notin P_i$ and therefore $f \in P_i$ for all i. This implies that $f \in I$. □

3. Recovering an ideal from finitely many cross sections

Let $I = \langle f_1, \dots, f_r \rangle \subseteq \mathbb{K}[x_1, \dots, x_n]$ be an ideal and let $\alpha \in \mathbb{K}$. Throughout this section we will use the notation

$$I|_{x_1=\alpha} = \langle f_1|_{x_1=\alpha}, \dots, f_r|_{x_1=\alpha} \rangle \subseteq \mathbb{K}[x_2, \dots, x_n].$$

Theorem 3.1. *Let $I \subseteq \mathbb{K}[x_1, \dots, x_n]$ be an ideal such that:*

- *$V(I)$ is equidimensional.*
- *$V(I)$ has no irreducible component contained in a hyperplane $\{x_1 = \alpha\}$.*

Let $f \in \mathbb{K}[x_1, \dots, x_n]$ satisfy $\deg(f) \leq d$. Then

$$f \in \sqrt{I} \iff f|_{x_1=\alpha} \in \sqrt{I|_{x_1=\alpha}}$$

for all $\alpha \in S$ with $|S| > (d+1)\deg(V(I))$.

Proof. The forward implication ($\Rightarrow$) is trivial. The backwards implication ($\Leftarrow$) is proved in the following way. We proceed by induction on $\dim(V(I))$.

Case $\dim(V(I)) = 1$. We have that $V(I)$ is a union of irreducible curves $\mathcal{C}_1 \cup \cdots \cup \mathcal{C}_m$. Our assumptions imply that f vanishes on $V(I) \cap \{x_1 = \alpha\}$ for all $\alpha \in S$, and in particular, f vanishes on $\mathcal{C}_i \cap \{x_1 = \alpha\}$ for all $\alpha \in S$ and $i = 1, \dots, m$. We know that $|\mathcal{C}_i \cap \{x_1 = \alpha\}| \geq 1$ for all α except maybe for those values where the compactification of $\mathcal{C}_i$ in $\mathbb{P}^n$ intersects the hyperplane $\{x_1 = \alpha\}$ at infinity. Since there are at most $\deg(V(I))$ such points, we have $|V(f) \cap \mathcal{C}_i| > \deg(V(I))d$. By Bezout's theorem (see Theorem 2.1 in [10]), we have that either $|V(f) \cap \mathcal{C}_i| \leq \deg(V(I))d$ or f vanishes on $\mathcal{C}_i$. We have shown above that the former cannot happen, so we conclude that $f \in I(\mathcal{C}_i)$ for all $i = 1, \dots, m$. Therefore $f \in \sqrt{I}$.

Case $\dim(V(I)) = e > 1$. Assume the theorem is true for $\dim(V(I)) \leq e - 1$. Without loss of generality we can assume that, after a suitable linear change of coordinates, there exist an infinite set $\Omega \subseteq \mathbb{K}$ such that the ideals $I|_{x_2=\beta}$ satisfy

- $\deg(V(I)) = \deg(V(I|_{x_2=\beta}))$,
- $V(I|_{x_2=\beta})$ is equidimensional,
- $\dim(V(I|_{x_2=\beta})) = \dim V(I) - 1 \geq 1$,
- $V(I|_{x_2=\beta})$ has no irreducible component contained in any hyperplane $\{x_1 = \alpha\}$,

for all $\beta \in \Omega$. In particular, the ideals $I|_{x_2=\beta}$ satisfy the induction hypothesis with $\dim(V(I|_{x_2=\beta})) = e - 1$. If $f|_{x_1=\alpha} \in \sqrt{I|_{x_1=\alpha}}$ for $\alpha \in S$ with $|S| > (d+1) \cdot \deg(V(I))$, then we also have that $f|_{x_1=\alpha,\ x_2=\beta} \in \sqrt{I|_{x_1=\alpha,\ x_2=\beta}}$. Consequently, $f|_{x_2=\beta} \in \sqrt{I|_{x_2=\beta}}$ for all $\beta \in \Omega$. By Theorem 1.3 (a), we conclude that $f \in \bigcap_{\beta \in S} \sqrt{I + \langle x_2 - \beta \rangle} = \sqrt{I}$. □

Now Theorem 1.4 (a) follows as a corollary.

Proof of Theorem 1.4 (a). Our assumptions imply that

$$V(I) = V = V_1 \cup V_2 \cup \ldots \cup V_e\,,$$

where $e = \dim V$ and the V_i are equidimensional varieties of dimension i, none of them included in a hyperplane $\{x_1 = \alpha\}$. The following diagram holds:

$$\begin{array}{ccc} f|_V \equiv 0 & \Longleftrightarrow & f|_{V\cap\{x_1=\alpha\}} \equiv 0 \\ \Big\Updownarrow{\scriptstyle \forall i} & & \Big\Updownarrow{\scriptstyle \forall i \atop \forall \alpha\in S} \\ f|_{V_i} \equiv 0 & \overset{(*)}{\Longleftrightarrow} & f|_{V_i\cap\{x_1=\alpha\}} \equiv 0 \end{array}$$

The arrow $(*)$ follows from Theorem 3.1. By the Nullstellensatz, the arrow on top is equivalent to the claim that $f \in I \iff f \in \sqrt{I + \langle x_1 - \alpha\rangle}\ \forall\, \alpha \in S$. □

In the algebraic case, we proceed as in the proof of Theorem 1.3 (b), but keeping track of the bounds on the degrees.

