AN IMPROVED PROJECTION OPERATION FOR CYLINDRICAL ALGEBRAIC DECOMPOSITION

by

Scott McCallum

Computer Sciences Technical Report #578

February 1985

578

AN IMPROVED PROJECTION OPERATION FOR CYLINDRICAL ALGEBRAIC DECOMPOSITION

by

Scott McCallum

A thesis submitted in partial fulfillment of the

requirements for the degree of

DOCTOR OF PHILOSOPHY

(Computer Sciences)

at the

UNIVERSITY OF WISCONSIN-MADISON

1984

AN IMPROVED PROJECTION OPERATION FOR CYLINDRICAL ALGEBRAIC DECOMPOSITION

Scott McCallum

Under the supervision of Professor George E. Collins

A fundamental algorithm pertaining to the solution of polynomial equations in several variables is the *cylindrical algebraic decomposition (cad)* algorithm due to G.E. Collins. Given as input a set A of integral polynomials in r variables, the cad algorithm produces a decomposition of the euclidean space of r dimensions into cells, such that each polynomial in A is invariant in sign throughout each of the cells of the decomposition.

A key component of the cad algorithm is the projection operation: the *projection* of a set A of r-variate polynomials is defined to be a certain set P of $(r-1)$-variate polynomials. The solution set, or variety, of the polynomials in P comprises a projection in the geometric sense of the variety 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 thesis is concerned with a refinement to the cad algorithm, and to its projection operation in particular. It is shown, using a theorem from real algebraic geometry, that the original projection set that Collins used can be substantially reduced in size, without affecting its essential properties. The results of theoretical analysis and empirical observations suggest that the reduction in the projection set size leads to an overall decrease in the computing time of the cad algorithm.

Acknowledgements

I would first like to thank my mother, Mrs. Margaret McCallum, for her unfailing support and encouragement from a great distance away. To my masters thesis supervisor, Dr. Tzee-Char Kuo, I owe a very great debt: for many inspiring lectures and conversations, for posing the problem that eventually led to this thesis, and for continued support. It has been a pleasure to share offices and ideas with Jian-Tu Hsieh and Mani Subramanian. Thanks also to the Computer Sciences Department for providing an excellent computing (and otherwise) environment. I am most grateful to three special friends - Liz and Ernst Hintz, and Tony Hirst - for their good company and camaraderie during our dissertating years. It has been a great pleasure to interact with Dennis Arnon on subjects both related and unrelated to this thesis: many thanks are due Dennis for his advice and encouragement, for the ideas from his thesis, and for the boundless energy he has put into our joint projects. I am indebted to Professor Joseph Lipman for bringing Zariski's work to my attention. Professors Hiroshi Gunji and Debby Joseph have been generous of their time in reading and discussing this thesis. To my advisor, Professor George E. Collins, I owe a very large debt: for providing several years of support and encouragement, for believing strongly in the value of this work, and for his unwavering commitment to excellence in every aspect of research.

Table of Contents

Chapter One

Introduction

The nature of the solutions to polynomial equations in more than one variable has been a subject of study for centuries. Conic sections were studied in antiquity, and Newton [NEW] classified all cubic curves. Hilbert [HIL35] posed a problem concerning the arrangement of the components of non-connected plane curves defined by algebraic equations. Since the advent of the digital computer, there has been growing interest in computing with multivariate polynomials and in the solution of multivariate polynomial equations.

A fundamental procedure that pertains to the solution of multivariate polynomial equations is the *cylindrical algebraic decomposition* (cad) algorithm due to G.E. Collins [COL75]. 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 [TAR51] pioneering method, and indeed any other subsequent method. The cad algorithm accepts as input a set of integral polynomials in some $r \geq 1$ 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 occuring in the input are thus obtained by retaining those cells in which the sign of each input polynomial is zero.

Implementation of the component parts of the cad algorithm (for example, real root isolation for polynomials of a single variable, and polynomial greatest common divisor computation) had begun before the algorithm's formulation. F. Mueller [MUE77] used portions of the cad algorithm to solve a nonlinear optimization problem. Dennis Arnon carried out the first complete implementation of the cad algorithm in 1979-80. As reported in [ARN81] Mueller and Arnon had both observed that certain steps of the algorithm appear to be very time-consuming, and seem to constitute a definite obstacle to the use of the method. The time-consuming steps involve computations with real algebraic numbers, and in particular the constructive version of the primitive element theorem.

In 1981 Arnon [ARN81] presented a modified form of the cad algorithm (applicable in low dimensions) which was designed to circumvent many of the expensive algebraic number calculations. The new method, known as the *clustering cad algorithm* uses cell adjacency information to combine cells into groups called *clusters*. Certain algebraic number computations, carried out for each individual cell in the original method, need only be carried out for each cluster in the new method. As the number of clusters is usually much less than the number of cells, far fewer algebraic number calculations are required in the clustering algorithm. The cell adjacency algorithm used by the clustering cad algorithm was developed by Arnon, Collins and McCallum [ACM84a,b] and was based upon a method for curve

triangulation in [MCC79].

A key component of the cad algorithm is the projection operation: the *projection* of a set A of r-variate polynomials is defined to be a certain set P of $(r-1)$-variate polynomials. The solution set, or variety, of the polynomials in P comprises a projection in the geometric sense of the variety of A. The cad algorithm proceeds by forming successive projections of the input set A, each projection resulting in the elimination of one variable.

The exact definition of the projection of a set A of r-variate integral polynomials is rather involved (see Sec. 3.1). However one can roughly describe the projection of A as consisting of the $(r-1)$-variate coefficients of the elements of A together with certain discriminants, subdiscriminants, resultants, and subresultants formed from the elements of A.

The work reported in this thesis stemmed from the surface triangulation procedure contained in [MCC79]. The relevant observation is that a triangulation of a surface defined by a polynomial equation $F(x,y,z) = 0$ can be "based upon" a triangulation of the plane curve defined by the vanishing of the discriminant of $F(x,y,z)$. This observation has an implication for the size of the projection of a set of trivariate polynomials: provided that the elements of A are primitive, squarefree, and pairwise relatively prime, it suffices to include just the coefficients, discriminants and resultants (of pairs) of the elements of A in the projection. It is unnecessary to include the other polynomials specified by the original projection operator. McCallum conjectured that a similar simplification to the projection would be possible in higher dimensions as well.

Through Joseph Lipman of Purdue University, McCallum learnt of work by O. Zariski in abstract algebraic geometry that appeared to have close connections with the projection problem. A recent paper by Zariski [ZAR75] contained a theorem on local properties of complex hypersurfaces that appeared to be relevant. McCallum was able to derive from this theorem a result pertaining to real polynomials, discriminants, and projection. The new result states that if $f(x_1,...,x_r)$ is a real polynomial with discriminant $D(x_1,...,x_{r-1})$, then under certain conditions a smooth cell in $\mathbb{R}^{r-1}$ in which the order of D is invariant can be "lifted" (or extended) in a certain sense to a sequence of disjoint smooth cells in $\mathbb{R}^r$ in each of which the order of f is invariant. This result, termed *the lifting theorem*, leads to a simplified projection for polynomials in several variables.

This thesis reports the proof and applications to cad construction of the lifting theorem. Chapter 2 provides background mathematical material on which the proof of the theorem is based. Analytic functions of several (real or complex) variables, and submanifolds of Euclidean space, are the main subjects dealt with. Chapter 3 gives a review of the cad algorithm, introduces the lifting theorem, and shows how the theorem leads to an improved (because reduced) projection operation for cad construction. In Chapter 4 is presented an exposition of the Zariski theorem on which the lifting theorem is based. The presentation is self-contained and original in many respects. It provides the interested reader with an alternative to studying Zariski's original paper, the grasping of which would require a command of advanced techniques in commutative algebra and algebraic geometry.

Chapter 5 presents algorithms for cad construction which make use of the reduced projection operation. For so-called well-oriented poynomials the application of the reduced projection to cad construction is straightforward. For more general polynomials, extra work is required to obtain order-invariant decompositions over the so-called nullifying cells of positive dimension. Clustering cad algorithms, producing smooth, order-invariant clusters of cells, are also presented. Chapter 6 contains both theoretical and empirical analysis of the cad algorithms from Chapter 5.

Chapter Two

Mathematical Preliminaries

This chapter presents mathematical background material which the reader should find helpful in reading Chapters 3 and 4.

Our discussion of projection of algebraic varieties presented in Chapter 3 involves a rather careful study of the properties of algebraic sets in the neighborhood of a particular point (such properties are called *local* properties). A basic tool in local analysis of algebraic sets is the (multiple) power series. Functions having power series expansions, or *analytic* functions, thus enter the discussion in a natural way.

There are a number of texts which include a discussion of the elementary properties of analytic functions of several complex variables (for example, [GRO65], [BMA48], and [KAP66]). Analytic functions of real variables are best studied with the aid of complex variables: Chapter 2 of [BMA48] contains a comparison between the real and complex cases. Section 1 of this chapter is a collection of many basic results about analytic functions (of both real and complex variables). For proofs one is generally referred to texts.

