A Construction of Radical Ideals in Polynomial Algebra

Josef Schicho Ziming Li
Research Institute for Symbolic Computation
Johannes Kepler University
A-4040 Linz, Austria
e-mail: {jschicho, zmli}@risc.uni-linz.ac.at

July 10, 1995

Abstract

Given an ideal I generated by n polynomials in $m+n$ indeterminates over a field, we construct an ideal J from the given basis of I and one of its Jacobians. We prove that J is radical and that J is the intersection of some isolated prime ideals of I if J is nontrivial. The result may be regarded as a generalization of a lemma by D. Lazard.

1 Introduction

The relation between linear equations (algebraic) and their solution set (geometric) is very simple. Much of this simplicity breaks down with polynomial equations, say, $f_1, f_2, \ldots, f_n$ in $m+n$ unknowns.

- There might be an equation, which is fulfilled on the solution set X but is not in the ideal I generated by $f_1, f_2, \ldots, f_n$. This happens if and only if I is *not* radical.
- The solution set X might contain components of different dimensions. This happens if and only if X is *not* unmixed.
- The dimension of X might be greater than the number of unknowns minus the minimal number of equations. This happens if and only if X is *not* a complete intersection.

Due to these complications, the manipulation of polynomial equations and their solution sets is much harder than the linear case. The last two decades have seen a rapid development of algorithms for manipulating polynomials and their solution sets. Several methods [2, 3] can take advantage of the three properties mentioned above.

In this paper, we establish these properties under comparatively mild restrictions. Apart from the zero set of one of the Jacobians, the ideal generated by $f_1, f_2, \ldots, f_n$ is radical and its solution set is a complete intersection (especially unmixed). Using this observation, we construct a radical ideal J, whose solution set consists of some of the m-dimensional components of the solution set I.

An important special case of this construction was considered by Lazard [7]. If $f_1, f_2, \ldots, f_n$ form a triangular set, i.e. f_i depends only on the first $m+i$ variables (with respect to a given ordering of unknowns), then the Jacobian of the f_i's with respect to the last n variables is the product of the separants, hence, the construction of J is similar to that of the differential prime ideals by their characteristic sets [5]. The fact that the so constructed ideal is radical, has some interesting applications. For instance, it simplifies the algorithm for computing the representation for a radical differential ideal in [2]. It might be interesting to note that this paper grew out of the efforts to clarify the details of the proof of Lazard's lemma in a draft of [5]. It was nice to observe that, in this case, clarification went hand in hand with generalization.

This paper is organized as follows. In Section 2, we review the results from commutative algebra that will be used later. Section 3 is devoted to proving that our construction yields a radical ideal. In Section 4, we generalize Lazard's lemma in [2].

2 Preliminaries

Throughout the paper, K is a field and $\bar{K}$ is an algebraically closed field containing K. Let u_1, u_2, …, u_m, x_1, x_2, …, x_n be $(m+n)$ indeterminates over $\bar{K}$. The polynomial ring $K[u_1, u_2, \ldots, u_m, x_1, x_2, \ldots, x_n]$ is denoted by R. For $A \subset R$, the algebraic set defined by A in the affine space $\mathbf{A}^{m+n}$ over $\bar{K}$ is denoted by $\mathcal{V}(A)$.

We state three classical lemmas that will be used in the sequel. The first lemma (see, Remarks in [1, p. 110]) is based on the fact that a formal power series over a field is invertible if and only if its constant term is nonzero.

Lemma 2.1 If M is the ideal generated by u_1, …, u_m, x_1, …, x_n in R, and S is the multiplicative set $R \setminus M$, then the $S^{-1}M$-*adic* completion of $S^{-1}R$ can be identified to be the formal power series ring $K[[u_1, \ldots, u_m, x_1, \ldots, x_n]]$.

The second lemma (see, Lemma 9 in [5, p. 18]) follows from the fact that the ring $\bar{K}[u_1, \ldots, u_m, x_1, \ldots, x_n]$ is a free R-module.

Lemma 2.2 If I is an ideal of R and I^e is the extended ideal of I in $\bar{K}[u_1, \ldots, u_m, x_1, \ldots, x_n]$, then $I^e \cap R = I$.

