J. Symbolic Computation (1988) **5**, 141–161

An Improved Projection Operation for Cylindrical Algebraic Decomposition of Three-dimensional Space†

SCOTT McCALLUM‡

Department of Computer Science,
University of Toronto, Toronto, Canada M5S 1A4

(*Received* 21 *May* 1986)

A key component of the cylindrical algebraic decomposition (cad) algorithm of Collins (1975) is the projection operation: the *projection* of a set A of r-variate polynomials is defined to be a certain set of $(r-1)$-variate polynomials. The zeros of the polynomials in the projection comprise a "shadow" of the critical zeros of A. The cad algorithm proceeds by forming successive projections of the input set A, each projection resulting in the elimination of one variable. This paper is concerned with a refinement to the cad algorithm, and to its projection operation in particular. It is shown, using a theorem from complex analytic geometry, that the original projection set for trivariate polynomials that Collins used can be substantially reduced in size, without affecting its essential properties. Observations suggest that the reduction in the projection set size leads to a substantial decrease in the computing time of the cad algorithm.

1. Introduction

A fundamental procedure that pertains to the solution of polynomial equations in several variables is the *cylindrical algebraic decomposition* (*cad*) algorithm due to Collins (1975). This method was developed as part of a decision procedure for elementary algebra and geometry (formally speaking, the theory of real closed fields) that was shown to be more efficient than Tarski's (1951) original method and, indeed, any other subsequent method. The cad algorithm accepts as input a set of integral polynomials (that is, polynomials with integer coefficients) in some $r \geqslant 1$ variables, and produces as output a description of a certain cellular decomposition of r-dimensional Euclidean space $\mathbb{R}^r$. This cellular decomposition of $\mathbb{R}^r$ has the property that each polynomial in the input set is invariant in sign throughout every cell of the decomposition. The "solutions" of the polynomials occurring in the input are thus obtained by retaining those cells in which the sign of each input polynomial is zero.

A key component of the cad algorithm is the projection operation: the *projection* of a set A of r-variate integral polynomials is defined to be a certain set $PROJ(A)$ of $(r-1)$-variate integral polynomials. The zeros of the polynomials in $PROJ(A)$ comprise a "shadow" of the "critical" zeros of A. The set $PROJ(A)$ contains, amongst other elements, all principal subresultant coefficients of all pairs of reducta of elements of A (see section 3).

† This research was supported by NSF (Grant DCR-840817) and NSERC (Grant 3-640-126-30).
‡ Present address: Institut für Mathematik, Johannes Kepler Universität, A-4040 Linz, Austria.

0747–7171/88/010141+21 $03.00/0

The property of the map *PROJ* of particular relevance to the cad algorithm is that if S is any connected subset of $\mathbb{R}^{r-1}$ in which every element of $PROJ(A)$ is invariant in sign and no element of A vanishes identically, then the portion of the zero set of A that lies in the cylinder $S \times \mathbb{R}$ over S consists of a number (possibly 0) of disjoint "layers" over S (that is, A is "delineable" on S). This property is stated as Theorem 5 by Collins (1975) and Theorem 3.4 by Arnon *et al.* (1984*a*). It follows from this property that any decomposition of $\mathbb{R}^{r-1}$ into connected regions such that every polynomial in $PROJ(A)$ is invariant in sign throughout every region can be extended to a decomposition of $\mathbb{R}^r$ (consisting of the union of all of the above-mentioned layers and the regions in between successive layers, for each region of $\mathbb{R}^{r-1}$) such that every polynomial in A is invariant in sign throughout every region of $\mathbb{R}^r$.

This paper is concerned with a refinement to the projection operation in the cad algorithm. Collins (1975) observed that a smaller projection suffices for a set A of bivariate integral polynomials. Provided that the elements of A are squarefree and pairwise relatively prime, it suffices to define $PROJ(A)$ to be the set of all leading coefficients, discriminants, and resultants (of pairs) of the elements of A. The reason is that the delineability property is readily seen to hold over any connected region of the real line in which just the leading coefficients, discriminants and resultants (of pairs) of the elements of A are invariant in sign. The main contribution of this paper is to show that a similar simplification can be made to the projection of a set of trivariate polynomials.

The main result underlying our refinement to the projection map is a theorem from complex analytic geometry which was stated in precise terms by Zariski (1965) (the essential idea used by us in this paper appears to have been known much earlier: Zariski, 1935). Zariski (1975) has, in fact, extended his result to higher dimensions. This extended result of Zariski is used in the author's (1984) PhD thesis to develop an improved projection operation for polynomials in an arbitrary number of variables. Another paper is planned to expose this work.

Section 2 of this paper provides background mathematical material that may be helpful to the reader. Section 3 defines the reduced projection map, states the relevant theorems on this map, and presents a cad construction algorithm that uses this map. Sections 4 and 5 contain the proofs of the theorems stated in section 3. Section 4 consists essentially of a derivation of the main theorem about the reduced projection from the theorem of Zariski (1965) mentioned above. Section 5 contains an exposition of Zariski's theorem. Section 6 comprises observations relating to the application of the cad algorithm from section 3 to two examples. Several details of the proofs from sections 4 and 5 are presented in the Appendix.

2. Background material

2.1. ANALYTIC FUNCTIONS OF SEVERAL VARIABLES

Let $\mathbb{R}$ denote the field of all real numbers, and let $\mathbb{C}$ denote the field of all complex numbers. Throughout this section K will denote either $\mathbb{R}$ or $\mathbb{C}$. A function $f: U \to K$ from an open subset U of K^n into K is said to be *analytic* (in U) if it has a multiple power series representation about each point of U. An analytic function is continuous and has continuous partial derivatives of all orders. A function defined as the sum of a convergent power series is analytic, and its partial derivatives can be obtained by differentiating the defining series term by term. Sums, products and quotients (where the denominator is non-zero) of analytic functions are analytic. The reader is referred to any of the texts

(Gunning & Rossi, 1965; Bochner & Martin, 1948, or Kaplan, 1966) for a more detailed discussion of the basic properties of analytic functions.

If $c \in K^n$, then a *neighbourhood* of c is an open subset W of K^n containing c. The *polydisc* in $\mathbb{C}^n$ about the point $c=(c_1, \ldots, c_n)$ of *polyradius* $(r_1, \ldots, r_n)$ is the set of points $(z_1, \ldots, z_n)$ in $\mathbb{C}^n$ satisfying $|z_1-c_1|<r_1, \ldots, |z_n-c_n|<r_n$. Let Δ be a polydisc about 0 in $\mathbb{C}^{n-1}$, where $n \geqslant 2$, and let R be the ring of all analytic functions $f(z_1, \ldots, z_{n-1})$ in Δ. As Δ is connected, R is an integral domain (by the identity theorem, Theorem I-6, Gunning & Rossi, 1965). The units of R are the analytic functions which are non-zero throughout Δ. An element of the polynomial ring $R[z_n]$ is called a *pseudopolynomial* in Δ. Let z denote the $(n-1)$-tuple $(z_1, \ldots, z_{n-1})$. A monic pseudopolynomial

$$h(z, z_n) = z_n^m + a_1(z)z_n^{m-1} + \ldots + a_m(z)$$

of positive degree m, such that $a_i(0)=0$ for each i, $1 \leqslant i \leqslant m$, is called a *Weierstrass polynomial* in Δ. The Weierstrass preparation theorem (Theorem 62, Chapter 9, Kaplan, 1966) states that every analytic function $f(z, z_n)$ defined in some neighbourhood of the origin in $\mathbb{C}^n$ either does not vanish at 0, or is associated to a Weierstrass polynomial in some polydisc about 0 (provided that $f(0, z_n)$ does not vanish identically).

Let f be an analytic function defined in some open domain U of K^n. Let p be a point of U. We say that f has *order* k at p, and write $\operatorname{ord}_p f = k$, provided that k is the least non-negative integer such that some partial derivative of f of order k does not vanish at p. If all partial derivatives of all orders vanish at p, then we say f has order ∞ at p, and write $\operatorname{ord}_p f = \infty$.

Let x denote $(x_1, \ldots, x_n)$. A mapping $G(x)=(g_1(x), \ldots, g_m(x))$ from the open subset U of K^n into the open subset V of K^m is said to be analytic if each of the component functions g_j is analytic. Where $f: V \to K$ is an analytic function and $G: U \to V$ is an analytic mapping, the composite function $f_o G$ of f and G is analytic, and its power series expansion about any point p of U can be obtained by formal substitution of the power series expansions about p of the component functions of G into the power series expansion about $G(p)$ of f (Bochner & Martin, 1948, p. 33). The following theorem is an immediate consequence of this fact:

THEOREM 2.1. *Let $U \subseteq K^n$ and $V \subseteq K^m$ be open sets, let $G: U \to V$ be an analytic mapping, and let $f: V \to K$ be an analytic function. Then, for every point p of U,*

$$\operatorname{ord}_{G(p)} f \leqslant \operatorname{ord}_p f_o G.$$

2.2. ANALYTIC SUBMANIFOLDS OF EUCLIDEAN SPACE

The original cad algorithm decomposes $\mathbb{R}^n$ into semi-algebraic subsets which Collins (1975) called *cells*. It was subsequently observed (Kahn, 1978) that the cells produced by this decomposition of n-space are actually bona fide cells in the sense of topology: that is, each cell is homeomorphic to an open unit ball in $\mathbb{R}^i$, for some i, $0 \leqslant i \leqslant n$. What is further true is that each cell is homeomorphic to an open unit ball via a mapping which is analytic: this smoothness property of the cells turns out to be quite important in developing an improved projection operation for the cad algorithm.