The original cylindrical algebraic decomposition (cad) algorithm

[COL75] decomposes $\mathbb{R}^n$ into semi-algebraic subsets which Collins called *cells*. It has been subsequently observed [KAH78] 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 the open unit ball in $\mathbb{R}^i$, for some i, $0 \leq i \leq n$. What is further true is that each cell is homeomorphic to an open unit ball via a mapping which is *analytic*: thus each cell is an analytic i-dimensional submanifold of $\mathbb{R}^n$, for some i. This smoothness property of the cells turns out to be quite important in developing an improved projection operation for the cad algorithm.

Section 2 develops the concept of submanifold as far as needed for our purposes. Although the material is standard, it does not appear in quite the form we require in any of the texts. Our presentation is tailored to the needs of our later chapters.

Section 3 is a collection of miscellaneous results which will prove useful in subsequent chapters.

2.1 Analytic Functions of Several Variables.

We assume that the reader is familiar with the elementary theory of analytic functions of a single complex variable. We discuss the notion of a multiple power series and that of an analytic function of several (real or complex) variables. We present statements of many basic theorems about such functions, often referring the reader to standard texts for the proofs.

We present a short summary of the material presented in this section. A function $f(x_1,\ldots,x_n)$ (the x_i real or complex variables) is said to be *analytic* if it has a (multiple) power series representation about each point of its

domain. An analytic function of complex variables is also termed *holomorphic*. 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 (assuming nonzero denominator) of analytic functions are analytic.

Let $\mathbb{R}$ denote the field of real numbers, and let $\mathbb{C}$ denote the field of complex numbers, i.e. numbers of the form $z = x + iy$, where x and y are elements of $\mathbb{R}$ and i is a square root of -1. *Throughout this section K will denote either $\mathbb{R}$ or $\mathbb{C}$.* K^n will denote the Cartesian product $K \times \cdots \times K$ of n copies of K. In this section, unless otherwise specified, we will use the notation $x = (x_1,...,x_n)$ for points of K^n.

Definition. Let $c = (c_1,...,c_n)$ be a point of K^n. A *power series about c over K* is an expression of the form

$$\sum_{i_1,\ldots,i_n = 0}^{\infty} a_{i_1,\ldots,i_n} (x_1-c_1)^{i_1} \cdots (x_n-c_n)^{i_n} \tag{2.1.1}$$

where the coefficients $a_{i_1,\ldots,i_n}$ are elements of K.

Remark. If $n > 1$ then the power series (2.2.1) is a multiple power series because of the multiple index $i_1,\ldots,i_n$. We can, however, arrange the terms to form a simple series, for example, with $n = 2$,

$$a_{00} + a_{10}(x_1-c_1) + a_{01}(x_2-c_2) + a_{20}(x_1-c_1)^2 + a_{11}(x_1-c_1)(x_2-c_2) + a_{02}(x_2-c_2)^2 + a_{30}(x_1-c_1)^2 + \cdots.$$

We are thus, in this example, sweeping out all the combinations (i_1, i_2) by

following diagonals of the corresponding array (see fig. 2.1.1).

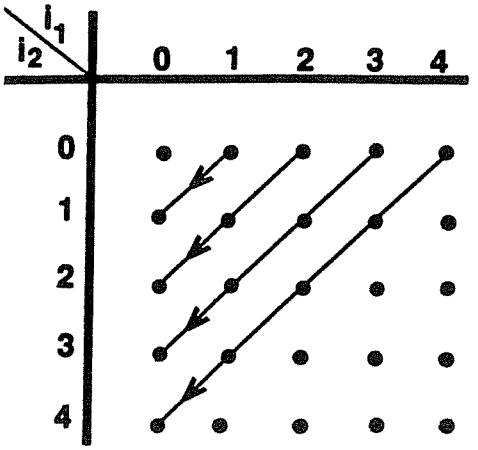

Fig. 2.1.1.

Another arrangement of the terms is obtained by going around the sides of squares of increasing size, that is, choosing the successive pairs (i_1,i_2) as follows:

$$(0,0), (1,0), (1,1), (0,1), (2,0), (2,1), (2,2), (1,2), (0,2), (3,0), \cdots .$$

If $x = (x_1, \ldots, x_n)$ is a point of K^n then one can ask whether the series (2.1.1) has some arrangement as a *convergent* simple series. If there exists an arrangement of the series as a simple series for which one has absolute convergnce, then by theorem 28 on $p.333$ of [KAP52], the series is absolutely convergent for *every* arrangement as a simple series, and the sum is the same for all arrangements. We shall say, simply, that the series (2.1.1) is absolutely convergent if it is absolutely convergent for some arrangement as

a simple series.

If $c \in K^n$ then a *neighborhood* of c is an open subset W of K^n containing c. Let $c \in K^n$ & let $r = (r_1, \ldots, r_n) \in \mathbb{R}^n$, with $r_i > 0$ for $i \leq 1 \leq n$. Consider the neighborhood

$$\{ x \in K^n : |x_i - c_i| < r_i, 1 \leq i \leq n \}$$

of c. In the case $K = \mathbb{R}$; we call this neighborhood a *box* about c and denote it by $B(c;r)$. In case $K = \mathbb{C}$, we call this neighborhood the *polydisc* about c of *polyradius* r and denote it by $\Delta(c;r)$. Note that if $c \in \mathbb{R}^n$, then $B(c;r) = \Delta(c;r) \bigcap \mathbb{R}^n$. Let $1 \leq s \leq n$ and let $\pi : K^n \to K^s$ be the projection $\pi(x_1, \ldots, x_n) = (x_1, \ldots, x_s)$. Let $K = \mathbb{R}$ and let B be the box $B(c;r)$ in $\mathbb{R}^n$. Then we shall denote by $B^{(s)}$ the image of B under π, i.e.

$$B^{(s)} = \{ (x_1, \ldots, x_s) \in \mathbb{R}^s : |x_i - x_c| < r_i, 1 \leq i \leq s \} .$$

Let $K = \mathbb{C}$ and let Δ be the polydisc $\Delta(c;r)$ in $\mathbb{C}^n$. We similarly denote by $\Delta^{(s)}$ the image of Δ under π.

Definition. Let U be an open subset of K^n and let $f : U \to K$ be a function. Then f is said to be *analytic* in U if each point c of U has a neighborhood $W \subseteq U$ such that f has a power series about c over K

$$f(x_1, \ldots, x_n) = \sum_{i_1, \ldots, i_n = 0}^{\infty} a_{i_1, \ldots, i_n} (x_1 - c_1)^{i_1} \cdots (x_n - c_n)^{i_n} \qquad (2.1.3)$$

which is absolutely convergent for every point x of W.

Example: Every polynomial in $x_1, \ldots, x_n$ over K is analytic in the whole of K^n.

Remark. If $K = \mathbb{C}$ and $U \subseteq K^n$ is open, then a function $f : U \to K$

analytic in U is also termed *holomorphic* in U.

Remark. In the case $K = \mathbb{R}$, the above is the definition of analytic function that appears in most texts. In the case $K = \mathbb{C}$, one sometimes finds an alternative, equivalent definition of holomorphic function: a complex-valued function $f(z_1, \ldots, z_n)$ defined in the open subset U of $\mathbb{C}^n$ is said to be holomorphic in U if it is continuous in U and has continuous partial derivatives $\frac{\partial f}{\partial z_i}$ in U. That this definition is equivalent to our definition for the case $K = \mathbb{C}$ follows from Theorems 2.1.1 and 2.1.8 below.

Theorem 2.1.1. Let $U \subseteq K^n$ be open and let $f : U \to K$ be an analytic function. Then f is continuous and has continuous partial derivatives of all orders, given by:

$$\frac{\partial^{i_1 + \cdots + i_n} f}{\partial x_1^{i_1} \cdots \partial x_n^{i_n}}(c) = (i_1!) \cdots (i_n!) a_{i_1, \ldots, i_n}$$

where the $a_{i_1, \ldots, i_n}$ are the coefficients of the power series expansion (2.1.3) of f about the point c of U.

References for *proof*. For the real case, (i.e. $K = \mathbb{R}$), we refer the reader to Sec. 6-20 of [KAP52]; and for the complex case, ($K = \mathbb{C}$), to Theorem 1 of Chapter II of [BMA48] □

Remark 1 : It follows from Theorem 2.1.1 that the power series expansion of an analytic function about a point is unique.

Remark 2 : The converse of Theorem 2.1.1 holds in the case $K = \mathbb{C}$ (this is

Theorem 2.1.8) but not in the case $K = \mathbb{R}$, as is shown by the example $f(x) = e^{-1/x^2}$ (discussed in Sec. 6-17 of [KAP52]).