The third lemma is the algebraic version of the implicit function theorem (see, Proposition 8 in [5, pp. 31–33]).

Lemma 2.3 If $p = (\underbrace{0, \ldots, 0}_{m+n})$, $f_i \in R$, and $f_i(p) = 0$, for $i = 1, \ldots, n$, and

$$\frac{\partial(f_1, \ldots, f_n)}{\partial(x_1, \ldots, x_n)}(0) \neq 0,$$

then there exist unique power series $a_1, \ldots, a_n \in K[[u_1, \ldots, u_m]]$ such that

$$a_i(\underbrace{0, \ldots, 0}_{m}) \quad \text{and} \quad f_i(u_1, \ldots, u_m, a_1, \ldots, a_n) = 0,$$

for $i = 1, \ldots, n$. These power series have the further property that the ideals

$$(f_1, \ldots, f_n) \quad \text{and} \quad (x_1 - a_1, \ldots, x_n - a_n)$$

of $K[[u_1, \ldots, u_m, x_1, \ldots, x_n]]$ coincide.

We remark that the power series $a_1, \ldots, a_n$ are all equal to 0 if $m = 0$.

3 Construction

In the remainder of this paper, we fix $f_1, \ldots, f_n \in R$ and denote the ideal $(f_1, \ldots, f_n)$ of R by I. The Jacobian

$$\frac{\partial(f_1, \ldots, f_n)}{\partial(x_1, \ldots, x_n)}$$

is denoted by Δ. By I and Δ we can construct a new ideal $J = I : \Delta^\infty$ of R, that is,

$$J = \{f \mid \exists k \in \mathbb{N}, f\Delta^k \in I\}.$$

This section is devoted to proving

Theorem 3.1 The ideal J is radical.[1]

For the time being, we assume $K = \bar{K}$ so that the points of $\mathbf{A}^{m+n}$ over $\bar{K}$ and maximal ideals of R are the same. Let $R[\Delta^{-1}]$ be the localization of R at the multiplicative set $\{\Delta^k \mid k \in \mathbb{N}\}$ and R_p the localization of R at a point p of $\mathbf{A}^{m+n}$. Obviously, for $p \in \mathbf{A}^{m+n}$ with $\Delta(p) \neq 0$, the inclusions

$$R \subset R[\Delta^{-1}] \subset R_p$$

hold. If I' is the extended ideal of I in $R[\Delta^{-1}]$, then the contracted ideal of I' is equal to J. Hence, to prove that J is radical, we need only to prove that I' is radical since the contraction of a radical ideal is also radical.

To illustrate the geometric and analytic ideas behind our algebraic deduction, we divide the proof of Theorem 3.1 into three lemmas.

Extending the ideal I to $R[\Delta^{-1}]$ can be seen as restricting one's attention to the points, where $\Delta \neq 0$. The maximal ideals of $R[\Delta^{-1}]$ correspond to the maximal ideals of R not containing R, i.e., the points where Δ does not vanish. By adjoining Δ^{-1}, we are, so to speak, forcing that $\Delta \neq 0$.

The following lemma is an instance of the principle that "radical is a local property."

Lemma 3.2 Let I_p be the extended ideal of I in R_p. If I_p is radical, for all $p \in \mathbf{A}^{m+n}$ with $\Delta(p) \neq 0$, then the ideal I' is radical, where I' is the extended ideal of I in $R[\Delta^{-1}]$.

Proof Let I'_p be the contracted ideal of I_p in $R[\Delta^{-1}]$, where $\Delta(p) \neq 0$. Then I'_p is radical, so, the intersection of all the I'_p's is radical. Hence, it suffices to prove that I' is equal to this intersection. The inclusion