Proof of Theorem 1.4 (b). Assume that $I = \bigcap_{i=1}^{l} Q_i$, where the Q_i are primary ideals with $Q_i \cap \mathbb{K}[x_1] = \{0\}$. By Theorem 2.4, we have that $f \in I$ if and only if there exist $g_1, \ldots, g_r \in \mathbb{K}[x_1, \ldots, x_n]$ with $\deg(g_i) \leq d + 2(\delta r)^{2^{n-1}}$ such that $f = f_1 g_1 + \cdots + f_r g_r$. This equation can be regarded as the linear system

$$f \in I \iff A(x_1)G = b(x_1) \tag{3.1}$$

of equations in $\mathbb{K}[x_1]$, where $A(x_1)$ and $b(x_1)$ are matrices whose entries are the coefficients of $f_1, \ldots, f_r$ and f respectively. The unknowns are the coefficients of g, represented by the vector G. Therefore $f \in I$ if and only if the system (3.1) is compatible in $\mathbb{K}[x_1]$. Thanks to the hypothesis of good position this is equivalent to being compatible in $\mathbb{K}(x_1)$. By Lemma 2.3, the system (3.1) is compatible if and only if the system $(A(\alpha)|b(\alpha))$ is compatible for $\alpha \in S$ with $|S| > \max\{d, \delta\} \max\{\mathrm{rows}(A), \mathrm{cols}(A) + 1\}$. Using Theorem 2.4 again, each of these systems is compatible if and only if $f|_{x_1=\alpha} \in I|_{x_1=\alpha}$, or equivalently, $f \in I + \langle x_1 - \alpha\rangle$. The result follows by counting the number of rows and columns of A. One obtains $\mathrm{rows}(A) \leq d^n$ and $\mathrm{cols}(A) \leq (d + 2(\delta r)^{2^{n-1}})^n$. □

4. Principal ideals

Remark 4.1. Let $I = \langle f\rangle \subseteq \mathbb{K}[x_1, \ldots, x_n]$ be a principal ideal, and let $J = I + \langle x_1 - \alpha\rangle$ with $\alpha \in \mathbb{K}$. Then $J \cap \mathbb{K}[x_2, \ldots, x_n] = \langle f(\alpha, x_2, \ldots, x_n)\rangle$ in $\mathbb{K}[x_2, \ldots, x_n]$.

Proof of Theorem 1.5. Throughout this proof we will write $x = x_1$ and $y = (x_2, \ldots, x_n)$. We will order the monomials in y using the graded lexicographic order $x_2 > x_3 > \cdots > x_n$. Let

$$f = \sum_{i\,:\,|i|\leq d} a_i(x) y^i,$$

where $i = (i_2, \dots, i_n)$, $y^i = x_2^{i_2} \cdots x_n^{i_n}$, and $|i| = i_2 + \cdots + i_n$. By Remark 4.1, for any $k = 1, \dots, 2d$, we have that

$$I_k \cap \mathbb{K}[y] = \langle f, x - \alpha_k \rangle \cap \mathbb{K}[y] = \langle g_k \rangle,$$

where $g_k = \lambda_k f(\alpha_k, y)$ has leading coefficient 1 and $\lambda_k \in \mathbb{K}^*$. The following identities show that it is possible to recover $\operatorname{multideg}_y(f)$ from the g_k:

$$\begin{aligned} e = \operatorname{multideg}_y(f) &= \max\{i : a_i(x) \neq 0\} \overset{(*)}{=} \max\{i : a_i(\alpha_k) \neq 0 \text{ for some } k\} \\ &= \max_{k=1,\dots,2d} (\max\{i : a_i(\alpha_k) \neq 0\}) = \max_{k=1,\dots,2d} \operatorname{multideg}_y(f(\alpha_k, y)) \\ &= \max_{k=1,\dots,2d} \operatorname{multideg}_y(g_k). \end{aligned}$$

The equality $(*)$ is true since $\deg(a_i) \leq d - |i| < 2d$.