A function defined as the sum of a convergent power series is, as might be expected, analytic:

Theorem 2.1.2 : Let $c = (c_1,...,c_n)$ be a point of K^n and let the power series over K

$$\sum_{i_1,...,i_n=0}^{\infty} a_{i_1,...,i_n} (x_1-c_1)^{i_1} \cdots (x_n-c_n)^{i_n} \tag{2.1.4}$$

converge (for some arrangement as a simple series) for $x_1 = c_1+r_1, \ldots, x_n = c_n+r_n$, where each $r_i > 0$. Let

$$D = \{ x = (x_1,...,x_n) \in K^n : |x_i-c_i| < r_i, 1 \le i \le n \}$$

Then the series (2.1.4) is absolutely convergent for every $x \in D$, and the sum of the series, say $f(x)$, is an analytic function in D. Moreover, every partial derivative (of any order) of f is analytic in D, and its power series expansion about c, absolutely convergent for every $x \in D$, is obtained by differentiating (2.1.4) term-by-term.

Proof : We first present a proof for the case $K = \mathbb{C}$. For the complex case let us imagine that z_i replaces each occurrence of x_i in the statement of the theorem. Note that in this case, the neighborhood D of c is the polydisc $\Delta(c;r)$ about c. The first part of the conclusions, as to the absolute convergence of the series (2.1.4), follows from the n-variable analogue of Theorem 54 in [KAP66]. By analogy with Theorem 55 of [KAP66], let E be the set of points $z \in \mathbb{C}^n$ for which the series (2.1.4) converges and let E^i be the

interior of E. As the series (2.1.4) converges for every $z \in D$, we have $D \subseteq E$. Consequently, $D \subseteq E^i$. Hence the hypothesis of the n-variable analogue of Theorem 55 of [KAP66] is satisfied. The holomorphicity of the function f now follows by the n-variable analogue of Theorem 56 of [KAP66]. The proof of this n-variable analogue of Theorem 56 yields the required results about the partial derivatives of f. The theorem is now proved for the case $K = \mathbb{C}$.

Let us now deal with the real case. In this case the neighborhood D of c is the box $B(c;r)$ about c. The first part of the conclusions as to the convergence of (2.1.4) follows from the n-variable analogue of Theorem 54 in [KAP66]. By the complex case, the series (2.1.4) (with the x_k's replaced by z_k's) is absolutely convergent in $\Delta_1 := \Delta(c;r)$ and its sum, say $F(z)$, is holomorphic in Δ_1. Moreover, every partial derivative of F is holomorphic in Δ_1, and its power series expansion about c is obtained by differentiating (2.1.4) term-by-term. It is not hard to see that, for every point d of D, the power series expansion of $F(z)$ about d has real coefficients. Hence, when x_k's are substituted for z_k's in this power series about d, a power series representation for $f(x)$ is obtained. It follows that f is analytic in D.

The proof of the assertion concerning the partial derivatives of f is straightforward. □

It is well-known that sums, products and quotients of analytic functions are analytic. We state this as

Theorem 2.1.3 : Let U be an open subset of K^n and let f and g be analytic in U. Then the functions $f + g$ and fg (defined pointwise) are analytic in

U. If $f \neq 0$ in U then the function $1/f$ is analytic in U.

Example : Any rational function $f(x_1,\ldots,x_n)/g(x_1,\ldots,x_n)$ (where f and g are polynomials over K) is analytic in the region of K^n where $g \neq 0$.

Theorem 2.1.4 (*IdentityTheorem*) : Let $D \subseteq K^n$ be a connected open set and let f be analytic in D. If $f(x) = 0$ for all points x in a nonempty open subset U of D, then $f \equiv 0$ everywhere in D.

Ref erences for*proof* : The complex identity theorem is Theorem 6 of Ch. I, [GRO65]. The real identity theorem is the theorem on page 53 of [JOH75]. □

Let U be an open subset of K^n and let $G : U \to K^m$ be a mapping. Then there are m functions $g_1, \ldots, g_m$ from U to K such that

$$G(x) = (g_1(x), \ldots, g_m(x))$$

for all $x \in U$. We call G an *analytic mapping* if the m functions $g_1,\ldots,g_m$ are analytic in U.

Theorem 2.1.5 (*Composition Theorem*) : Let U and $U\cdot$ be open subsets of K^n and K^m respectively, let $G : U \to U\cdot$ be an analytic mapping, and let $f : U\cdot \to K$ be an analytic function. Then the composite $f \circ G$ is an analytic function in U.

Ref erences for*proof* : For the real case, see the last paragraph of Sec. 2, Ch. 2 of [BMA48]. For the complex case, see Theorem 5 of Sec.A, Ch. I of [GRO65]. □

If F is an analytic mapping from $U \subseteq K^n$ into K^m, $F(x) = (f_1(x),...,f_m(x))$, and if p is a point of U, then we denote the Jacobian matrix $(\frac{\partial f_i}{\partial x_j}(p))$ of F at p by $J_F(p)$. We can now state a couple of fundamental theorems on the local properties of analytic mappings. These theorems, the inverse mapping and the implicit mapping theorems, generalize the familiar inverse function and implicit function theorems from the elementary calculus.

Theorem 2.1.6 (*Inverse Mapping Theorem*): Let F be an analytic mapping from the open subset U of K^n into K^n, and let p be a point of U. Suppose that $J_F(p)$ is invertible. Then there is a neighborhood $V \subseteq U$ of p in which F is invertible. That is, the set $V\cdot := F(V)$ is open in K^n, and there is an analytic map $G : V\cdot \to V$ such that, for all x in V and y in W,

$$y = F(x) \text{ if and only if } x = G(y).$$

References: The real case of the theorem is stated without proof in the appendix on Calculus in [HIR76]. (Note that the linear map $Df_p : \mathbb{R}^n \to \mathbb{R}^n$, which is mentioned in the statement of the theorem in [HIR76], has matrix $J_F(p)$ with respect to the standard basis of unit coordinate vectors of $\mathbb{R}^n$. Hence, the mapping Df_p is invertible if and only if the matrix $J_F(p)$ is invertible.)

The complex version of the theorem appears in [GRO65]: it is Theorem 7 of Sec.B, Ch. I of this book. □

Theorem 2.1.7 (*Implicit Mapping Theorem*): Let $0 \le s \le n$, let U be an open subset of K^n, and let $F : U \to K^{n-s}$ be an analytic map with

component functions $f_{s+1}, \ldots, f_n$. Let $p = (p_1, \ldots, p_n)$ be a point of U and suppose $F(p) = 0$. Suppose that the $(n-s)\times(n-s)$ square submatrix of $J_F(p)$ consisting of the last $n-s$ rows and columns of $J_F(p)$ is invertible. Then there are neighborhoods $V \subseteq K^s$ of $(p_1, \ldots, p_s)$ and $W \subseteq K^{n-s}$ of $(p_{s+1}, \ldots, p_n)$, with $V \times W \subseteq U$, and analytic functions $\psi_{s+1}, \ldots, \psi_n$ from V into K, such that for all $(x_1, \ldots, x_s)$ in V and all $(x_{s+1}, \ldots, x_n)$ in W,

$$F(x_1, \ldots, x_n) = 0 \text{ iff } x_{s+1} = \psi_{s+1}(x_1, \ldots, x_s), \ldots, x_n = \psi_n(x_1, \ldots, x_s).$$

This result can be proved using the inverse mapping theorem (cf. [BUC56]). Up to now, the theories of real and complex analytic functions have been developed in parallel. We now mention a couple of differences between the two theories. The following theorem holds for complex but not real analytic functions:

Theorem 2.1.8 : Let U be an open subset of $\mathbb{C}^n$ and let f be a complex-valued function defined in U. Suppose that f is continuous in U and that each partial derivative $\frac{\partial f}{\partial z_i}$ exists and is continuous in U. Then f is analytic in U.

References for *Proof* : The result follows from the n-variable analogue of Theorem 53 in Sec. 9-3 of [KAP66] (note that the definition of holomorphicity in [KAP66] is equivalent to the conditions in the hypothesis of Theorem 2.1.8).

We include one more theorem that is valid for holomorphic functions

but which does not have a real analogue.

Theorem 2.1.9 : Let U be an open subset of $\mathbb{C}^n$ and let f be holomorphic in U. Let c be a point of U, let $r = (r_1,...,r_n)$, where each $r_i > 0$, and suppose that $\Delta(c;r) \subseteq U$. Then the power series expansion of f about c is absolutely convergent in $\Delta(c;r)$.

Reference for *proof* : See Theorem 3 in Ch. II of [BMA48].

Remark. In a real analogue of the above theorem one would presumably have boxes $B(c;r)$ in place of polydiscs $\Delta(c;r)$. That there is no real analogue of the theorem, however, is shown by the following example: the function $f(x) = \frac{1}{1+x^2}$ is analytic on the whole real line, but the interval of convergence of the power series expansion for f about 0

$$1 - x^2 - x^4 - x^6 + \cdots$$

is $|x| < 1$.