$$I' \subset \bigcap_{\Delta(p)\neq 0} I'_p$$

holds by the respective definitions of I' and I'_p. To prove the inclusion

$$I' \supset \bigcap_{\Delta(p)\neq 0} I'_p,$$

we let $f \in \cap_{\Delta(p)\neq 0} I'_p$. Then, for each p with $\Delta(p) \neq 0$, there exists an $h_p \in R$ with $h_p(p) \neq 0$ such that $h_p f \in I$. Let H be the ideal generated by the h_p's. Then Δ vanishes on $\mathcal{V}(H)$, for, otherwise, there would exist a point $q \in \mathcal{V}(H)$ with $\Delta(q) \neq 0$, consequently, there would exist an $h_q \in H$ with $h_q(q) \neq 0$, which is a contradiction to the fact that $q \in \mathcal{V}(H)$. Hence, $\Delta^k \in H$, for some $k \in \mathbb{N}$, by Hilbert Nullstellensatz. Accordingly, $f\Delta^k \in I$ since $fH \subset I$. Therefore, $f \in I'$ since Δ is invertible in $R[\Delta^{-1}]$. $\square$

The equality $I' = \bigcap_{\Delta(p)} I'_p$ just proved above is a special case of a fundamental lemma in the theory of coherent sheaves (see, Proposition 2.2 in [4]). For radical ideals of polynomials, this equality reveals nothing more than that a polynomial vanishes on an algebraic set if and only if it vanishes at every point of the algebraic set.

To prove that I' is radical, by Lemma 3.2, we need only to prove that I_p is radical, where $\Delta(p) \neq 0$. The next two lemmas will assert the stronger result that I_p is prime.

Lemma 3.3 Let L be a Noetherian local ring with the maximal ideal M and $\hat{L}$ the M-*adic* completion of L. If A is an ideal of L, $\hat{A}$ is the extended ideal of A in $\hat{L}$, and B is the contracted ideal of $\hat{A}$ in L, then $A = B$.

Proof Consider the exact sequence

$$0 \to A \hookrightarrow B \to N \to 0$$

of L-modules, where $N = A/B$. Then we have the exact sequence

$$0 \to \hat{A} \hookrightarrow \hat{B} \to \hat{N} \to 0$$

[1] A different proof of this theorem is given by S. Morrison [8].

of $\hat{L}$-modules by Proposition 10.20 in [1]. Since $B \subset \hat{A}$, $\hat{B} \subset \hat{A}$. Thus, the injection in the second exact sequence is an isomorphism, consequently, $\hat{N} = 0$. By the definition of completion, there is a surjective map from $\hat{N}$ to $N/(MN)$. Hence, the L-module $N/(MN) = 0$. By Nakayama's lemma, we have $N = 0$, accordingly, $A = B$. □

The next lemma is closely related to the geometrical observation: the ideal I looks like the ideal of a linear space in a neighborhood of a point p, where $\Delta(p) \neq 0$.

Lemma 3.4 Let $p \in \mathbf{A}^{m+n}$ with $\Delta(p) \neq 0$. If I_p is the extended ideal of I in R_p, then I_p is prime.

Proof If there exists an f_i, for some i with $1 \leq i \leq n$ such that $f_i(p) \neq 0$, then $I_p = R_p$. So, we assume that $f_i(p) = 0$, for $i = 1, \ldots, n$.

As K is algebraically closed, we may further assume that p is the origin. Let $\hat{I}$ be the extended ideal of I in $K[[u_1, \ldots, u_m, x_1, \ldots, x_n]]$. It follows from Lemma 2.3 that there are $a_1, \ldots, a_n \in K[[u_1, \ldots, u_m]]$ without constant terms such that

$$\hat{I} = (x_1 - a_1, \ldots, x_n - a_n).$$

Hence, $\hat{I}$ is a prime ideal.

Note that $K[[u_1, \ldots, u_m, x_1, \ldots, x_n]]$ is the completion of R_p at the origin by Lemma 2.1. Thus, $\hat{I}$ is the extended ideal of I_p in $K[[u_1, \ldots, u_m, x_1, \ldots, x_n]]$ because $I \subset I_p \subset \hat{I}$. Since $\hat{I} \cap R_p = I_p$ by Lemma 3.3, we see that I_p is a prime ideal. □

This lemma implies that the ideal I_p of R_p is radical if $\Delta(p) \neq 0$. It then follows from Lemma 3.2 that the ideal I' given in Lemma 3.2 is radical. So, the ideal J of R is also radical. Consequently, Theorem 3.1 holds if K is algebraically closed. Now, we prove Theorem 3.1 without assuming that $K = \bar{K}$.