Before giving a precise definition of an analytic submanifold of $\mathbb{R}^n$ we define the notion of a regular point of an analytic mapping. Let $U \subseteq \mathbb{R}^n$ be open and let $F(x)=(F_1(x), \ldots, F_m(x))$ be an analytic mapping from U into $\mathbb{R}^m$. The point p of U is said

to be a *regular* point of F if the rank of the Jacobian matrix $J_F(p) = (\partial F_i/\partial x_j(p))$ of F at p is equal to m. For example, let $F : \mathbb{R}^3 \to \mathbb{R}$ be defined by $F(x, y, z) = x^2 + y^2 + z^2 - 1$. Then $J_F = (2x, 2y, 2z)$, so every point of $\mathbb{R}^3$ other than the origin is a regular point of F. The non-empty subset S of $\mathbb{R}^n$ is an *analytic submanifold* of $\mathbb{R}^n$ of dimension s if for each point p of S there is a neighbourhood $W \subseteq \mathbb{R}^n$ of p and an analytic mapping $F : W \to \mathbb{R}^{n-s}$ which has p as a regular point, such that

$$S \cap W = \{x \in W : F(x) = 0\}.$$

The only kind of submanifold we shall consider in this paper is the analytic kind. Thus, we shall henceforth omit the term "analytic" when referring to submanifolds: all submanifolds will be understood to be analytic. For example, let

$$S^2 = \{(x, y, z) \in \mathbb{R}^3 : x^2 + y^2 + z^2 = 1\}$$

be the unit sphere in $\mathbb{R}^3$. For each point p in S^2 we may take $W = \mathbb{R}^3$ and $F : W \to \mathbb{R}$ to be the map $F(x, y, z) = x^2 + y^2 + z^2 - 1$. As noted above, F is regular at every point $p \neq 0$, and hence at every point p of S^2. Thus S^2 is a submanifold of $\mathbb{R}^3$ of dimension 2.

Let U and V be open subsets of $\mathbb{R}^n$. A homeomorphism $\Phi : U \to V$ such that both Φ and Φ^{-1} are analytic mappings is called an analytic isomorphism. Such a mapping Φ is also called a *coordinate system* in U; if $p \in U$, $0 \in V$, and $\Phi(p) = 0$, then Φ is called a coordinate system (in U) *about* p. The next theorem expresses the intuitive idea that a submanifold of $\mathbb{R}^n$ of dimension s is a set which "looks locally like Euclidean s-space".

THEOREM 2.2. *The non-empty subset S of $\mathbb{R}^n$ is a submanifold of $\mathbb{R}^n$ of dimension s, where $0 \leqslant s \leqslant n$, if and only if for every point p of S there is a neighbourhood $U \subseteq \mathbb{R}^n$ of p and a coordinate system $\Phi : U \to V$, $\Phi = (\phi_1, \ldots, \phi_n)$, about p such that*

$$S \cap U = \{x \in U : \phi_{s+1}(x) = 0, \ldots, \phi_n(x) = 0\}. \tag{2.1}$$

REMARK. If $\Phi = (\phi_1, \ldots, \phi_n)$ is a coordinate system about the point p, one often identifies $(y_1, \ldots, y_n)$ with $(\phi_1, \ldots, \phi_n)$ and speaks of the y-coordinates about p. Equation 2.1 can then be paraphrased "S is defined near p by the equations $y_{s+1} = 0, \ldots, y_n = 0$ in the y-coordinate system". Theorem 2.2 above is essentially Lemma 4F of Appendix II in Whitney (1972).

3. Cad construction using reduced projection map

Let A be a finite set of r-variate integral polynomials. An *A-invariant cylindrical algebraic decomposition* (*cad*) of $\mathbb{R}^r$ partitions $\mathbb{R}^r$ into a finite collection of cylindrically-arranged semialgebraic cells in each of which every polynomial in A is sign-invariant. A more precise definition of cad is given by Arnon *et al.* (1984*a*).

The cad algorithm (Arnon *et al.*, 1984*a*) accepts as input a finite set A of integral polynomials in r variables, and yields as output a description of an A-invariant cad D of $\mathbb{R}^r$. The description of D takes the form of a list of cell indices and sample points for the cells of D. The algorithm consists of three phases: projection (computing successive sets of polynomials in one fewer variables, the zeros of each set containing a "shadow" of the "critical" zeros in the next higher dimensional space), base (constructing a cad of $\mathbb{R}^1$), and extension (successive extension of the cad of $\mathbb{R}^i$ to a cad of $\mathbb{R}^{i+1}$, $i = 1, 2, \ldots, r-1$). Each of these phases is described by Arnon *et al.* (1984*a*).

The key component of the projection phase is the projection operation: the *projection*

PROJ(A) of a set A of r-variate integral polynomials is defined to be a certain set of $(r-1)$-variate integral polynomials.

In this section the map *PROJ* from Collins (1975) or Arnon *et al.* (1984*a*) is reviewed, and a new projection map P is defined. The map P is essentially just a reduced version of the original projection map *PROJ*. It is proved that, for an input set A of trivariate polynomials with integer coefficients, one can use the map P in place of its larger counterpart *PROJ* in constructing an A-invariant cad of $\mathbb{R}^3$.

In order to define the maps *PROJ* and P we first need to recall some definitions and notation from Collins (1975) or Arnon *et al.* (1984*a*). Let R be any commutative ring and let $f(x)$ be a polynomial over R. We denote by deg (f) the degree of $f(x)$, and take deg $(0) = -\infty$. We denote by *red* (f) the *reductum* of $f(x)$, that is, the difference of $f(x)$ and the leading term of $f(x)$ (*red* $(0) = 0$). We let *red*^{k} (f) denote the kth reductum of $f(x)$. Let $f(x)$ and $g(x)$ be non-zero polynomials over R, with deg $(f) = m$ and deg $(g) = n$. For $0 \leqslant j \leqslant \min(m, n)$, let $psc_j(f, g)$ denote the jth *principal subresultant coefficient* of f and g, that is, the coefficient of x^j in $S_j(f, g)$, the jth subresultant of f and g. Note that $psc_0(f, g)$ is the resultant of f and g, *res* (f, g).

Assume now that R is an integral domain, and let $f(x)$ be a polynomial over R of degree $m \geqslant 1$. Where a is the leading coefficient of $f(x)$, and $\alpha_1, \ldots, \alpha_m$ are the m roots of $f(x)$ in some algebraic closure of the quotient field of R, define the *discriminant* of $f(x)$, *discr*(f), as follows:

$$discr(f) = a^{2m-2} \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

Let $f'(x)$ denote the derivative of $f(x)$. The following well-known theorem (Lang, 1984, Proposition V-10.5) relates *discr*(f) to *res*(f, f').

THEOREM 3.0. *Let R be an integral domain and let $f(x)$ be a polynomial of degree $m \geqslant 1$ over R with leading coefficient a. Assume that the characteristic of R,* char R *does not divide m. Then*

$$a\, discr(f) = (-1)^{m(m-1)/2} res(f, f').$$

COROLLARY. *With the hypotheses of the theorem, discr(f) is seen to be a polynomial in the coefficients of $f(x)$.*

Assume char R does not divide m. For $0 \leqslant j \leqslant \deg(f) - 1$, define the jth *principal subdiscriminant* of f, $psd_j(f)$, by the equation

$$a\, psd_j(f) = (-1)^{m(m-1)/2} psc_j(f, f').$$

Note that $psd_j(f)$ is a polynomial in the coefficients of $f(x)$ as a is a factor of $psc_j(f, f')$, and that $psd_0(f) = discr(f)$.

Let $\mathbb{Z}[x_1, \ldots, x_r]$ denote the ring of all integral polynomials in $x_1, \ldots, x_r$. We regard the elements of $\mathbb{Z}[x_1, \ldots, x_r]$ as polynomials in x_r over $\mathbb{Z}[x_1, \ldots, x_{r-1}]$. Thus, for example, the degree deg(f) of a polynomial f in $\mathbb{Z}[x_1, \ldots, x_r]$ means the degree of f in x_r. Let A be a set of polynomials in $\mathbb{Z}[x_1, \ldots, x_r]$. We now define several sets of $(r-1)$-variate polynomials. The *coefficient set of A*, *coeff*(A), is the set of all non-zero coefficients of all elements of A. The *reducta set of A*, *red*(A), is the set of all *red*$^k(f)$ such that f belongs to A and $0 \leqslant k \leqslant \deg(f)$ The *principal subdiscriminant set of A*, *psd*(A), is the set of all $psd_j(f)$ such that f belongs to A and $0 \leqslant j < \deg(f) - 1$. The *discriminant set*

of A, *discr*(A), is the subset of *psd*(A) consisting of all discriminants of all elements f of A with $\deg(f) > 1$. The *principal subresultant coefficient set of A*, *psc*(A), is the set of all $psc_j(f, g)$, such that f and g are elements of A with $f \neq g$ and $0 \leqslant j < \min(\deg(f), \deg(g))$. The *resultant set of A*, *res*(A), is the subset of *psc*(A) consisting of all resultants of elements f and g of A, with $f \neq g$ and $\deg(f)$ and $\deg(g)$ both positive.

We can now define *PROJ*(A) and $P(A)$:

$$PROJ(A) = coeff(A) \cup psd(red(A)) \cup psc(red(A));$$
$$P(A) = coeff(A) \cup discr(A) \cup res(A).$$

REMARKS.

(1) $P(A)$ is a subset of *PROJ*(A).

(2) If A has m elements, with the degree of each polynomial in each variable at most n, then *PROJ*(A) has $0(m^2n^3)$ elements, whereas $P(A)$ has only $0(mn+m^2)$ elements.

(3) These definitions of the projection maps have been kept conceptually simple for ease of exposition. In practice, there may be elementary improvements that can be made to reduce the size of the sets *PROJ*(A) and $P(A)$. Some of these will be discussed in section 6.