By a *zero* of a holomorphic function $f(z_1,...,z_n)$ is meant a point $p = (p_1,...,p_n)$ such that $f(p) = 0$. It is noted in Sec. 9-7 of [KAP66] that if $n \geq 2$, then a holomorphic function $f(z_1,...,z_n)$ can have no isolated zeros. Further information on the set of zeros is given by the Weierstrass preparation theorem. We need a definition before we can state the theorem. Let z denote the $(n-1)$-tuple $(z_1,...,z_{n-1})$.

Definition: Let

$$h(z,z_n) = a_0(z)z_n^m + a_1(z)z_n^{m-1} + ... + a_m(z) \qquad (2.1.6)$$

where each $a_i(z)$ is holomorphic in the polydisc $\Delta_1 \subseteq \mathbb{C}^{n-1}$ about 0. Then $h(z,z_n)$ is called a *pseudopolynomial* (in Δ_1). If a_0 is not identically zero, then the *degree* of $h(z,z_n)$ is m. If $a_0 \equiv 1$ and $a_i(0) = 0$ for each i, $1 \leq i \leq m$, then $h(z,z_n)$ is called a *Weierstrass polynomial* (in Δ_1).

Theorem 2.1.10 (*Weierstrass preparation theorem*): Let $f(z,z_n)$ be holomorphic in the polydisc $\Delta_1 \times \Delta(0;\epsilon) \subseteq \mathbb{C}^{n-1} \times \mathbb{C}$, let $z_n = 0$ be a root of $f(0,z_n)$ of multiplicity $m \geq 1$, and assume that $f(0,z_n) \neq 0$ for $0 < |z_n| \leq \epsilon$. Then there is a polydisc $\Delta_2 \subseteq \Delta_1$ about 0 in $\mathbb{C}^{n-1}$, a function $u(z,z_n)$ holomorphic and non-vanishing in $\Delta\cdot := \Delta_2 \times \Delta(0;\epsilon)$, and a Weierstrass polynomial $h(z,z_n)$ in Δ_2, of the form (2.1.6) (with $a_0 \equiv 1$), such that

$$f(z,z_n) = u(z,z_n)\,h(z,z_n) \tag{2.1.7}$$

for all $(z,z_n) \in \Delta\cdot$, and such that for each fixed $z \in \Delta_2$, all the m roots of $h(z,z_n)$ are contained in the disc $\Delta(0;\epsilon)$.

Ref erences for *proof* : We refer the reader to the proof of the Weierstrass preparation theorem (Theorem 62) in Ch. 9 of [KAP66]. (Although there are minor respects in which our statement of the Weierstrass preparation theorem differs from that of Kaplan, the careful reader will note that our theorem follows from the proof of Theorem 62 of [KAP66].)

2.2 Submanifolds of Euclidean space

In this section we develop the concept of a submanifold of real n-space $\mathbb{R}^n$.

We first give a summary of the material presented in this section. An *s-submanifold* of $\mathbb{R}^n$ is a set S which "looks locally like Euclidean s-space $\mathbb{R}^s$"; that is, for every point p of S, there is an (analytic) coordinate system about p with respect to which S is locally the intersection of some $n-s$ coordinate hyperplanes. For example, the $(n-1)$-sphere $S^{n-1} = \{x = (x_1,\ldots,x_n) \in \mathbb{R}^n : \Sigma x_i^2 = 1\}$ is an $(n-1)$-submanifold of $\mathbb{R}^n$. The first part of this section gives a rigorous definition of submanifold, and shows that it corresponds to the above intuitive notion.

Nonempty open subsets of $\mathbb{R}^n$ are submanifolds - in fact, the nonempty open subsets are the n-dimensional submanifolds. But lower-dimensional submanifolds are not open. One can, however, define in a natural way the notion of an analytic function from an s-submanifold S into $\mathbb{R}$, where $0 \leq s \leq n$. A function $f : S \to \mathbb{R}$ is said to be analytic if for every point p of S, there is a coordinate system about p with respect to which S looks locally like $\mathbb{R}^s$, and with respect to which f looks locally like an analytic function from $\mathbb{R}^s$ to $\mathbb{R}$. The second part of this section gives a rigorous definition of an analytic function on a submanifold, and proves that the definition is independent of any particular coordinate system for the submanifold.

The third and last part of this section gives a couple of results on the creation of new submanifolds from old. In particular, it is shown that the graph of an analytic function defined on a submanifold of $\mathbb{R}^n$ is a submanifold of $\mathbb{R}^{n+1}$.

We now begin to look at the material described above in detail. Before giving a formal definition of submanifold we define the notion of a regular

point of an analytic mapping.

Definition. Let $U \subseteq \mathbb{R}^n$ be open and let $F: U \to \mathbb{R}^n$, $m \leq n$, be an analytic map. For $x = (x_1,...,x_n) \in U$ let $F(x) = (F_1(x),...,F_m(x))$. The point p of U is said to be a *regular* point of F if the rank of the Jacobian matrix $J_F(p) = (\frac{\partial F_i}{\partial x_j}(p))$ of F at p is equal to m. □

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.

Definition. The nonempty subset S of $\mathbb{R}^n$ is an *analytic s-dimensional submanifold* of $\mathbb{R}^n$ (or C^ω *s-submanifold, or* C^ω smooth, for short), where $0 \leq s \leq n$, if for each point p of S there is a neighborhood $W \subseteq \mathbb{R}^n$ of p and an analytic map $F: W \to \mathbb{R}^{n-s}$ which has p as a regular point, such that

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

We remark that there is a notion of an s-submanifold of $\mathbb{R}^n$ *of class* C^r, defined as above in terms of maps F which are required to be of class C^r (i.e. to possess continuous partial derivatives through the order r). Here, r is allowed to be any non-negative integer, ∞, or ω (meaning analytic). The only kind of submanifold we shall consider is the analytic kind. Thus we shall henceforth omit the term 'analytic' when referring to submanifolds: all submanifolds will be understood to be analytic.

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 2-submanifold of $\mathbb{R}^3$. □

Definition. Let U and V be open subsets of $\mathbb{R}^n$. A homomorphism $\Phi: U \to V$ such that both Φ and Φ^{-1} are analytic maps is called an *analytic isomorphism.*

Definition. Let U and V be open subsets of $\mathbb{R}^n$ and let $\Phi: U \to V$ be an analytic isomorphism. Then Φ is called a *coordinate system* in U. Suppose that $p \in U$, $0 \in V$, and $\Phi(p) = 0$. Then Φ is called a coordinate system (in U) *about* p. □

The next theorem expresses the intuitive idea that an s-submanifold of $\mathbb{R}^n$, $0 \leq s \leq n$, is a set which "looks locally like Euclidean s-space".

Theorem 2.2.1. The nonempty subset S of $\mathbb{R}^n$ is an s-submanifold of $\mathbb{R}^n$, $0 \leq s \leq n$, if and only if for every point p of S there is a neighborhood $U \subseteq \mathbb{R}^n$ of p and a coordinate system $\Phi: U \to V$, $\Phi = (\phi_1, \ldots, \phi_n)$, about p such that

$$S \cap U = \{x \in U : \phi_{s+1}(x) = 0, \ldots, \phi_n(x) = 0\}. \tag{2.2.1}$$

Remarks. Let $0 \leq s \leq n$ and let T be the s-dimensional linear subspace

$$T = \{y = (y_1, \ldots, y_n) \in \mathbb{R}^n : y_{s+1} = 0, \ldots, y_n = 0\} \tag{2.2.2}$$

of $\mathbb{R}^n$. Then $\mathbb{R}^s$ may be identified with T under the natural identification mapping $\iota(y_1, \ldots, y_s) = (y_1, \ldots, y_s, 0, \ldots, 0)$ (we write $\mathbb{R}^s \equiv T$). By Theorem 2.2.1, the nonempty subset S of $\mathbb{R}^n$ is an s-submanifold of $\mathbb{R}^n$ if and only if S "looks locally like the subspace $T \equiv \mathbb{R}^s$ of $\mathbb{R}^n$" (i.e. for each point p of

S there is a neighborhood $U \subseteq \mathbb{R}^n$ of p and a coordinate system $\Phi: U \to V$ about p such that $\Phi(S \cap U) = T \cap V$.)