Now we know that $f = \sum_{i \leq e} a_i(x) y^i$ with $a_e \neq 0$. Since $f \notin \mathbb{K}[x]$, then $|e| \geq 1$. The polynomial $a_e(x)$ vanishes on exactly $r \leq d - |e|$ points in $\{\alpha_1, \dots, \alpha_{2d}\}$. Without loss of generality we can assume $a_e(\alpha_{2d-r+1}) = \cdots = a_e(\alpha_{2d}) = 0$, i.e.,

$$a_e(x) = \tilde{a}_e(x) \cdot \prod_{l=2d-r+1}^{2d} (x - \alpha_l), \tag{4.1}$$

where $\tilde{a}_e \in \mathbb{K}[x]$ has degree at most $d - |e| - r$. Since the polynomials $g_k = \lambda_k f(\alpha_k, y)$ have leading coefficients 1, $\lambda_k = 1/a_e(\alpha_k)$ for $k = 1, \dots, 2d - r$. In particular, the coefficients of g_k, which are all known, are equal to $a_i(\alpha_k)/a_e(\alpha_k)$ for $1 \leq k \leq 2d - r$ and $0 \leq i \leq e$. Combining this with equation (4.1), we obtain the fractions

$$\frac{a_i(\alpha_k)}{\tilde{a}_e(\alpha_k)} = \frac{a_i(\alpha_k)}{a_e(\alpha_k)} \cdot \prod_{l=2d-r+1}^{2d} (\alpha_k - \alpha_l).$$

Since $\deg(a_i) \leq d - |i|$ and $\deg(\tilde{a}_e) \leq d - |e| - r$, it is possible to reconstruct the rational function $a_i(x)/\tilde{a}_e(x)$ from the $2d - r \geq 2d - |i| - |e| - r + 1$ points $\alpha_1, \dots, \alpha_{2d-r}$ using rational interpolation. □

The following example shows that $2d - 1$ cross sections are not enough.

Example 4.2. Consider the polynomials $f = p(x)y + 1$ and $g = a(x)y + b(x)$, where $p(x) = x^d$, $a(x) = -x^{d-1} + 2^{2d-1}$, and $b(x) = x^d - 1$. The ideals $I = \langle f \rangle$ and $J = \langle g \rangle$ are both principal, generated by polynomials of degree d, and clearly satisfy $I \neq J$. Let $\alpha_i = 2\xi_{2d-1}^i$, where $\xi_{2d-1} \in \mathbb{C}$ is a primitive $(2d-1)$st root of unity. The ideals $I + \langle x - \alpha_i \rangle$ and $J + \langle x - \alpha_i \rangle$ are equal for $i = 1, \dots, 2d - 1$. Indeed, a simple computation shows that $(2^d \, \xi_{2d-1}^{id} - 1) f(\alpha_i, y) = g(\alpha_i, y)$.

Acknowledgements. We would like to thank Jessica Aliaga Lavrijsen, José Ignacio Cogolludo-Agustín, Álvaro Lozano-Rojo, and Silvia Vilariño Fernández for many valuable comments and corrections.

References

[1] Becker, E. and Wörmann, T.: Radical computations of zero-dimensional ideals and real root counting. *Math. Comput. Simulation* **42** (1996), 561–569.

[2] Blanco, C., Jeronimo, G. and Solernó, P.: Computing generators of the ideal of a smooth affine algebraic variety. *J. Symbolic Comput.* **38** (2004), 843–872.

[3] Fitchas, N. and Galligo, A.: Nullstellensatz effectif et conjecture de Serre (théorème de Quillen–Suslin) pour le Calcul Formel. *Math. Nachr.* **149** (1990), 231–253.

[4] Hermann, G.: Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. *Math. Ann.* **95** (1926), 736–788.

[5] Jelonek, Z.: On the effective Nullstellensatz. *Invent. Math.* **162** (2005), 1–17.

[6] Krick, T. and Logar, A.: An algorithm for the computation of the radical of an ideal in the ring of polynomials. In *Applied algebra, algebraic algorithms and error-correcting codes (New Orleans, LA, 1991)*, 195–205. Lecture Notes in Comput. Sci. 539, Springer, Berlin, 1991.

[7] Kollár, J.: Sharp effective nullstellensatz. *J. Amer. Math. Soc.* **1** (1988), no. 4, 963–975.

[8] Mayr, E. W.: Some complexity results for polynomial ideals. *J. Complexity* **13** (1997), 303–325.

[9] Sombra, M.: A sparse effective Nullstellensatz. *Adv. Appl. Math.* **22** (1999), no. 2, 271–295.

[10] Vogel, W. and Patil, D. P.: *Lectures on results on Bézout's theorem.* Tata Institute of Fundamental Research Lectures on Mathematics and Physics 74, Tata Institute of Fundamental Research, Bombay; Springer-Verlag, Berlin, 1984.

Received March 13, 2013.

Martín Avendaño: Centro Universitario de la Defensa-IUMA, Academia General Militar, Ctra. de Huesca s/n, 50090, Zaragoza, Spain.
E-mail: avendano@unizar.es

Jorge Ortigas-Galindo: Centro Universitario de la Defensa-IUMA, Academia General Militar, Ctra. de Huesca s/n, 50090, Zaragoza, Spain.
E-mail: jortigas@unizar.es

The second author is partially supported by the Spanish Ministry of Education grant MTM2010-21740-C02-02 and the E15 Grupo Consolidado Geometría grant from the Gobierno de Aragón.