Recall a couple of basic concepts from Collins (1975). A set A of polynomials in $\mathbb{Z}[x_1, \ldots, x_r]$ is said to be a *squarefree basis* if the elements of A have positive degree, and are primitive, squarefree and pairwise relatively prime. Let x denote the $(r-1)$-tuple $(x_1, \ldots, x_{r-1})$. An r-variate polynomial $f(x, x_r)$ over the reals is said to be *delineable* on a subset S (usually connected) of $\mathbb{R}^{r-1}$ if

(1) the portion of the real variety of f that lies in the cylinder $S \times \mathbb{R}$ over S consists of the union of the graphs of some $k \geqslant 0$ continuous functions $\theta_1 < \ldots < \theta_k$ from S to $\mathbb{R}$: and

(2) there exist integers $m_1, \ldots, m_k \geqslant 1$ such that for every $a \in S$, the multiplicity of the root $\theta_i(a)$ of $f(a, x_r)$ (considered as a polynomial in x_r alone) is m_i.

(Remark that if f has no zeros in $S \times \mathbb{R}$, then f is delineable on S as we may take $k = 0$ in this definition.) In the above definition, the θ_i are sometimes called the *real root functions* of f on S, the graphs of the θ_i are called the *f-sections* over S, and the regions between successive f-sections are called *f-sectors*.

One more definition: let $K = \mathbb{R}$ or $\mathbb{C}$ and let U be an open subset of K^r; an analytic function $f: U \to K$ is said to be *order-invariant* in a subset S of U provided that the order of f (see section 2) is the same at every point of S.

Remark that if $K = \mathbb{R}$, and if the analytic function $f: U \to K$ is order-invariant in the connected subset S of U, then f is sign-invariant in S.

An example: let $\mathbb{R}^2 \to \mathbb{R}$ be given by $f(x, y) = x^2 - y^2$. Let C_f be the curve defined by $f(x, y) = 0$ and let $S = C_f - \{0\}$. Then f is order-invariant in S ($\mathrm{ord}_{(x_0, y_0)} f = 1$ for every point (x_0, y_0) of S). However, f is not order-invariant in C_f ($\mathrm{ord}_{(0,0)} f = 2$) (but f is sign-invariant in C_f).

The main result pertaining to P follows.

THEOREM 3.1. *Let A be a finite squarefree basis of integral polynomials in r variables, where $r = 2$ or 3. Let S be a connected submanifold of $\mathbb{R}^{r-1}$ of positive dimension. Suppose that each element of $P(A)$ is order-invariant in S. Then each element of A is delineable on S, and*

the sections of the elements of A over S are pairwise disjoint. Moreover, if $r = 2$, then every such section is a submanifold of $\mathbb{R}^2$ and is order-invariant with respect to each element of A.

REMARKS.

(1) The counterpart of Theorem 3.1 for the map *PROJ* is Theorem 5 from Collins (1975) (also stated as Theorem 3.4 by Arnon *et al.*, 1984*a*). The proof of Theorem 5 from Collins (1975) makes essential use of the fundamental theorem of polynomial remainder sequences (Brown & Traub, 1971).

(2) Theorem 3.1 has a generalisation to arbitrary r reported in McCallum (1984): this generalisation requires an additional hypothesis, namely, that each element of A does not vanish identically on S (an r-variate polynomial $f(x_1, \ldots, x_r)$ over $\mathbb{R}$ is said to *vanish identically* on a subset S of $\mathbb{R}^{r-1}$ if $f(p, x_r) = 0$ for every point p of S). The conclusions, however, are stronger: each element f of A is *analytic-delineable* on S in the sense that the sections of f over S are the graphs of analytic functions defined in S; moreover, each element of A is order-invariant in every such section.

Theorem 3.1 can be quite readily derived from the following theorem (an r-variate polynomial $f(x_1, \ldots, x_r)$ over $\mathbb{R}$ is said to be *degree-invariant* on the subset S of $\mathbb{R}^{r-1}$ if the degree of $f(p, x_r)$ (as a polynomial in x_r) is the same for every point p of S):

THEOREM 3.2. *Let x denote the $(r-1)$-tuple $(x_1, \ldots, x_{r-1})$. Regard elements of $\mathbb{R}[x, x_r]$ as polynomials in x_r over $\mathbb{R}[x]$. Let $r = 2$ or 3. Let $f(x, x_r)$ be a polynomial of positive degree in $\mathbb{R}[x, x_r]$, let $D(x)$ be the discriminant of $f(x, x_r)$, and suppose that $D(x) \neq 0$. Let S be a connected submanifold of $\mathbb{R}^{r-1}$ on which f is degree-invariant and not identically vanishing, and in which D is order-invariant. Then f is delineable on S. Moreover, if $r = 2$, then every f-section over S is a submanifold of $\mathbb{R}^2$ and is order-invariant with respect to f.*

Theorem 3.2. can, in turn, be derived in a straightforward manner from the following (recall the definition of Weierstrass polynomial given in section 2):

THEOREM 3.3 (Zariski). *Let $h(x, y, z)$ be a Weierstrass polynomial of degree $m \geqslant 1$ in the polydisc Δ_1 about 0 in $\mathbb{C}^2$, and assume that for every fixed (x, y) in Δ_1, every root of $h(x, y, z)$ (considered as a polynomial in z alone) is contained in the disc $|z| < \varepsilon$. Let $F(x, y)$ be the discriminant of $h(x, y, z)$, and assume that F does not vanish identically. Let $T* = \{(x, 0) | x \in \mathbb{C}\}$ be the complex x-axis in $\mathbb{C}^2$, and assume that F is order-invariant in $T* \cap \Delta_1$. Then there exists a polydisc $\Delta_2 \subseteq \Delta_1$ about 0 such that for every fixed $(x, 0)$ in $T* \cap \Delta_2$, $h(x, 0, z)$ (as a polynomial in z) has exactly one root (necessarily of multiplicity m) in the disc $|z| < \varepsilon$.*

This theorem follows from Theorem 4.5 in Zariski (1965). The setting for Zariski's formulation of the theorem is more abstract than ours (he works over an arbitrary algebraically closed field of characteristic zero). In fact, a reader unfamiliar with abstract algebraic geometry may have difficulty discerning the relationship between our Theorem 3.3 and Zariski's Theorem 4.5. So that our presentation is as self-contained as possible, we present in Section 5 a proof of Theorem 3.3. Our exposition is different from Zariski's.

REMARK. The generalisation of Theorem 3.1 mentioned above takes quite a bit longer to prove than Theorem 3.1 itself. The proof is again based on work of Zariski (1975).

Another paper is planned to expose this generalisation and its proof. Parts of this present paper readily generalise to arbitrary r, and will be used in the forthcoming sequel.

We now present the

PROOF OF THEOREM 3.1. There is nothing to prove if A is empty, so assume A is non-empty. Let $A = \{f_1, \ldots, f_m\}$ and let f be the product of the f_i. Let x denote the $(r-1)$-tuple $(x_1, \ldots, x_{r-1})$, and let $D(x)$ be the discriminant of $f(x, x_r)$. By Lemma A.1 and Theorem 3 of Loos (1982),

$$D = \prod_{i=1}^{m} discr(f_i) \cdot \prod_{1 \leqslant i < j \leqslant m} res(f_i, f_j)^2.$$

It follows from this equation that $D(x) \neq 0$ (because each $discr(f_i)$ and each $res(f_i, f_j)$ are non-zero, as the f_i are squarefree and pairwise relatively prime). Now f is degree-invariant on S, as each element of $coeff(A)$ is order-invariant, hence sign-invariant, in S. Moreover, f is primitive (as the f_i are primitive) and hence, by Lemma A.2, f does not vanish identically on S (S has positive dimension and therefore comprises an infinite set of points). By hypothesis, each $discr(f_i)$ and each $res(f_i, f_j)$ are order-invariant in S. Hence, by Lemma A.3, D is order-invariant in S. Hence, by Theorem 3.2, f is delineable on S. Moreover, if $r = 2$, then every f-section over S is a submanifold of $\mathbb{R}^2$ and is order-invariant with respect to f. Therefore, by Lemma A.7, every f_i is delineable on S. It follows that the sections over S of all the f_i are pairwise disjoint. Moreover, if $r = 2$, then by Lemma A.3, each f_i is order-invariant in every such section. □

The proofs of Theorems 3.2 and 3.3 occupy the next two sections respectively.

We now present a cad construction algorithm *CADR*3 which can be applied to any set A of polynomials in r variables, where $1 \leqslant r \leqslant 3$, yielding a list of cell indices and sample points for an A-invariant cad D of $\mathbb{R}^r$. The algorithm *CADR*3 is modelled on the algorithm *CAD* from Arnon *et al.* (1984*a*), which is in turn a summary of algorithm *DECOMP* from Collins (1975).

Apart from the restriction on r in *CADR*3, there are two differences between *CADR*3 and *CAD*. The main difference is that in *CADR*3 the map P is used in place of the map *PROJ*. The other difference is that while squarefree basis computation is optional in *CAD* (Collins, 1975, p. 152), it is essential in *CADR*3 (because of the hypotheses of Theorem 3.1).

Some definitions first: let A be a subset of $\mathbb{Z}[x_1, \ldots, x_r]$, where $r \geqslant 1$. Define $cont(A)$ to be the set of non-zero non-unit contents of the elements of A. Define $prim(A)$ to be the set of those primitive parts of elements of A that have positive degree. Now suppose that A consists of primitive polynomials of positive degree. The *finest squarefree basis for* A is the set of all ample irreducible factors of the elements of A (see Collins, 1975, p. 146)

$$CADR3(r, A; I, S)$$

Inputs: r is an integer with $1 \leqslant r \leqslant 3$. A is a list of r-variate integral polynomials.
Outputs: I is a list of the indices of the cells comprising an A-invariant cad D of $\mathbb{R}^r$. S is a list of sample points for D.

(1) [Initialise.] Set $B \leftarrow$ the finest squarefree basis for $prim(A)$ (algorithms for polynomial factorization are given by Kaltofen, 1982). Set $I \leftarrow$ the empty list. Set $S \leftarrow$ the empty list.

(2) [$r = 1$.] If $r > 1$ then go to 3. Isolate the real roots of B. Construct the indices of the cells of D (as described by Arnon *et al.*, 1984*a*) and add them to I. Construct

sample points for the cells of D (as described by Arnon *et al.*, 1984*a*) and add them to S. Exit.