Proof of 2.2.1. Suppose that S is an s-submanifold of $\mathbb{R}^n$. Let p be a point of S. Then there is a nbd $W \subseteq \mathbb{R}^n$ of p and an analytic map $F: W \to \mathbb{R}^{n-s}$ having p as a regular point such that $S \cap W = \{x \in W: F(x) = 0\}$. If $s = n$ then set $U = W$ and $\Phi(x) = x - p$: note that (2.2.1) holds. Assume that $s < n$. Write $F(x) = (f_{s+1}(x), \ldots, f_n(x))$. As the Jacobian matrix $J_F(p)$ of F at p has rank $n-s$, we may assume after a renumbering of the coordinates that the $(n-s) \times (n-s)$ submatrix

$$\left(\frac{\partial f_i}{\partial x_j}(p)\right)_{\substack{s+1 \le i \le n, \\ s+1 \le j \le n}}$$

of $J_F(p)$ is invertible. Define $\Phi: W \to \mathbb{R}^n$, $\Phi = (\phi_1, \ldots, \phi_n)$, as follows:

$$\phi_i(n) = \begin{cases} x_i - p_i, & 1 \le i \le s \\ f_i(x), & s+1 \le i \le n \end{cases}$$

Then Φ is an analytic map, and the Jacobian matrix $J_\Phi(p)$ of Φ at p is invertible. Hence, by the inverse mapping theorem (Theorem 2.1.6), there is a neighborhood $U \subseteq W$ of p in which Φ is invertible (i.e. $V := \Phi(U)$ is open in $\mathbb{R}^n$, and the restriction of Φ to U has an analytic inverse which maps V onto U). By definition of Φ, (2.2.1) holds. The other direction of the theorem is obvious. □

Now nonempty open subsets of $\mathbb{R}^n$ are submanifolds - in fact the nonempty open subsets are the n-dimensional submanifolds. But lower-dimensional submanifolds are not open. One can, however, define in a natural way the notion of an analytic function from an s-submanifold S into $\mathbb{R}$, where $0 \le s \le n$. Having the notion of chart at one's disposal

facilitates this definition. Let S be a subset of $\mathbb{R}^n$. A *chart* for S is a homomorphism from an open subset of S onto an open subset of $\mathbb{R}^s$, for some s, $0 \leq s \leq n$. Let S now be an s-dimensional submanifold, $0 \leq s \leq n$, and let p be a point of S. Let $U \subseteq \mathbb{R}^n$ be a neighborhood of p, and let $\Phi: U \to V$, $\Phi = (\phi_1, \ldots, \phi_n)$, be a coordinate system about p such that $\Phi(S \cap U) = T \cap V$, where T is given by (2.2.2). As remarked following the statement of Theorem 2.2.1, $T \equiv \mathbb{R}^s$ under the identification mapping $\iota: \mathbb{R}^s \to T$: let $T \cap V$ correspond to the neighborhood W of 0 in $\mathbb{R}^s$ under this identification (written $T \cap V \equiv W$). The mapping $\phi: S \cap U \to W$ given by

$$\phi(x) = (\phi_1(x), \ldots, \phi_s(x))$$

is a homomorphism with analytic inverse †, and is called the chart for S *corresponding to* Φ.

Definition. Let S be an s-submanifold of $\mathbb{R}^n$, $0 \leq s \leq n$, let T be given by (2.2.2), and let $f: S \to \mathbb{R}$ be a function. Then f is said to be *analytic* (in S) if for each point q of S there is a neighborhood U of q and a coordinate system $\Phi: U \to V$ about some point p of $S \cap U$, such that

(a) $\Phi(S \cap U) = T \cap V$; and

(b) $f \circ \phi^{-1}: W \to \mathbb{R}$ is analytic, where W is the neighborhood of 0 in $\mathbb{R}^s$ for which $T \cap V \equiv W$, and $\phi: S \cap U \to W$ is the chart for S corresponding to Φ. □

Condition (b) in the above definition can be paraphrased, "f is analytic

† (ϕ^{-1} is the composite of Φ^{-1} and the restriction of ι to W.)

with respect to the coordinate system Φ''. The following theorem states that if $f : S \to \mathbb{R}$ is analytic then, for each point p of S, f is analytic with respect to any coordinate system Φ about p satisfying condition (a) of the above definition.

Theorem 2.2.2. Let S be an s-submanifold of $\mathbb{R}^n$, $0 \leq s \leq n$, let T be given by (2.2.2), and let $f : S \to \mathbb{R}$ be an analytic function. Let p be a point of S and let $\Phi: U \to V$ be a coordinate system about p such that $\Phi(S \cap U) = T \cap V \equiv W$. Then $f \circ \phi^{-1}: W \to \mathbb{R}$ is analytic, where $\phi: S \cap U \to W$ is the chart for S corresponding to Φ.

Proof. Let $w \in W$. Then $w = \phi(q)$ for some point q of $S \cap U$. By definition there is a neighborhood U' of q and a coordinate system $\Psi: U' \to V'$ such that $\Psi(S \cap U') = T \cap V' \equiv W'$ and $f \circ \Psi^{-1}: W' \to \mathbb{R}$ is analytic, where $\psi: S \cap U' \to W'$ is the chart for S corresponding to Ψ. Let $\pi: \mathbb{R}^n \to \mathbb{R}^s$ be the projection $\pi(y_1,...,y_n) = (y_1,...,y_s)$. Then we have $(f \circ \phi^{-1})(y_1,...,y_s) = (f \circ \psi^{-1}) \circ (\pi \circ \Psi \circ \phi^{-1})(y_1,...,y_s)$ for every point $(y_1,...,y_s)$ of the neighborhood $\psi(S \cap U \cap U')$ of w. Therefore, by the composition theorem (Theorem 2.1.5), $f \circ \phi^{-1}$ is analytic near w. Hence $f \circ \phi^{-1}$ is analytic in W. □

Finally, a couple of results on the creation of new submanifolds from old.

Theorem 2.2.3. Let S be an s-submanifold of $\mathbb{R}^{n-1}$, $0 \leq s \leq n-1$, and let $f : S \to \mathbb{R}$ be an analytic function. Then the graph of f is an s-submanifold of $\mathbb{R}^n$.

Proof. Let G be the graph of f and let (p,p_n) be a point of G, where $p = (p_1,\ldots,p_{n-1})$. We shall find a coordinate system about (p,p_n) in $\mathbb{R}^n$ with respect to which G is locally the intersection of the last $n-s$ coordinate hyperplanes. By Theorem 2.2.1 there is a neighborhood $U \subseteq \mathbb{R}^{n-1}$ of p and a coordinate system $\Phi: U \to V$ about p such that $\Phi(S \cap U) = T \cap V$, where T is given by (2.2.2). Let W be the neighborhood of 0 in $\mathbb{R}^s$ such that $W \equiv T \cap V$ and let $\phi: S \cap U \to W$ be the chart for S corresponding to Φ. Let $\pi:\mathbb{R}^{n-1} \to \mathbb{R}^s$ be the projection $\pi(y_1,\ldots,y_{n-1}) = (y_1,\ldots,y_s)$. Then $\pi_0\Phi$ is an analytic map from U into $\mathbb{R}^s$. Hence, as W is a neighborhood of 0 in $\mathbb{R}^s$, the set $U' := (\pi_0\Phi)^{-1}(W)$ is a neighborhood of p in $\mathbb{R}^{n-1}$, with $U' \subseteq U$. Let $V' = \Phi(U')$ and define a map $\Psi: U' \times \mathbb{R} \to V' \times \mathbb{R}$ by

$$\Psi(x,x_n) = (\Phi(x),x_n - (f_0\phi^{-1})_0(\pi_0\Phi)(x)),$$

for $(x,x_n) \in U' \times \mathbb{R}$. Then Ψ is an analytic map (the n-th component of Ψ is analytic because $f_0\phi^{-1}$ is analytic in W by Theorem 2.2.2). In fact, one can verify that Ψ is invertible, with analytic inverse Ψ^{-1} given by

$$\Psi^{-1}(y,y_n) = (\Phi^{-1}(y),y_n + (f_0\phi^{-1})(y_1,\ldots,y_s),$$

for $y = (y_1,\ldots,y_{n-1}) \in V'$ and $y_n \in \mathbb{R}$. Thus Ψ is a coordinate system about (p,p_n). Where $\psi_1, \ldots, \psi_n$ are the components of Ψ, we have

$$G \cap (U' \times \mathbb{R}) = \{(x,x_n) \in U' \times \mathbb{R}: \psi_{s+1}(x,x_n) = 0,\ldots,\psi_n(x,x_n) = 0\}.$$

By Theorem 2.2.1, G is an s-submanifold of $\mathbb{R}^n$. □

Theorem 2.2.4. Let S be an s-submanifold of $\mathbb{R}^{n-1}$, $0 \le s \le n-1$, and let f and g be continuous functions from S into $\mathbb{R}$ (also allowed are $f \equiv -\infty$ or $g \equiv +\infty$) with $f < g$. Let $R = \{(x,x_n) \in S \times \mathbb{R}: f(x) < x_n < g(x)\}$. Then R is an $(s+1)$-submanifold of $\mathbb{R}^n$.