Proof of Theorem 3.1 The extended ideal of J in $\bar{K}[u_1, \ldots, u_m, x_1, \ldots, x_n]$ is radical by Lemmas 3.4 and 3.2. Therefore, J is radical by Lemma 2.2. □

4 Properties of the Ideal J

We will give further properties of the ideal J and generalize Lazard's lemma in [2]. Proofs of these properties are based on Theorem 3.1 and some classical results from commutative algebra. In this section, the ideal J is assumed to be neither R nor (0). For a proper ideal N of R, the total quotient field of R/N is denoted by $\mathcal{Q}(R/N)$.

The following lemma describes the relation between the ideals I and J.

Lemma 4.1 If $P_1, \ldots, P_r$ are the associated prime ideals of $\sqrt{I}$ and do not contain Δ, then

$$J = \bigcap_{i=1}^{r} P_i.$$

Proof If $f \in J$, then $f\Delta^k \in \sqrt{I}$. Hence, $f\Delta^k \in P_i$, and, consequently, $f \in P_i$ since Δ is not in P_i, where $1 \leq i \leq r$. Conversely, if $f \in \cap_{i=1}^{r} P_i$, then $f\Delta \in \sqrt{I}$ since $f\Delta$ belongs to each of the associated prime ideals of $\sqrt{I}$. Therefore, $(f\Delta)^k \in I$, for some $k \in \mathbb{N}$. Accordingly, $f^k \in J$. It then follows Theorem 3.1 that $f \in J$. □

The next lemma shows that a nonzero polynomial of $K[u_1, \ldots, u_n]$ is a nonzerodivisor of R/J.

Lemma 4.2 If $f \in R$, $g \in K[u_1, \ldots, u_m]$ with $g \neq 0$, and $gf \in J$, then $f \in J$.

Proof First, we assume that $K = \bar{K}$. Let $p \in \mathcal{V}(I)$ with $\Delta(p) \neq 0$. Since all the coordinates of p are in K, we may further assume that p is the origin. By Lemma 2.3 there exist $a_1, \ldots a_n \in K[[u_1, \ldots, u_m]]$ without constant terms such that

$$h(u_1, \ldots, u_m, a_1, \ldots, a_n) = 0,$$

for all $h \in \sqrt{I}$. Since $gf \in J$, $gf\Delta \in \sqrt{I}$. Hence,

$$g(u_1, \ldots, u_m) f(u_1, \ldots, u_m, a_1, \ldots, a_n) \Delta(u_1, \ldots, u_m, a_1, \ldots, a_n) = 0,$$

and, consequently,

$$f(u_1, \ldots, u_m, a_1, \ldots, a_n) \Delta(u_1, \ldots, u_m, a_1, \ldots, a_n) = 0.$$

Substituting 0 for u_i $(1 \le i \le m)$ in the above equality yields $f(p)\Delta(p) = 0$. Thus, $f(p) = 0$. It then follows that $f\Delta$ vanishes on $\mathcal{V}(I)$. By Hilbert's Nullstellensatz, $f\Delta \in \sqrt{I}$. Thus, there is a positive integer k such that $f^k \in J$, so $f \in J$ by Theorem 3.1. We may then drop the assumption $K = \bar{K}$ by Lemma 2.2. □

Theorem 4.3 *If $P_1, \ldots, P_r$ are the associated prime ideals of J and U is the set $K[u_1, \ldots, u_m] \setminus \{0\}$, then the field $\mathcal{Q}(R/P_i)$ has transcendence degree m over K and is K-isomorphic to $U^{-1}R/U^{-1}P_i$, for all i with $1 \le i \le m$.*

Proof Let i be an integer between 1 and r. Since Δ is not in P_i, there is a point $p_i \in \mathcal{V}(P_i)$ with $\Delta(p_i) \neq 0$. Hence, $\mathcal{Q}(R/P_i)$ is separable over K, with transcendence degree m, by Corollary 2 in [5, p. 46]. Since the set U is prime relative to J by Lemma 4.2, the elements

$$u_1 + P_i, \ldots, u_m + P_i$$

of $\mathcal{Q}(R/P_i)$ are algebraically independent over K. Therefore, $\mathcal{Q}(R/P_i)$ is a separably algebraic extension over $K(u_1 + P_i, \ldots, u_m + P_i)$.