(3) [$r > 1$.] Set $P \leftarrow cont(A) \cup P(B)$. Call $CADR3$ recursively with inputs $r-1$ and P to obtain outputs I' and S' which specify a P-invariant cad D' of $\mathbb{R}^{r-1}$. For each cell c of D', let i denote the index of c and let α denote the sample point for c; carry out the following sequence of steps: set $f_*(x_r) \leftarrow$ the product of all the $f(\alpha, x_r)$ such that $f \in B$ and $f(\alpha, x_r) \neq 0$; ($f_*(x_r)$ is constructed using exact arithmetic in $Q(\alpha)$, Loos, 1982); isolate the real roots of $f_*(x_r)$ (Loos, 1982, section 2); use i, α and the isolating intervals for the roots of f_* to construct cell indices and sample points (as described by Arnon *et al.*, 1984*a*) for the sections and sectors over c of those elements of B that are not identically zero on c; add the new indices to I and the new sample points to S. Exit. □

It is straightforward to prove the validity of algorithm $CADR3$ using Theorem 3.1.

REMARKS.

(1) Step 1 of $CADR3$ prescribes the computation of the *finest* squarefree basis for $prim(A)$. In fact, if $r > 1$, then *any* squarefree basis for $prim(A)$ can be computed in this step (see Collins, 1975, for the definition of a squarefree basis *for* a set of polynomials).

(2) The generalisation of Theorem 3.1 mentioned above can be used to prove the validity of a cad construction algorithm (McCallum, 1984) for arbitrary r in which the map P is used in place of the map $PROJ$ provided that the input set of polynomials is assumed to be *well-oriented* (a set A of r-variate polynomials over $\mathbb{R}$ is said to be *well-oriented* if no element of $prim(A)$ vanishes identically on any submanifold of $\mathbb{R}^{r-1}$ of positive dimension and, moreover, this property holds recursively for the set $cont(A) \cup P(B)$, where B is the finest squarefree basis for $prim(A)$).

4. Proof of Theorem 3.2.

We assume that S has positive dimension. (The dimension 0 case is trivial.) By connectedness of S, it suffices to show that f is delineable on S near an arbitrary point p of S. That is, it is enough to show that for every point p of S, there exists a neighbourhood $N \subseteq \mathbb{R}^{r-1}$ of p such that f is delineable on $S \cap N$ (and that, if $r = 2$, then every f-section over $S \cap N$ is a submanifold of $\mathbb{R}^2$ and is order-invariant with respect to f). Let p be a point of S, and let the degree of $f(p, x_r)$ (considered as a polynomial in x_r alone) be l. Then $l \geqslant 0$ (that is, $f(p, x_r)$ is not the zero polynomial), as f is degree-invariant and not identically vanishing on S.

Let $\alpha_1 < \ldots < \alpha_k$, $k \geqslant 0$, be the real roots of $f(p, x_r)$, let $\alpha_{k+1}, \ldots, \alpha_t$, $k \leqslant t$, be the distinct non-real roots of $f(p, x_r)$, and let m_i be the multiplicity of the root α_i, for $1 \leqslant i \leqslant t$. Let

$$\kappa = \min(\{|\alpha_i - \alpha_j| : 1 \leqslant i < j \leqslant t\} \cup \{1\}).$$

Let $0 < \varepsilon < \kappa/2$, and let C_i be the circle of radius ε centred at α_i, $1 \leqslant i \leqslant t$. By root continuity (Theorem (1,4), Marden, 1966) and degree-invariance of f on S, there exists a neighbourhood $N_0 \subseteq \mathbb{R}^{r-1}$ of p such that for every fixed point x of $S \cap N_0$, the interior of each C_i contains exactly m_i roots (multiplicities counted) of $f(x, x_r)$ (considered as a polynomial in x_r alone).

To prove the delineability of f on S near p, it suffices to show that for each i, $1 \leqslant i \leqslant k$, there exists a neighbourhood $N_i \subseteq N_0$ of p such that for every fixed $x \in S \cap N_i$, the interior of C_i contains exactly one root, say $\theta_i(x)$ of $f(x, x_r)$ (considered as a polynomial in x_r alone), necessarily of multiplicity m_i and necessarily real. (For if this has been shown, then let

$$N = \bigcap_{i=0}^{i} N_i.$$

By root continuity, each θ_i is continuous in $S \cap N$. Let (p', α') be a point belonging to the cylinder $(S \cap N) \times \mathbb{R}$ over $S \cap N$, and assume $f(p', \alpha') = 0$. By degree-invariance of f on S, the degree of $f(p', x_r)$ is l. As $p' \in S \cap N \subseteq S \cap N_0$, the interior of each C_i, $1 \leqslant i \leqslant t$, contains exactly m_i roots (multiplicities counted) of $f(p', x_r)$. Since

$$\sum_{i=1}^{t} m_i = l,$$

every root of $f(p', x_r)$ is contained within one of the C_i. Each C_i with $k+1 \leqslant i \leqslant t$ contains no real points, however, as the non-real roots of $f(p, x_r)$ occur in conjugate pairs. Hence, as α' is a real root of $f(p', x_r)$, α' must lie inside a C_i with $1 \leqslant i \leqslant k$, so $\alpha' = \theta_i(p')$. This proves that f is delineable on $S \cap N$.)

We now proceed to prove that for each i, with $1 \leqslant i \leqslant k$, there exists a neighbourhood $N_i \subseteq N_0$ of p such that for every fixed $x \in S \cap N_i$, the interior of C_i contains exactly one root, say $\theta_i(x)$, of $f(x, x_r)$ (as a polynomial in x_r), necessarily of multiplicity m_i. (It will be shown that, informally speaking, each real root α_i of $f(p, x_r)$ does not "split" into many roots as p is perturbed a little within S.)

That the root α_i does not split into many roots as p is perturbed a little within S is quite easy to see in the case in which the dimension of S is equal to $r-1$. For in this case, S is an open subset of $\mathbb{R}^{r-1}$. Hence, as f is degree-invariant on S, the leading coefficient of f (with respect to x_r) vanishes nowhere in S. Also, as $D(x)$, a non-zero polynomial, is order-invariant in S, D vanishes nowhere in S. Therefore, for fixed $x \in S$, every root of $f(x, x_r)$ (as a polynomial in x_r) is simple; hence $m_i = 1$. It follows that the graph of each real root function $\theta_i : S \cap N_0 \to \mathbb{R}$ is a submanifold of $\mathbb{R}^r$ (of dimension $r-1$) and is order-invariant with respect to f (because $x_r = \theta_i(x)$ if and only if $f(x, x_r) = 0$, for all $(x, x_r) \in (S \cap N_0) \times C_i$, and $\partial f / \partial x_r \neq 0$ in the graph of θ_i).

The remaining case to consider is that in which $r = 3$ and the dimension of S is 1, that is, S is a smooth curve in the plane. For the remainder of the proof, let (x, y, z) denote the triple (x_1, x_2, x_3), and let the coordinates of the point p be (a, b). There is no loss of generality in assuming that $\alpha_i = 0$. By Theorem 2.2, we choose coordinates (u, v) about the point p such that S is defined locally by the equation $v = 0$ in the new coordinate system. Let $g(u, v, z)$ denote the function $f(x, y, z)$ transformed into the new coordinates (that is, if Φ is the coordinate system mapping from the (x, y)-plane to the (u, v)-plane, then $g(u, v, z) \sim f(\Phi^{-1}(u, v), z)$). Then $g(u, v, z)$ is a polynomial in z whose coefficients are (real) analytic functions of (the real variables) u and v, defined near the origin (the analyticity here comes from the analyticity of the coordinate system mapping Φ). The discriminant $E(u, v)$ of $g(u, v, z)$ is analytic near 0, and is order-invariant in the u-axis near 0, by Theorem 2.1.

Each coefficient of $g(u, v, z)$ can be expanded in a convergent double power series about 0 (by definition of analyticity). By the two-variable analogue (Theorems 54–56 of Kaplan, 1966) of a well-known result on convergence, each of these double power series is absolutely convergent in a polydisc $\Delta_1 : |u| < r_1, |v| < s_1$ about 0 in complex 2-space $\mathbb{C}^2$,

and sums to a function that is analytic in Δ_1. In this way, each coefficient of $g(u, v, z)$, and hence also $g(u, v, z)$ itself, can be extended (uniquely) to a neighbourhood of 0 in $\mathbb{C}^2$. We do not use new notation for this extension of g: henceforth, $g(u, v, z)$ will denote the complex pseudopolynomial (section 2.1) that extends the real g. It is not difficult to show (Lemma A.4) that the discriminant $E(u, v)$ of $g(u, v, z)$ is order-invariant in the complex u-axis $T*$ near 0 (the complex u-axis is the subset $\{(u, 0)|u \in \mathbb{C}\}$). By refining Δ_1 to a smaller polydisc about 0 if necessary, let us assume that $E(u, v)$ is order-invariant in $T* \cap \Delta_1$.