Proof. Let (p_1,p_n) be a point of R. By Theorem 2.2.1 there is a neighborhood $U \subseteq \mathbb{R}^{n-1}$ of p and a coordinate system $\Phi: U \to V$ about p, $\Phi = (\phi_1, \ldots, \phi_{n-1})$, such that

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

Choose $\epsilon > 0$ such that $f(p) < p_n - \epsilon < p_n + \epsilon < g(p)$. By continuity of f and g, there exists a neighborhood $U' \subseteq U$ of p in $\mathbb{R}^{n-1}$ such that $f(x) < x_n < g(x)$ for every $x \in S \cap U'$ and every $x_n \in (p_n - \epsilon, p_n + \epsilon)$. Let $I = (p_n - \epsilon, p_n + \epsilon)$, let $J = (-\epsilon,+\epsilon)$, and let $V' = \Phi(U')$. Define $\Psi: U' \times I \to V' \times J$ by $\Psi(x,x_n) = (\Phi(x),x_n - p_n)$. Then Ψ is an analytic map, with analytic inverse Ψ^{-1} given by $\Psi^{-1}(y,y_n) = (\Phi^{-1}(y),y_n + p_n)$. Where $\psi_1, \ldots, \psi_n$ are the components of Ψ, we have

$$R \cap (U' \times I) = \{(x,x_n) \in U' \times I : \psi_{s+1}(x,x_n) = 0,\ldots,\psi_{n-1}(x,x_n) = 0\}.$$

Even though $\psi_n(x,x_n) = 0$ is not included amongst the local defining equations for R, by an obvious analogue of Theorem 2.2.1, R is an $(s+1)$-submanifold of $\mathbb{R}^n$. □

2.3 Miscellaneous Results

Definition. Let $K = \mathbb{R}$ or $\mathbb{C}$. Let U be an open subset of K^n and let $f : U \to K$ be an analytic function. Let p be a point of U. If some partial derivative of f of non-negative order does not vanish at p then we say that f has *order* k at p, and write $ord_p f = k$, provided that k is the least non-negative integer such that some partial derivative of f of order k does not vanish at p; we also say that f has *order* k_i at p *in* x_i, provided that k_i is the least non-negative integer such that some partial derivative of f of order k_i in x_i does not vanish at p. If, on the other hand, all partial

derivatives of f of all orders vanish at p, then we say that f has order ∞ at p, and write $ord_p f = \infty$; we also say that f has order ∞ at p in each x_i.

Theorem 2.3.1. Let $K = \mathbb{R}$ or $\mathbb{C}$. 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,

$$ord_{G(p)} f \leq ord_p f \circ G.$$

Proof. Let the coordinates of K^n be $(x_1,...,x_n)$ and let those of K^m be $(y_1,...,y_m)$. Let $h = f \circ G$. We prove by induction on k that every partial derivative of h of order k is a finite sum of terms of the form

$$(P \circ G)Q$$

where $P = P(y_1,...,y_m)$ is a partial derivative of $f = f(y_1,...,y_m)$ of order $\leq k$ and Q is an analytic function. This is true for $k = 0$ by definition of h. Assume that the above proposition is true for $k \geq 0$. Let $R = \dfrac{\partial^{k+1} h}{\partial x_1^{i_1} \cdots \partial x_n^{i_n}}$ be a partial derivative of h of order $k+1$. As some $i_s > 0$, we have $R = \dfrac{\partial S}{\partial x_s}$, where S is a partial derivative of h of order k. By the induction hypothesis, S is a finite sum of terms of the form $(P \circ G)Q$, where P is a partial derivative of f of order $\leq k$. (Let $g_1,...,g_m$ be the component functions of G.) As

$$\frac{\partial (P \circ G)Q}{\partial x_s} = \frac{\partial (P \circ G)}{\partial x_s} \cdot Q + (P \circ G) \frac{\partial Q}{\partial x_s}$$

and

$$\frac{\partial (P \circ G)}{\partial x_s} = \left(\frac{\partial P}{\partial y_1} \circ G\right)\frac{\partial g_1}{\partial x_s} + \cdots + \left(\frac{\partial P}{\partial y_m} \circ G\right)\frac{\partial g_m}{\partial x_s},$$

it follows that $\frac{\partial(P_0G)Q}{\partial x_s}$ is a finite sum of terms of the form $(P_0'G)Q'$, where P' is a partial derivative of f of order $\leq k+1$. Hence R is such a sum. We have shown that the required proposition holds for $k+1$. The proof by induction is complete.

Let p be a point of U and let the order of f at $G(p)$ be l. If $l=0$ then clearly $ord_p h = 0$, so assume $l > 0$. Let R be a partial derivative of h of order $k < l$. Then R is a finite sum of terms of the form $(P_0G)Q$, where P is a partial derivative of f of order $\leq k$. But $P(G(p)) = 0$ for every partial derivative P of f of order $\leq k$, as $ord_{G(p)} f = l > k$. Hence $R(p) = 0$. It follows that $ord_p h \geq l$. □

Theorem 2.3.2 (Root continuity principle).

Let $f(z) = f_0 z^d + f_1 z^{d-1} + \cdots + f_d$ be a polynomial in $\mathbb{C}[z]$, with $f_0 = f_1 = \cdots = f_{d-b-1} = 0$ and $f_{d-l} \neq 0$, for some l, $0 \leq l \leq d$. Let α be a root of $f(z)$ of multiplicity m and let C be a circle in the complex plane centered at α, of radius $\epsilon > 0$, such that $f \neq 0$ in the punctured disc $0 < |z-\alpha| \leq \epsilon$. Then there is a number $\delta > 0$ such that if $g_0, g_1, \ldots, g_d \in \mathbb{C}$ and $|g_j - f_j| < \delta$ for $0 \leq j \leq d$, then the polynomial

$$g(z) = g_0 z^d + g_1 z^{d-1} + \cdots + g_d \tag{2.3.1}$$

has exactly m roots inside C.

Proof. There exists $\delta > 0$ such that if $g_1, \ldots, g_d \in \mathbb{C}$, $|g_j - f_j| < \delta$ for $0 \leq j \leq d$, and $g(z)$ is given by (2.3.1), then $|g(z) - f(z)| < |f(z)|$ for $|z| = \epsilon$. Let $g_0, \ldots, g_d \in \mathbb{C}$ and let $|g_j - f_j| < \delta$ for $0 \leq j \leq d$. Let $g(z)$ be defined by (2.3.1) and let $f_s(z) = f(z) + s(g(z) - f(z))$, for $0 \leq s \leq 1$.

Now if $0 \leq s \leq 1$ then

$$\begin{aligned} |f_s(z)| = |f(z)+s(g(z)-f(z))| &\geq ||f(z)|-|s(g(z)-f(z))|| \\ &= ||f(z)|-s|g(z)-f(z)|| \\ &> 0 \end{aligned}$$

for $|z| = \epsilon$. Hence, if $0 \leq s \leq 1$, then $f_s(z)$ has a total number m_s of zeros inside C given by

$$m_s = \frac{1}{2\pi i} \int_C \frac{f_s'(\zeta)d\zeta}{f_s(\zeta)}. \tag{2.3.2}$$

But the integral on the right-hand side of (2.3.2) is continuous in s and is integer-valued, and hence is constant. Therefore $m_0 = m_1$. □

Let R be an integral domain and let

$$\begin{aligned} A(x) &= a_0x^m + a_1x^{m-1} + \cdots + a_m, \\ B(x) &= b_0x^n + b_1x^{n-1} + \cdots + b_n \end{aligned}$$

be polynomials in $R[x]$, not both constant, of degrees m and n respectively. The *Sylvester matrix* of A and B is the $m+n$ by $m+n$ matrix

$$M = \begin{bmatrix} a_0 & a_1 & \cdot & \cdot & \cdot & a_m & & \\ & a_0 & a_1 & \cdot & \cdot & \cdot & a_m & \\ & & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ & & & a_0 & a_1 & \cdot & \cdot & \cdot\ a_m \\ b_0 & b_1 & \cdot & \cdot & \cdot & b_n & & \\ & b_0 & b_1 & \cdot & \cdot & \cdot & b_n & \\ & & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ & & & & b_0 & b_1 & \cdot & \cdot\ b_n \end{bmatrix}$$