As $P_i \cap U = \emptyset$, the canonical homomorphism from R to R/P_i induces a K-homomorphism η from $U^{-1}R$ to $\mathcal{Q}(R/P)$ with

$$\eta\left(\frac{f}{g}\right) = \frac{f + P_i}{g + P_i}, \text{ for all } f \in R \text{ and } g \in U.$$

Clearly, $\ker(\eta) = U^{-1}P_i$. So it suffices to prove that η is surjective. As $\mathcal{Q}(R/P_i)$ is separably algebraic over $K(u_1+P_i, \ldots, u_m+P_i)$, each element of $\mathcal{Q}(R/P_i)$ can be represented as $(f+P_i)/(g+P_i)$, for some $f \in R$ and $g \in K[u_1, \ldots, u_m]$. Thus, η is surjective. □

This theorem reveals that J is an unmixed ideal with dimension m. Furthermore, the extended ideal of J in $K(u_1, \ldots, u_m)[x_1, \ldots, x_n]$ is a zero-dimensional ideal. Consequently, the ideal membership problem of J can be solved by computing a Gröbner basis for a zero-dimensional ideal over $K(u_1, \ldots, u_m)$.

The next corollary extends Lazard's lemma in [7, 2].

Corollary 4.4 If $P_1, \ldots, P_r$ are the associated prime ideals of J and U is the set $K[u_1, \ldots, u_m] \setminus \{0\}$, then

$$\mathcal{Q}(R/J) = \left(U^{-1}R/U^{-1}P_1\right) \times \cdots \times \left(U^{-1}R/U^{-1}P_r\right). \tag{1}$$

Proof Since

$$\mathcal{Q}(R/J) = \mathcal{Q}(R/P_1) \times \cdots \times \mathcal{Q}(R/P_r)$$

by Proposition 2.8 in [6], the corollary follows from Theorem 4.3. □

This corollary extends Lazard's lemma in two aspects. First, the assumption that $f_1, \ldots, f_n$ form a triangular set, is dropped. Second, the fields on the right-hand side of (1) are given more explicitly.

Acknowledgments

This paper grew out of a seminar in the Special Year (1995) in Computational Differential Algebra and Algebraic Geometry at the City College of New York. Our thanks go to the participants of this seminar. We also thank Sally Morrison, William Sit and Kazuhiro Yokoyama for their comments on a draft of this paper.

References

[1] M. F. Atiyah and I. G. Macdonald. *Introduction to Commutative Algebra.* Addison-Wesley, 1969.

[2] F. Boulier, D. Lazard, F. Ollivier, and M. Petitot. Representation for the radical of a Finitely Generated Differential Ideal. In *Proceedings of the International Symposium on Symbolic and Algebraic Computation,* A. H. M. Levet (ed.), pp. 158–166, 1995.

[3] A. Dickenstein, N. Fichas, M. Guisti, and C. Sessa. The Membership Problem for Unmixed Polynomial Ideals Is Solvable in Sub-Exponential Time. In *Discrete Applied Mathematics,* Vol. 33, No. 1–3, (Proceedings 7th International Conference, AAECC-7) North-Holland-Amsterdam, pp. 77–94, 1991.

[4] R. Hartshone. *Algebraic Geometry*, Springer-Verlag, 1977.

[5] E. R. Kolchin. *Differential Algebra and Algebraic Groups.* Vol. 54 in Pure and Applied Math. Academic Press, New York-London. 1973.

[6] Ernst Kunz. *Introduction to Commutative Algebra and Algebraic Geometry.* Translated by M. Ackerman, Birkhäuser Boston, 1985.

[7] D. Lazard. Solving Algebraic Systems of Positive Dimension In *Discrete Applied Mathematics,* Vol. 33, No. 1–3, (Proceedings 7th International Conference, AAECC-7) North-Holland-Amsterdam, pp. 147–160, 1991.

[8] S. Morrison. Yet another Proof of Lazard's Lemma, *Private Communication*, August, 1995.

[9] O. Zariski and P. Samuel. *Commutative Algebra.* Vol. 1 Graduate Texts in Math 29, Springer-Verlag, 1958.