It will be shown that the root $\alpha_i = 0$ of $g(0, 0, z)$ does not split into many roots as $(u, v) = (0, 0)$ is perturbed a little within $T*$. (This will imply, in the old coordinates, the desired result that the root α_i of $f(a, b, z)$ does not split into many roots as (a, b) is perturbed a little within S.) To do this, it will be convenient to focus attention on the zero set of $g(u, v, z)$ near the origin in $\mathbb{C}^3$, using the Weierstrass preparation theorem (Theorem 62 of Kaplan, 1966; see also section 2.1 of the present paper) from the theory of several complex variables. Recall that $\alpha_i = 0$ is a root of $g(0, 0, z)$ of multiplicity $m := m_i$, and that $g(0, 0, z) \neq 0$ for $0 < |z| \leqslant \varepsilon$. By the Weierstrass preparation theorem, there is a polydisc $\Delta_2 \subseteq \Delta_1$, a function $q(u, v, z)$ analytic and nowhere-vanishing in the polydisc $\Delta' : (u, v) \in \Delta_2$, $|z| < \varepsilon$, and a Weierstrass polynomial

$$h(u, v, z) = z^m + a_1(u, v)z^{m-1} + \ldots + a_m(u, v)$$

in Δ_2, such that

$$g(u, v, z) = q(u, v, z)h(u, v, z) \tag{3.1}$$

for all $(u, v, z) \in \Delta'$, and such that for each fixed $(u, v) \in \Delta_2$, all the m roots of $h(u, v, z)$ (as a polynomial in z) are contained in the disc $|z| < \varepsilon$. By (3.1), as $q(u, v, z) \neq 0$ for all $(u, v, z) \in \Delta'$, the zero set of g is the same as that of h, in Δ'. Thus, the non-splitting of the root $\alpha_i = 0$ of $g(0, 0, z)$ as $(u, v) = (0, 0)$ is perturbed a little within $T*$ will follow from the non-splitting of the root $\alpha_i = 0$ of $h(0, 0, z)$. But the non-splitting of the root $\alpha_i = 0$ of $h(0, 0, z)$ as $(u, v) = (0, 0)$ is perturbed a little within $T*$ is precisely the conclusion of Theorem 3.3. It remains to show that the hypotheses of Theorem 3.3 are satisfied.

Let $F(u, v)$ be the discriminant of $h(u, v, z)$: we shall prove that F does not vanish identically, and that F is order-invariant in $T* \cap \Delta_2$. To do this we first need to take a closer look at the function q: this is done in the proof of Lemma A.5, whose conclusion is that $q(u, v, z)$ is, in fact, a pseudopolynomial in Δ_2. We shall find a function $Q(u, v)$, analytic in Δ_2, such that

$$E(u, v) = Q(u, v)F(u, v) \tag{3.2}$$

for all $(u, v) \in \Delta_2$. Let d be the degree of $g(u, v, z)$. If $d > m$, in which case $q(u, v, z)$ has positive degree $d - m$, then set

$$Q(u, v) = G(u, v)R(u, v)^2,$$

where $G(u, v)$ is the discriminant of $q(u, v, z)$ and $R(u, v)$ is the resultant of $q(u, v, z)$ and $h(u, v, z)$. Equation (3.2) holds by Lemma A.1. If $d = m$, in which case $q(u, v, z) = q(u, v)$ has degree 0, then set

$$Q(u, v) = q(u, v)^{2m-2}.$$

Equation (3.2) holds by the definition of discriminant. Now it follows by (3.2) that F does not vanish identically (as $D(x, y)$, hence $E(u, v)$, does not vanish identically). Furthermore, by Lemma A.3, F is order-invariant in $T* \cap \Delta_2$. The hypotheses of

Theorem 3.3 are satisfied. Hence, by Theorem 3.3, there exists a polydisc $\Delta_3 \subseteq \Delta_2$ about 0 such that for every fixed $(u, v) \in T* \cap \Delta_3$, $h(u, v, z)$ (as a polynomial in z) has exactly one root (necessarily of multiplicity m) in the disc $|z| < \varepsilon$. Hence, by (3.1), the same holds true for $g(u, v, z)$, and the desired conclusion as to the non-splitting of the root α_i of $f(a, b, z)$ as (a, b) is perturbed a little within S now follows. Theorem 3.2 has been proved. □

5. Proof of Theorem 3.3 (and Lemmas)

Let Δ be a polydisc about 0 in $\mathbb{C}^{n-1}$, where $n \geqslant 2$, and let R be the ring of all analytic functions $f(z_1, \ldots, z_{n-1})$ in Δ. We have noted previously that R is an integral domain, and have called an element of the polynomial ring $R[z_n]$ a *pseudopolynomial* in Δ. Now R is not a unique factorisation domain (Whitney, 1972, Appendix IV, Example 2C) and, hence, neither is $R[z_n]$. However, it follows by induction on the degree that every monic pseudopolynomial h of positive degree can be factored as a product of monic irreducible psuedopolynomials thus:

$$h = h_1 \ldots h_k.$$

It will follow from Lemma 5.2 below that the h_i are uniquely determined, provided that the discriminant of h (an element of R) does not vanish identically.

We use the notation $z = (z_1, \ldots, z_{n-1})$. Let U be an open subset of $\mathbb{C}^{n-1}$. A continuous function $\Gamma: [0, 1] \to U$, such that $\Gamma(0) = w_0$ and $\Gamma(1) = w_1$, is called a *path* in U from w_0 to w_1.

LEMMA 5.1. *Let Δ be a polydisc about 0 in $\mathbb{C}^{n-1}$ and let $h(z, z_n)$ be a monic pseudopolynomial of positive degree in Δ. Let U be an open subset of Δ in which the discriminant of h vanishes nowhere. Let p and q be points of U, not necessarily distinct, and let Γ be a path in U from p to q. Let α be a root of $h(p, z_n)$ (a polynomial in z_n). Then there exists a unique path ϕ in $\mathbb{C}^1$ such that $\phi(0) = \alpha$ and $h(\Gamma(t), \phi(t)) = 0$ for all $t \in [0, 1]$.*

PROOF. Let the degree of h be m, let $V = \{(z, z_n) \in U \times \mathbb{C} | h(z, z_n) = 0\}$, and let w be a point of U. As h is monic and the discriminant of h is non-zero at w, $h(w, z_n)$ (as a polynomial in z_n) has m distinct, simple roots. By m applications of the implicit function theorem (Gunning & Rossi, 1965, Theorem I-4) there exists a neighbourhood $W \subseteq U$ of w such that the portion of V contained in $W \times \mathbb{C}$ consists of the disjoint graphs of m analytic functions from W into $\mathbb{C}$. Hence (Munkres, 1975, Chapter 8), V is an m-fold covering of U, with covering map $\pi: V \to U$ given by $\pi(z, z_n) = z$. The existence and uniqueness of ϕ now follow by the path lifting property (Munkres, 1975, Chapter 8, Lemma 4.1.) □

REMARK. With the notation of the above lemma, we set $\Gamma_h[\alpha] := \phi(1)$ and say Γ *carries* α *into* $\phi(1)$ *(via h)*. We also say α is continued along Γ to $\phi(1)$.

The following is an important lemma about monic irreducible pseudopolynomials:

LEMMA 5.2. *Let Δ be a polydisc about 0 in $\mathbb{C}^{n-1}$ and let $h(z, z_n)$ be a monic irreducible pseudopolynomial in Δ. Let $G(z)$ be the discriminant of $h(z, z_n)$, let $F(z)$ be an analytic function in Δ such that $F(z) \neq 0$ implies $G(z) \neq 0$ for all $z \in \Delta$, and let $U = \{z \in \Delta | F(z) \neq 0\}$. Let $w \in U$ and let α be a root of $h(w, z_n)$ (as a polynomial in z_n). Then for every $w' \in U$ and every root α' of $h(w', z_n)$ (a polynomial in z_n), there exists a path Γ in U from w to w' such that $\Gamma_h[\alpha] = \alpha'$.*

PROOF. A proof of this result, using slightly different notation and terminology, is given by Bochner & Martin (1948, Chapter 9, Sec. 3, pp. 194–198). □

REMARK. The above lemma implies that the monic irreducible factors of a monic pseudopolynomial of positive degree whose discriminant does not vanish identically are uniquely determined.

IDEA OF PROOF OF THEOREM 3.3. The hypothesis as to the order-invariance of the discriminant of h in the complex x-axis near 0 amounts to assuming that the zero set of the discriminant of h is identical with the complex x-axis near 0 (or is empty). Our approach is to consider a monic irreducible factor h_i of h first. Now h_i satisfies the same hypotheses as h. Thus the complement U of the zero set of the discriminant of h_i is topologically the product of a punctured plane and a full plane (or, if the zero set is empty, simply $\mathbb{C} \times \mathbb{C}$). Lemma 5.2 implies that all roots of h_i over U can be obtained from a given root by continuation along some path in U. Furthermore, continuous deformation (or homotopy) of any such path within U yields the same root of h_i. But any such path in U from a point (a, b') to itself can be continuously deformed within U to a path with constant x-value $x = a$. We conclude that $h_i(a, y, z)$, as a pseudopolynomial in y and z, remains irreducible, and hence that there is just one root (necessarily of multiplicity equal to the degree of h_i) of $h_i(a, 0, z)$ (as a polynomial in z). By considering the resultant of the pair of monic irreducible factors h_i, h_j of h we then see that the root of $h_i(a, 0, z)$ must be equal to the root of $h_j(a, 0, z)$. □

We now give the details of the

PROOF OF THEOREM 3.3. By Lemma A.6, there exists a polydisc $\Delta_2 \subseteq \Delta_1$ about 0 such that the zero set of F in Δ_2 is either empty or equal to $T* \cap \Delta_2$. Let (r, s) be the polyradius of Δ_2. Factor h into irreducible Weierstrass polynomials:

$$h = h_1 \ldots h_k.$$

Let $1 \leqslant i \leqslant k$, and let $G(x, y)$ be the discriminant of $h_i(x, y, z)$. By Lemma A.3, G is order-invariant in $T* \cap \Delta_2$ (as G is a factor of F, by Lemma A.1, and F is order-invariant in $T* \cap \Delta_2$, by hypothesis). But the zero set of G in Δ_2 is contained in the zero set of F in Δ_2 (as G is a factor of F). Hence, the zero set of G in Δ_2 is either empty or equal to $T* \cap \Delta_2$.