The *resultant* of A and B, $res(A,B)$, is defined by

$$res(A,B) = \det(M).$$

Suppose now that the characteristic of R is zero and that A is not constant. Then $ma_0 \neq 0$, and so the degree of the derivative

$$A'(x) = ma_0x^{m-1} + (m-1)a_1x^{m-2} + \cdots + a_{m-1}$$

of $A(x)$ is $m-1$. Consider the Sylvester matrix of A and A'. The first column has two nonzero entries, a_0 and ma_0. Hence we can factor out a_0 from $res(A,A')$. The *discriminant* of A, $discr(A)$, is defined by the equation

$$a_0 discr(A) = (-1)^{m(m-1)/2}\, res(A,A')$$

Let K be the quotient field of R and let Ω be an algebraic closure of K. Then we can completely factor $A(x)$ and $B(x)$ into linear factors over Ω thus:

$$A(x) = a_0(x-\alpha_1)\cdots(x-\alpha_m), \tag{2.3.3}$$

$$B(x) = b_0(x-\beta_1)\cdots(x-\beta_n). \tag{2.3.4}$$

The following expressions for $res(A,B)$ and $discr(A))$ are well-known:

$$res(A,B) = a_0^n b_0^m \prod_{i,j} (\alpha_i - \beta_j) \tag{2.3.5}$$

$$discr(A) = a_0^{2m-2} \prod_{i<j} (\alpha_i - \alpha_j)^2. \tag{2.3.6}$$

Theorem 2.3.3. Let $A(x)$ and $B(x)$ be non-constant polynomials over the integral domain R of characteristic zero. Let $C(x) = A(x)B(x)$. Then

$$discr(C) = discr(A)(res(A,B))^2\, discr(B).$$

Proof. Let K be the quotient field of R and let Ω be an algebraic closure of K. Factor $A(x)$ and $B(x)$ completely over Ω as in (2.3.3) and (2.3.4). Let $\gamma_1 = \alpha_1, \ldots, \gamma_m = \alpha_m$, $\gamma_{m+1} = \beta_1, \ldots, \gamma_{m+n} = \beta_n$. Let $c_0 = a_0b_0$ and $l = m + n$. Then

$$C(x) = c_0(x - \gamma_1)\cdots(x - \gamma_l).$$

Therefore

$$\begin{aligned} discr(C) &= c_0^{2l-2} \prod_{1\le i<j\le l} (\gamma_i - \gamma_j)^2 \\ &= \left(a_0^{2m-2} \prod_{1\le i<j\le m} (\alpha_i - \alpha_j)^2 \right) \cdot \left(a_0^{2n} b_0^{2m} \prod_{\substack{1\le i\le m,\\ 1\le j\le n}} (\alpha_i - \beta_j) \right)^2 \end{aligned}$$

$$\cdot \left(b_0^{2n-2} \prod_{1 \le i < j \le n} (\beta_i - \beta_j)^2 \right)$$

$$= discr(A)(res(A,B))^2 \, discr(B). \square$$

The *sum-norm* (or just *norm* for short) of an integral polynomial A in r variables is the sum of the absolute values of the integer coefficients of A. The *max-norm* of such a polynomial is the maximum of the absolute values of the integer coefficients. We denote the sum-norm by $|A|_1$, and the max-norm by $|A|_\infty$. The following theorem leads to a bound for the coefficients of the factors of an r-variate integral polynomial.

Theorem 2.3.4 (*Gelfond*) : Let $A_1, \ldots, A_k$ be r-variate polynomials with complex coefficients, and let $A = A_1 \cdots A_k$. Let n_i be the degree of A in the i-th variable, assume $n_i > 0$ for all i, and let $m = \sum_{i=1}^{r} n_i$. Then

$$\prod_{j=1}^{k} |A_j|_\infty \le 2^{m-r/2} |A|_1 .$$

Proof : See [GEL60], pp 135-139.

Corollary 2.3.5 : Let A be a non-zero integral polynomial in r variables, and let B be a factor of A. Let n be a bound for the degree of A in each variable. Then

$$|B|_1 \le (n+1)^r \, 2^{rn-r/2} . |A|_1 .$$

Proof : As B has at most $(n+1)^r$ terms, we have

$$|B|_1 \le (n+1)^r . |B|_\infty .$$

The corollary now follows from the theorem. □

Chapter Three

Reduced Projection Map for Cylindrical Algebraic Decomposition

In this chapter we launch the main thrust of the thesis. Section 1 contains a review of the essential aspects of the cylindrical algebraic decomposition (cad) algorithm. The main focus of the review is the projection operation used in the cad algorithm. In Section 2 we introduce a new projection map, which is a reduced version of the original. Theorems are presented which suggest the usefulness of the reduced projection map in cad construction (algorithms for cad computation using the new projection are presented in Chapter 5). Section 3 contains mathematical details that substantiate the results in Section 2.

3.1 The original cad algorithm and its projection map

The purpose of this section is to provide a quick introduction to the cad algorithm. More detailed accounts appear in a number of sources, e.g. [COL75], [ARN81], [ACM84a].

Let A be a finite set of r-variate polynomials, $r \geq 1$. An *A-invariant cylindrical algebraic decomposition* (cad) of $\mathbb{R}^r$ partitions $\mathbb{R}^r$ into a finite collection of semialgebraic cells in each of which every polynomial in A is sign-invariant. A more precise definition of cad is given in [ACM84a]. An

A-invariant cad of the plane, where

$$A = \{F(x,y) = y^4 - 2y^3 + y^2 - 3x^2y + 2x^4\},$$

is depicted in Figure 3.1.1. Note that $F(x,y)$ vanishes in each of the 0-cells and "curved" 1-cells, and is either positive or negative throughout each of the remaining cells.

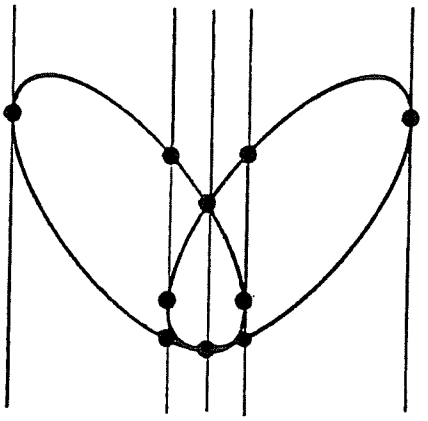

Fig. 3.1.1.

The cad algorithm 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 sample points and (if required) defining formulas 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 projection 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 $\mathbb{R}^{i+1}$, $i = 1,2,...,r-1$). We shall describe each of the phases in turn.

For a set A of r-variate integral polynomials, we shall define a set $PROJ(A)$ of $r-1$-variate polynomials whose zeros contain the projection of the "critical locus" of A. We shall show that for any $PROJ(A)$-invariant j-cell R in $\mathbb{R}^{r-1}$, the cylinder over R (i.e. $R \times \mathbb{R}$) is partitioned by the zeros of A into a finite number of pairwise disjoint j-cells (the graphs of continuous functions defined on R) and their complementary $j+1$-cells. This property will enable us to carry out the extension of a $PROJ(A)$-invariant cad of $\mathbb{R}^{r-1}$ to an A-invariant cad of $\mathbb{R}^r$.

We introduce some terminology first. The *reductum* of a polynomial F is the polynomial $F - ldt(F)$, where $ldt(F)$ is the leading term of F, i.e. the term of highest degree. Let $red^k(F)$ denote the k-th reductum of F. Let $F(x)$ and $G(x)$ be nonzero polynomials over an integral domain D, F and G not both constant. Let $n = min(deg(F), deg(G))$. For $0 \leq j \leq n$, let $S_j(F,G)$ denote the j-th subresultant polynomial of F and G, an element of $D[x]$ of degree $\leq j$. (Each coefficient of $S_j(F,G)$ is the determinant of a certain matrix of F and G coefficients; see [LOO82b], [BRT71], or [COL75] for the exact definition. Subresultant polynomials are intimately connected with polynomial remainder sequences: the fundamental theorem of polynomial remainder sequences [BRT71] makes the connections explicit. The fact concerning subresultant polynomials of chief importance to us is that if D is a unique factorization domain, then where $k = deg(gcd(F,G))$, we have $S_j(F,G) = 0$ for $0 \leq j < k$, and $S_k(F,G) = gcd(F,G)$ modulo multiplication by elements of D.) For $0 \leq j \leq n$, the *j-th subresultant of F and G*, written $subres_j(F,G)$, is the coefficient of x^j in $S_j(F,G)$. Note that $subres_0(F,G) = res(F,G)$. Suppose now that the characteristic of D is 0.

Let $ldcf(F)$ denote the leading coefficient of F, and assume that $(n :=) deg(F) > 0$. Then $n.ldcf(F) \neq 0$, and so the degree of F', the derivative of F, is $n-1$. By considering the Sylvester matrix of F and F', it can be seen that, for $0 \leq j \leq n-1$, $ldcf(F)$ is a divisor of $subres_j(F,F')$. For $0 \leq j \leq n-1$, we define the *j-th subdiscriminant of F and G*, written $subdiscr_j(F,G)$, by the equation

$$ldcf(F).subdiscr_j(F) = (-1)^{n(n-1)/2}.subres_j(F,F')$$

(cf. definition of $discr(F)$ in Sec. 2.3). Note that $subdiscr_0(F) = discr(F)$.