We shall show that for each point a with $|a| < r$, there exists exactly one distinct root of $h_i(a, 0, z)$ (considered as a polynomial in z). This is clearly true if $G \neq 0$ in Δ_2, as in this case the degree of h_i is 1. Suppose, on the other hand, that the zero set of G in Δ_2 is equal to $T* \cap \Delta_2$, and that for some a with $|a| < r$, $h_i(a, 0, z)$ has $l \geqslant 2$ distinct roots, say $\alpha_1, \ldots, \alpha_l$, with multiplicities $m_1, \ldots, m_l$ respectively. Choose disjoint open discs $D_1, \ldots, D_l$ in the z-plane about $\alpha_1, \ldots, \alpha_l$ respectively. By root continuity of $h_i(a, y, z)$ (considered as a pseudopolynomial in y and z), there exists a disc $D' : |y| < s'$ in the y-plane such that $s' \leqslant s$, and for every fixed b in D', there are exactly m_j roots (counted according to multiplicity) of $h_i(a, b, z)$ (a polynomial in z) in D_j, for $1 \leqslant j \leqslant l$.

Let b' be a non-zero point of D', and let α and β be roots of $h_i(a, b', z)$ in D_1 and D_2 respectively. Let $U = \{(x, y) \in \Delta_2 : G(x, y) \neq 0\}$. Then $U = \Delta_2 - T*$. By Lemma 5.2, there is a path $\Gamma(t) = (\Gamma_x(t), \Gamma_y(t))$ in U from (a, b') to itself such that $\Gamma_{h_i}[\alpha] = \beta$. We can deform Γ in U to a path Γ' in the disc $x = a$, $|y| < s$ (contained in the plane $\{a\} \times \mathbb{C}$) by means of the

path homotopy (Munkres, 1975, Chapter 8)

$$H(u, t) = ((1-u)\Gamma_x(t)+ua, \Gamma_y(t))$$

(for which $0 \leqslant u \leqslant 1$, $H(0, t) = \Gamma(t)$ and $H(1, t) = (a, \Gamma_y(t))$). Furthermore, we can deform Γ' in U to a path Γ'' along the circle $x = a$, $|y| = |b'|$ by means of the path homotopy

$$K(u, t) = \left(a, (1-u)\Gamma_y(t) + \frac{u\Gamma_y(t)|b'|}{|\Gamma_y(t)|}\right).$$

Let ϕ'' be the path in $\mathbb{C}^1$ such that $\phi''(0) = \alpha$ and $h_i(\Gamma''(t), \phi''(t)) = 0$ for all $t \in [0, 1]$, given by Lemma 5.1. By Theorem 4.3 of Chapter 8 of Munkres (1975) $\phi''(1) = \beta$ (which implies $\Gamma''_{h_i}[\alpha] = \beta$). Yet, as $\phi''(t)$ is a root of $h_i(\Gamma''(t), z)$ (a polynomial in z) for each fixed $t \in [0, 1]$, we must have that

$$\phi''(t) \in \bigcup_{j=1}^{l} D_j,$$

for each $t \in [0, 1]$. Hence, as ϕ'' is continuous, the D_j are disjoint, and $\phi''(0) \in D_1$, we must have that $\phi''(t) \in D_1$ for every $t \in [0, 1]$. This contradicts $\phi''(1) = \beta$, as β is an element of D_2. Hence, our assumption that $h_i(a, 0, z)$ has more than one distinct root must be false. Thus $h_i(a, 0, z)$ has exactly one distinct root, for each fixed a in the disc $|a| < r$.

We can now show that $h(a, 0, z)$ has exactly one distinct root, for each fixed a in the disc $|x| < r$. There is nothing further to prove if $k = 1$, so assume $k > 1$. Let $1 \leqslant i < j \leqslant k$ and let $R(x, y)$ be the resultant of $h_i(x, y, z)$ and $h_j(x, y, z)$. By Lemma A.3, R is order-invariant in $T* \cap \Delta_2$ (as R is a factor of F, by Lemma A.1, and F is invariant in $T* \cap \Delta_2$, by hypothesis). But the zero set of R in Δ_2 is contained in the zero set of F in Δ_2 (as R is a factor of F). Hence, the zero set of R in Δ_2 is equal to $T* \cap \Delta_2$ (the zero set of R in Δ_2 is non-empty because $R(0, 0) = 0$). Let $|a| < r$ and let α_i and α_j be the unique roots of $h_i(a, 0, z)$ and $h_j(a, 0, z)$ respectively. Then we must have $\alpha_i = \alpha_j$, as $\alpha_i \neq \alpha_j$ would imply $R(a, 0) \neq 0$. Hence, $h(a, 0, z)$ has exactly one distinct root (necessarily of multiplicity m). Theorem 3.3 has been proved. □

6. Examples

As remarked following the definitions of the projection operators *PROJ* and *P*, there may be elementary improvements that can be made in practice to reduce the size of the sets $PROJ(A)$ and $P(A)$ (where A is a set of r-variate integral polynomials). In fact, as pointed out by Collins (1975, p. 160), we can always use the following set in place of $psc(red(A))$ in the definition of $PROJ(A)$:

$$\{psc_j(red^k(f), red^l(g)) | f, g \in A, f < g, 0 \leqslant k \leqslant \deg(f), \\ 0 \leqslant l \leqslant \deg(g), 0 \leqslant j < \min(\deg(red^k(f)), \deg(red^l(g)))\},$$

where "$<$" is an arbitrary linear ordering of the elements of A. That is to say, one does not need to compute psc_j's of pairs of different reducta of the same element of A. This is incorporated into Arnon *et al.*'s (1984*a*) definition of *PROJ*.

Collins (1975, p. 176) notes that if the first i coefficients of some polynomial f in A can be seen to have only finitely many (or no) common zeros in $\mathbb{R}^{r-1}$, then $red^k(f)$ can be excluded from $red(A)$ for $k \geqslant i$. Moreover, in this case, one need include no more than the first i coefficients of f in $coeff(A)$. Thus, in particular, when the leading coefficient of f is a

non-zero integer constant, $red^k(f)$ can be excluded from $red(A)$ for $k \geqslant 1$, and no coefficients of f need be included in $coeff(A)$.

The algorithms *CAD* from Arnon *et al.* (1984*a*) and *CADR*3 from section 3 of the present paper have been implemented using the SAC-2 computer algebra system. All of the improvements mentioned above have been incorporated into the SAC-2 programs *CAD* and *CADR*3. We remark that the SAC-2 program *CAD*, like *CADR*3, computes finest squarefree bases prior to projection.

Slightly modified versions of the standard SAC-2 programs *CAD* and *CADR*3 have been applied to several examples and observations relating to two of these examples are presented in sections 6.1 and 6.2 respectively. The computing times reported in section 6.1 were measured on a MicroVAX II computer running the MicroVMS operating system, and the times reported in the second subsection were measured on a VAX 11/780 computer running the UNIX operating system.

6.1. CATASTROPHE SURFACE AND SPHERE

Two well-known surfaces are the unit sphere

$$(f(x, y, z) = z^2 + y^2 + x^2 - 1 = 0)$$

and the catastrophe surface

$$(g(x, y, z) = z^3 + xz + y = 0).$$

Each surface by itself would present a quite trivial application of the cad algorithm. However, an interesting example for the algorithm can be made by taking the two surfaces together, that is, taking the input set to be $A = \{f, g\}$.

Regard f and g as polynomials in the main variable z over the ring $\mathbb{Z}[x, y]$. Now A is its own finest squarefree basis. The reduced projection $P(A)$ of A computed by *CADR*3 consists of the discriminant D_f of f, the discriminant D_g of g and the resultant R of f and g:

$$\begin{aligned} D_f &= -4y^2 - 4x^2 + 4 \\ D_g &= -27y^2 - 4x^3 \\ R &= y^6 + 3x^2y^4 - 2xy^4 - 3y^4 + 3x^4y^2 - 4x^3y^2 - 5x^2y^2 + 4xy^2 + 4y^2 + \\ &\quad x^6 - 2x^5 - 2x^4 + 4x^3 + 2x^2 - 2x - 1. \end{aligned}$$

(According to remarks made above it is not necessary to include any coefficients of either f or g in the projection, as f and g are both monic.) The three curves defined by these polynomials are illustrated in Fig. 1. Note that the curve $R = 0$ has an isolated point on the x-axis.

The projection phase of *CADR*3, that is, the computation of the bivariate and univariate projections, took 37·3 seconds. The base phase of the algorithm, that is, the construction of the decomposition of the real line, took 16·4 seconds. The first stage of the extension phase of the algorithm, that is, the construction of the $P(A)$-invariant cad of the plane, took approximately 3 hours and 20 minutes. This cad of the plane is illustrated in Fig. 2. Let the cylinders of this cad be numbered consecutively from left to right, starting at 1. (Then the two-dimensional cylinders or strips have odd numbers and the one-dimensional cylinders or vertical lines have even numbers.) Most of the time for construction of this cad was spent computing sample points for the cells in cylinders 4 and 6.

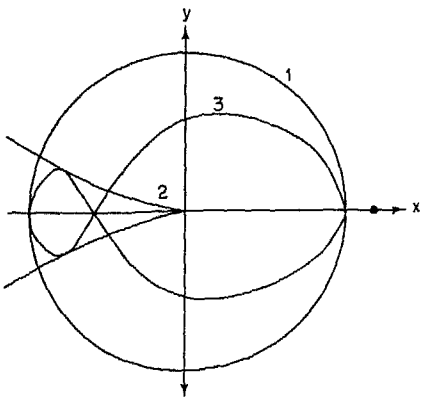

Fig. 1. Where $f(x, y, z) = z^2 + y^2 + x^2 - 1$ and $g(x, y, z) = z^3 + xz + y$, curve 1 is $discr(f) = D_f = 0$, curve 2 is $discr(g) = D_g = 0$, curve 3 is $res(f, g) = R = 0$.

The cad constructed by *CADR*3 actually includes several one-dimensional cylinders containing no portions of any curve. These extraneous cylinders are not included in Fig. 2. Two such extraneous cylinders lie between cylinders 14 and 16, and five of them lie to the right of cylinder 16. These cylinders are defined by certain real roots of the polynomials $discr(R)$, $res(D_f, D_g)$, and $res(D_g, R)$, which real roots correspond to non-real intersections of pairs of the complex curves $R = 0$, $\partial R/\partial y = 0$, $D_f = 0$ and $D_g = 0$.

Figures 1 and 2 were drawn with the help of cell adjacency information which was provided by the algorithm from Arnon *et al.* (1984*b*).

We have not yet attempted to run *CADR*3 long enough to construct an A-invariant cad of $\mathbb{R}^3$.

The projection $PROJ(A)$ of A computed by *CAD* is the set

$$P(A) \cup \{psd_1(g), psc_1(f, g)\},$$

where $psd_1(g) = -6x$ and $psc_1(f, g) = -y^2 - x^2 + x + 1$. (By earlier remarks, no reducta of f or g, except for f and g themselves, need be considered, and no coefficients of f or g need be included in $PROJ(A)$.) The curve $psc_1(f, g) = 0$ is the circle with centre $(1/2, 0)$ and radius $\sqrt{5}/2$. This circle passes through the two real singularities of the curve $R = 0$.

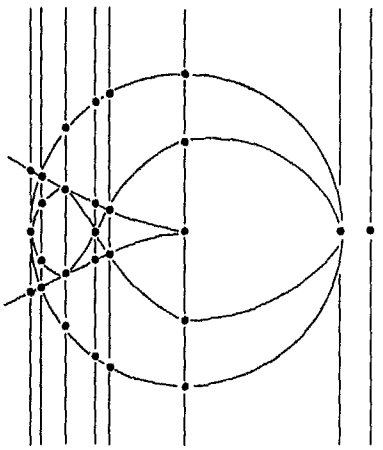

Fig. 2. Cad of the plane for the curves of Fig. 1.

The projection phase of *CAD* took 45·9 seconds, and the base phase took 12·2 seconds. The construction of the *PROJ*(*A*)-invariant cad of the plane took approximately 5 hours and 45 minutes. This cad of the plane has one more "meaningful" cylinder, and two more extraneous cylinders than the *P*(*A*)-invariant cad of the plane.

6.2. RANDOM TRIVARIATE POLYNOMIAL

The following trivariate polynomial of degree 4 in the main variable z, degree 1 in each of the variables x and y, and random integer coefficients from the closed interval $[-1, +1]$ was generated:

$$f(x, y, z) = (y-1)z^4 + xz^3 + x(1-y)z^2 + (y-x-1)z + y.$$

The set $A = \{f\}$ was supplied as input to each of the SAC-2 programs *CAD* and *CADR*3. The polynomial f is found to be primitive and irreducible, and A is hence its own finest squarefree basis.

The projection *PROJ*(*A*) of A, computed by *CAD*, is the set

$$PROJ(A) = \{ldcf(f), discr(f), psd_1(f), psd_2(f), ldcf(g), discr(g)\},$$

where *ldcf* denotes "leading coefficient", and g is the reductum of f. (The first two coefficients of f, viz. $y-1$ and x, have only one common zero in the plane. Hence, according to the remarks made at the beginning of section 6, it is not necessary to consider any other reducta of f besides f and g, and the other coefficients of f can be left out of *coeff*(*A*). It is also the case that *ldcf*(f) and *discr*(g) have only finitely many common zeros in the plane. Hence (Collins, 1975, p. 177), $psd_1(g)$ is also superfluous.)

The characteristics of the polynomials in *PROJ*(*A*) are summarized in Table 1. *CAD* computes the finest squarefree basis B_1 for *prim*(*PROJ*(*A*)), constructs the projection of B_1, and then performs a squarefree basis computation. The set U_1 of univariate basis polynomials obtained is described in Table 2. Note that U_1 contains 17 polynomials, including a polynomial of degree 22 (the highest degree present), the maximum length of whose coefficients is 16 decimal digits. *CAD* isolates the real roots of the polynomials in U_1. A total of 31 real roots is found, yielding a decomposition of the real line into $2 \times 31 + 1 = 63$ cells. The computing times for the various subtasks of *CAD* discussed so far are given in Table 3.

The reduced projection *P*(*A*) of A, computed by *CADR*3, is the set

$$P(A) = \{ldcf(f), discr(f), ldcf(g)\}.$$

*CADR*3 computes the finest squarefree basis B_2 for *prim*(*P*(*A*)), constructs the projection of B_2, and then performs a squarefree basis computation. The set U_2 of univariate basis polynomials obtained is described in Table 2. *CADR*3 determines that the polynomials in

Table 1. Composition of *PROJ*(*A*) (coefficient length in decimal digits)

Poly	Deg in x	Deg in y	Total deg	Max coeff length
ldcf(f)	0	1	1	1
discr(f)	6	6	10	4
$psd_1(f)$	4	4	7	3
$psd_2(f)$	2	2	3	2
ldcf(g)	1	0	1	1
discr(g)	4	4	7	2

Table 2. Composition of U_1 and U_2 (coefficient length in decimal digits)

	U_1		U_2	
Degree	No. polys	Max coeff length	No. polys	Max coeff length
22	1	16	0	
21	1	12	0	
15	1	8	0	
11	1	10	0	
10	1	6	1	6
6	2	7	1	1
4	3	3	2	3
3	3	2	0	
2	1	2	1	2
1	3	1	1	1
	17		6	

Table 3. Computing times in seconds for subtasks

	CAD	*CADR3*
Computation of basis for input	10·9	10·9
Construction of bivariate proj	303	4·8
Computation of bivariate basis	11·4	2·8
Construction of univariate proj	246	114
Computation of univariate basis	131	24·5
Real root isolation	28·2	3·1
Total	730	160

U_2 have a total of 11 real roots. Thus the decomposition of the real line has $2 \times 11 + 1 = 23$ cells. The computing times for the various subtasks of *CADR3* are included in Table 3, for comparison with those of *CAD*.

We have not yet attempted to run either program long enough to complete construction of the cad of the plane. It is to be expected that our current version of the program would take a considerable amount of time and space to do this, due to the high cost of sample point construction.

This paper is based on the author's PhD thesis. I would like to acknowledge the support, guidance and encouragement given to me by my thesis advisor, George Collins. Thanks also to Pierre Milman for helping me to better understand Zariski's theorem. I am grateful to the referees for their helpful comments.

References

Arnon, D. S., Collins, G. E., McCallum, S. (1984*a*). Cylindrical algebraic decomposition I: the basic algorithm. *SIAM J. Comp.* **13/4,** 865–877.

Arnon, D. S., Collins, G. E., McCallum, S. (1984*b*). Cylindrical algebraic decomposition II: an adjacency algorithm for the plane. *SIAM J. Comp.* **13/4,** 878–889.

Bochner, S., Martin, W. T. (1948). *Several Complex Variables.* Princeton: Princeton Univ. Press.

Brown, W. S., Traub, J. F. (1971). On Euclid's algorithm and the theory of subresultants. *J. Assoc. Comp. Mach.*, **18/4,** 505–514.

Collins, G. E. (1975). Quantifier elimination for real closed fields by cylindrical algebraic decomposition. In: Second GI Conference on Automata Theory and Formal Languages. *Springer Lec. Notes Comp. Sci.* **33,** 134–183.

Gunning, R. C., Rossi, H. (1965). *Analytic Functions of Several Complex Variables.* Englewood Cliffs: Prentice-Hall.
Kahn, P. J. (1978). Private communication to G. E. Collins.
Kaltofen, E. (1982). Polynomial factorization. In: *Computing*, Supplementum 4: *Computer Algebra—Symbolic and Algebraic Computation.* Vienna and New York: Springer-Verlag.
Kaplan, W. (1966). *Introduction to Analytic Functions.* Reading: Addison-Wesley.
Lang, S. (1984). *Algebra*, 2nd edn. Menlo Park: Addison-Wesley.
Loos, R. G. K. (1982). Computing in algebraic extensions. In: *Computing*, Supplementum 4: *Computer Algebra—Symbolic and Algebraic Computation.* Vienna and New York: Springer-Verlag.
Marden, M. (1966). *Geometry of Polynomials*, 2nd edn. Providence: American Mathematical Society.
McCallum, S. (1984). *An Improved Projection Operation for Cylindrical Algebraic Decomposition.* PhD thesis, Technical Report No. 578, Computer Sciences Department, University of Wisconsin-Madison.
Munkres, J. (1975). *Topology—A First Course.* Englewood Cliffs: Prentice-Hall.
Tarski, A. (1951). *A Decision Method for Elementary Algebra and Geometry*, 2nd edn. University of California Press.
Walker, R. T. (1978). *Algebraic Curves.* New York: Springer-Verlag.
Whitney, H. (1972). *Complex Analytic Varieties.* Menlo Park: Addison-Wesley.
Zariski, O. (1935). *Algebraic Surfaces.* New York–Heidelberg–Berlin: Springer-Verlag.
Zariski, O. (1965). Studies in equisingularity II. *Amer. J. Math.* **87/4**, 972–1006.
Zariski, O. (1975). On equimultiple subvarieties of algebroid hypersurfaces. *Proc. Nat. Acad. Sci., USA* **72/4**, 1425–1426.

Appendix

LEMMA A.1. *Let $f(x)$ and $g(x)$ be polynomials of degrees $m>0$ and $n>0$ respectively over an integral domain R. Assume that the characteristic of R divides neither m nor n. Then*

$$discr(fg) = discr(f)(res(f,g))^2 discr(g).$$

PROOF.

$$\begin{aligned} res(fg,(fg)') &= res(fg, f'g+fg') \\ &= res(f,f'g+fg')\,res(g,f'g+fg') \\ &= res(f,f'g)\,res(g,fg') \\ &= res(f,f')\,res(f,g)\,res(g,f)\,res(g,g') \end{aligned}$$

by Theorems 3 and 4 from Loos (1982). The result now follows by Theorem 3.0. □

LEMMA A.2. *Let $f(x, y, z)$ be a primitive polynomial in $\mathbb{Z}[x, y, z]$. Then there exist only finitely many common zeros of the (bivariate) coefficients of $f(x, y, z)$.*

PROOF. By induction on the degree of f in z using Bezout's theorem (Walker, 1978, Theorem III–3.1). □

LEMMA A.3. *Let $K = \mathbb{R}$ or $\mathbb{C}$. Let f and g be analytic functions defined in a connected, open subset U of K^n, and assume that neither f nor g vanishes identically. Let S be a connected subset of U. Then fg is order-invariant in S if and only if both f and g are order-invariant in S.*

PROOF. Now

$$\operatorname{ord}_q fg = \operatorname{ord}_q f + \operatorname{ord}_q g, \tag{A.1}$$

for all $q \in U$. Assume that both f and g are order-invariant in S. Then, by (A.1), fg is order-invariant in S. Conversely, assume that fg is order-invariant in S. Let $p \in S$. Then $\operatorname{ord}_p fg < \infty$, as fg does not vanish identically in U (by the identity theorem). Now there

exists a neighbourhood $V \subseteq U$ of p such that $\operatorname{ord}_q f \leqslant \operatorname{ord}_p f$ and $\operatorname{ord}_q g \leqslant \operatorname{ord}_p g$ for every $q \in V$ (by continuity of the partial derivatives of f and g). It now follows from (A.1) that both f and g are order-invariant in $V \cap S$. Hence, by connectedness of S, both f and g are order-invariant in S. □

LEMMA A.4. *Let $E(u, v)$ be real analytic in a neighbourhood of 0 in $\mathbb{R}^2$, let the power series expansion of $E(u, v)$ about 0 be absolutely convergent in the polydisc $\Delta: |u| < r, |v| < s$ about 0 in $\mathbb{C}^2$, and let $E*(u, v)$ denote the sum of this series (for $(u, v) \in \Delta$), a complex analytic function in Δ. Suppose that E is order-invariant in the real u-axis $T = \{(u, 0) | u \in \mathbb{R}\}$ near the origin. Then E^* is order-invariant in the complex u-axis $T* = \{(u, 0) | u \in \mathbb{C}\}$ near the origin.*

PROOF. Let $\operatorname{ord}_0 E = m$. If $m = \infty$, then all partial derivatives of E vanish at 0, and hence $E*$ vanishes identically near 0. So assume $m < \infty$. Let

$$P*(u, v) = \frac{\partial^{i+j} E*}{\partial u^i \, \partial v^j}$$

be a partial derivative of $E*(u, v)$ of order $i+j$. By (the proof of) Theorem 56 of Kaplan (1966) $P*(u, v)$ is analytic in Δ_1, and its power series expansion about 0, which is absolutely convergent in Δ_1, is obtained by differentiating the power series for E about 0 term by term. Let

$$P(u, v) = \frac{\partial^{i+j} E}{\partial u^i \, \partial v^j}$$

for $(u, v) \in \Delta \cap \mathbb{R}^2$. Clearly, $P(u, v) = P*(u, v)$ for all $(u, v) \in \Delta \cap \mathbb{R}^2$. Assume $i+j < m$. Then $P(u, 0) = 0$ for all u in some neighbourhood of 0 in $\mathbb{R}^1$. Hence, when one substitutes $v = 0$ into the power series expansion for $P(u, v)$ about 0, one obtains the zero power series in u. It follows that $P*(u, 0) = 0$ for all u in some neighbourhood of 0 in $\mathbb{C}^1$ (as P and $P*$ have the same power series about 0). We have shown that every partial derivative of $E*$ of order less than m vanishes in $T*$, near 0.

As $\operatorname{ord}_0 E = \operatorname{ord}_0 E* = m < \infty$, some partial derivative of $E*$ of order m does not vanish at 0, and hence does not vanish in a neighbourhood of 0 in $\mathbb{C}^2$. It now follows that, for all points $(u, 0)$ in some neighbourhood of 0 in $\mathbb{C}^2$, $\operatorname{ord}_{(u,0)} E* = m$. Thus $E*$ is order-invariant in $T*$, near 0. □

LEMMA A.5. *Let $q(u, v, z)$ be a nowhere-vanishing function in the polydisc $\Delta': |u| < r_2$, $|v| < s_2$, $|z| < \varepsilon$, let $g(u, v, z)$ be a pseudopolynomial of degree $d \geqslant 1$ in the polydisc $\Delta_2: |u| < r_2$, $|v| < s_2$, and let $h(u, v, z)$ be a Weierstrass polynomial of degree $m \geqslant 1$ in Δ_2. Assume that the relation*

$$g(u, v, z) = q(u, v, z) h(u, v, z) \tag{A.2}$$

holds for all $(u, v, z) \in \Delta'$, and that for each fixed point (u, v) of Δ_2, every root of $h(u, v, z)$ (a polynomial in z alone) is contained in the disc $|z| < \varepsilon$. Then $q(u, v, z)$ is a pseudopolynomial in Δ_2.

PROOF. Let (u, v) be a fixed point of Δ_2. Let ξ be a root of $h(u, v, z)$ (a polynomial in z alone). Then $|\xi| < \varepsilon$, by hypothesis. Hence, as (A.2) holds near the point ξ in the z-plane, and as $q(u, v, z) \neq 0$ near ξ, $g(u, v, \xi) = 0$ and the multiplicity of the root ξ of $h(u, v, z)$ (a polynomial in z alone) is equal to the multiplicity of the root ξ of $g(u, v, z)$ (a polynomial in z alone). It follows that $h(u, v, z) | g(u, v, z)$ in $\mathbb{C}[z]$ and hence that the quotient $q(u, v, z)$

is a polynomial in z. Let l be the degree of $g(u, v, z)$. Then $m \leqslant l \leqslant d$, and the degree of $q(u, v, z)$ is $l-m$. Thus $q(u, v, z)$ can be expressed as follows:

$$q(u, v, z) = q_0(u, v)z^{d-m} + q_1(u, v)z^{d-m-1} + \ldots + q_{d-m}(u, v),$$

where $q_0(u, v) = \ldots = q_{d-l-1}(u, v) = 0$, and $q_{d-l}(u, v) \neq 0$. Letting (u, v) now be a variable point of Δ_2, the coefficients $q_j(u, v)$ of $q(u, v, z)$ can be regarded as functions defined in Δ_2. That these functions are in fact analytic in Δ_2 can be seen by equating coefficients in (A.2) □

LEMMA A.6. *Let $F(x, y)$ be analytic and not identically vanishing in the polydisc $\Delta: |x| < r, |y| < s$ about 0 in $\mathbb{C}^2$. Assume that F is order-invariant in $T* \cap \Delta$, where $T*$ is the complex x-axis. Then there exists a polydisc $\Delta' \subseteq \Delta$ about 0 such that the zero set of F in Δ' is either empty or equal to $T* \cap \Delta'$.*

PROOF. Let $\operatorname{ord}_0 F = m$. Let

$$F(x, y) = F_0(x) + F_1(x)y + F_2(x)y^2 + \ldots$$

be the power series expansion for F about 0 arranged as an iterated series. Let $|x_0| < r$. The power series expansion for F about $(x_0, 0)$ is

$$F_0'(x-x_0) + F_1'(x-x_0)y + F_2'(x-x_0)y^2 + \ldots$$

where $F_i'(x-x_0)$ is the power series expansion of $F_i(x)$ about x_0. Now $\operatorname{ord}_{(x_0,0)} F = m$ as F is order-invariant in $T* \cap \Delta$. Therefore, $F_i'(0) = 0$ for $0 \leqslant i \leqslant m-1$. Hence, $F_i(x_0) = 0$ for $0 \leqslant i \leqslant m-1$. We have shown that the functions F_i are identically zero in the disc $|x| < r$, for $0 \leqslant i \leqslant m-1$. Hence,

$$F(x, y) = F_m(x)y^m + F_{m+1}(x)y^{m+1} + \ldots,$$

where $F_m(0) \neq 0$ (as $\operatorname{ord}_0 F = m < \infty$). Thus, if we set

$$N(x, y) = F_m(x) + F_{m+1}(x)y + F_{m+2}(x)y^2 + \ldots,$$

then $F(x, y) = y^m N(x, y)$ for all $(x, y) \in \Delta$. As $N(0, 0) = F_m(0) \neq 0$, there exists a polydisc $\Delta' \subseteq \Delta$ about 0 such that $N(x, y) \neq 0$ for all $(x, y) \in \Delta'$. The zero set of F in Δ' is either empty (when $m = 0$) or equal to $T* \cap \Delta'$ (when $m > 0$). □

LEMMA A.7. *Let x denote the $(r-1)$-tuple $(x_1, \ldots, x_{r-1})$, let f and g be polynomials in $\mathbb{R}[x, x_r]$, and let S be a connected subset of $\mathbb{R}^{r-1}$. Suppose that the product $h = fg$ is delineable on S. Then both f and g are delineable on S.*

PROOF. Let s be a section of h on S. Then s is the graph of some continuous function ϕ from s to $\mathbb{R}$. Suppose that $f(a, \alpha) = 0$, for some $(a, \alpha) \in s$. We will show that $\phi(b)$ is a root of $f(b, x_r)$ of the same multiplicity as that of the root α of $f(a, x_r)$, for all $b \in S$. Let m (respectively m_1, m_2) be the multiplicity of the root α of $h(a, x_r)$ ($f(a, x_r)$, $g(a, x_r)$ respectively). (Note: if α is not a root of $g(a, x_r)$, then α is said to have multiplicity 0.) Then $m = m_1 + m_2$. We claim that there exists a neighbourhood N of a such that if $b \in S \cap N$, then the multiplicity of the root $\phi(b)$ of $f(b, x_r)$ (respectively $g(b, x_r)$) is less than or equal to m_1 (respectively m_2).

It follows by the delineability of h on S that for all $b \in S \cap N$ the multiplicity of the root $\phi(b)$ of $f(b, x_r)$ (respectively $g(b, x_r)$) equals m_1 (respectively m_2). Hence, by connectedness of S, the multiplicity of the root $\phi(b)$ of $f(b, x_r)$ equals m_1 for all $b \in S$. □