Let A be a set of integral polynomials in the r variables $x_1,\ldots,x_r$. We regard the elements of A as polynomials in x_r over the ring of polynomials in $x_1,\ldots,x_{r-1}$. We now define several sets of $(r-1)$-variate polynomials. The *reducta set of* A written $red(A)$ is the set

$$\{ red^k(F) : F \in A, 0 \leq k \leq deg(F), red^k(F) \neq 0 \}$$

The *coeffficient set of* A, written $coeff(A)$, is the set

$$\{ f(x_1,\ldots,x_{r-1}) : f \text{ is a non-zero coefficient of some } F \in A \}.$$

The *subdiscriminant set of* A, written $subdiscr(A)$, is defined to be

$$\{ subdiscr_j(F) : F \in A, 0 \leq j < deg(F') \}$$

The *subresultant set of* A, written $subres(A)$, is defined to be

$$\{ subres_j(F,G) : F,G \in A, F \neq G, 0 \leq j < min(deg(F),deg(G)) \}.$$

We can now define the projection of A. Suppose first that A is a squarefree basis (that is, the elements of A have positive degree, and are primitive, squarefree and pairwise relatively prime). Then we define $PROJ(A)$ to be

the set

$$coef\,f\,(A) \cup subdiscr\,(red\,(A)) \cup subres\,(red\,(A)).$$

Now let A be any set of r-variate integral polynomials. Let $cont\,(A)$ be the set of non-constant contents of elements of A, and let $prim\,(A)$ be the set of primitive parts of positive degree of elements of A. Then where B is the finest squarefree basis for $prim\,(A)$ (that is, the set of irreducible divisors of elements of $prim\,(A)$), we set

$$PROJ\,(A) = cont\,(A) \cup PROJ\,(B).$$

The following concept is crucial:

Definition: A real polynomial $F\,(x, x_r)$ is said to be *delineable* on a subset S of $\mathbb{R}^{r-1}$ if

(1) the portion of the real variety of F lying in the cylinder over S consists of the union of the graphs of some $k \geq 0$ continuous functions $\theta_1 < \cdots < \theta_k$ from S to $\mathbb{R}$; and

(2) there exist integers $m_1,\ldots,m_k \geq 1$ such that for every $a \in S$, the multiplicity of the root $\theta_i(a)$ of $F\,(a, x_r)$ is m_i.

In the above definition, the graphs of the functions θ_i are called the *F-sections* over S. The regions between successive F-sections are called *F-sectors*.

We can now state the main theorem about *PROJ*:

Theorem 3.1.1: Let A be a finite set of integral polynomials in r variables and let $c \subseteq \mathbb{R}^{r-1}$ be a connected set in which every element of $PROJ\,(A)$ is

sign-invariant. Then every element of A is either delineable or identically zero on c, and the sections of A over c are pairwise disjoint.

We briefly discuss the ideas involved in the proof. It is shown in [COL75] that for a polynomial $F(x, x_r)$ whose leading coefficient does not vanish on a set $c \subseteq \mathbb{R}^{r-1}$, the invariance of the number of distinct roots of $F(a, x_r)$ as a varies within c implies the delineability of F on c. On the other hand, the number of distinct roots of $F(a, x_r)$ is equal to $d - k$, where d is the degree of F in x_r and k is the least integer $j \geq 0$ such that $subdiscr_j(F)(a) \neq 0$ (this follows from the fundamental theorem of polynomial remainder sequences [BRT71]).

Let us assume the hypotheses of the main theorem, and assume first that A is a squarefree basis. Let F be an element of A which is not identically zero on c. Then as the elements of $coeff(A)$ are sign-invariant on c, F is identical with some reductum G of F on c, such that G has non-vanishing leading coefficient on c. As the elements of $subdiscr(red(A))$ are sign-invariant on c, $subdiscr_j(G)$ is sign-invariant on c, for $0 \leq j \leq deg(G)$. Thus, by the above remarks, the number of distinct roots of $G(a, x_r)$ is invariant throughout c, hence G (and therefore F) is delineable on c. The invariance of $subres(red(A))$ on c ensures that the various sections of elements of A on c are pairwise disjoint.

If A is an arbitrary set of polynomials, then we can apply the above argument to the basis B for $prim(A)$. The required conclusions for A follow immediately. The reader can consult either [COL75] or [ACM84a] for a more detailed proof □

Let A be the input to the cad algorithm. Let us assume for the present that defining formula construction is not required. In the projection phase of the algorithm we compute $PROJ(A)$,$PROJ(PROJ(A)) = PROJ^2(A)$, and so on, until we compute $PROJ^{r-1}(A)$. It is the task of the base phase to construct a $PROJ^{r-1}(A)$-invariant cad of $\mathbb{R}^1$. We begin the base phase by constructing the set of all distinct irreducible factors of nonzero elements of $PROJ^{r-1}(A)$. We then isolate the real roots of (the product of) these factors. We thus have an exact representation for each root consisting of its minimal polynomial and and an isolating interval (see [LOO82a], Section 1 for more information on this). The cad of $\mathbb{R}^1$ consists of the collection of these roots (the 0-cells) together with the collection of complementary open intervals (the 1-cells). Sample points for the 0-cells are the roots themselves represented as above, while rational sample points for the 1-cells can be readily chosen. Defining formulas for the 0-cells and 1-cells can be obtained in a straightforward manner (see p. 45 of [ARN81]).

Let $D*$ be the cad of $\mathbb{R}^1$ constructed as above. Let us first consider the extension of $D*$ to a cad of $\mathbb{R}^2$. In the projection phase we computed a set $J = PROJ^{r-2}(A)$. Let c be a cell of $D*$. Then by Theorem 3.1.1, the cylinder over c is partitioned by the zeros of J into a finite number of sections and sectors. These sections and sectors will be cells of our decomposition of $\mathbb{R}^2$. We now describe how to determine the number of these cells over c, as well as a sample point for each cell. Let α be the sample point for c, and let J_c be the product of all elements G of J for which $G(\alpha,x_2) \neq 0$. Using algorithms for exact arithmetic in $Q(\alpha)$ [LOO82a], we construct $J_c(\alpha,x_2)$. We isolate the real roots of $J_c(\alpha,x_2)$, which provides us

with the number of sections and sectors of J lying over c. Now (α,β) lies on a section of J over c if and only if β is a root of $J_c(\alpha,x_2)$. For each such β, we use the representation for α, the isolating interval for β, and the algorithms NORMAL and SIMPLE of [LOO82a] to construct a primitive element γ for $Q(\alpha,\beta)$; we use γ to construct an appropriate representation for the algebraic point (α,β), by expressing α and β as polynomials in γ. We readily get sector sample points of the form (α,r), with r rational.

After processing each cell c of D^* in this way, we have determined a cad of $\mathbb{R}^2$ and constructed a sample point for each cell.

Extension from $\mathbb{R}^{i-1}$ to $\mathbb{R}^i$ for $3 \leq i \leq r$ is essentially the same as from $\mathbb{R}^1$ to $\mathbb{R}^2$. The only difference is that a sample point in $\mathbb{R}^{i-1}$ has $i-1$, instead of just one, coordinates. But where α is the primitive element of an $\mathbb{R}^{i-1}$ sample point, and F is a polynomial in r variables, arithmetic in $Q(\alpha)$ still suffices for constructing the univariate polynomial over $Q(\alpha)$ that results from substituting the coordinates $(\alpha_1, \ldots, \alpha_{i-1})$ for $(x_1,\ldots,x_{i-1})$ in F.

We have also to define the *augmented projection* $APROJ(A)$ of A, which is used when defining formulas are to be constructed. First some notation:

Definition Let us take the degree of the zero polynomial to be -1. Let

$$f(x,x_r) = f_0(x)x_r^d + f_1(x)x_r^{d-1} + \cdots + f_d(x)$$

be a polynomial in $\mathbb{R}[x,x_r]$ and let S be a subset of $\mathbb{R}^{r-1}$. Say that f is *degree-invariant* in S if there exists l, $-1 \leq l \leq d$, called the degree of f in S (written $deg_S(f)$), such that for every point p of S, the univariate polynomial $f(p,x_r)$ has degree l. If f is degree-invariant and of non-negative degree l in S then $f_0 = f_1 = \cdots = f_{d-l-1} = 0$ in S, while

$f_{d-l} \neq 0$ in S (the converse is also true).

Let $F^{(j)}$ denote the j-th derivative of F. Define the *derivative set* $der(A)$ of A to be the set

$$\{ F^{(j)} : F \in A, 0 < j \leq deg(F) \}.$$

Suppose first that A is a squarefree basis. Then we define $APROJ(A)$ to be the set

$$subdiscr(der(red(A))) \cup PROJ(A).$$

If A is an arbitrary set of polynomials then where B is the finest squarefree basis for $prim(A)$, we set

$$APROJ(A) = cont(A) \cup APROJ(B).$$

The role of the augmented projection in defining formula construction is indicated by the following two theorems:

Theorem 3.1.2: Let A be a finite set of integral polynomials in r variables and let $c \subseteq \mathbb{R}^{r-1}$ be a connected set in which every element of $APROJ(A)$ is sign-invariant. Then for every $F \in A$, F is degree-invariant on c, and $F^{(j)}$ is delineable on c, for every j, $0 \leq j \leq deg_c(F)$.

Theorem 3.1.3: Let F be an integral polynomial in r variables. Let $c \subseteq \mathbb{R}^{r-1}$ be a connected set on which F is degree-invariant and not identically zero, and on which $F^{(j)}$ is delineable for $0 \leq j \leq deg_c(F)$. Then, given a sample point and a defining formula for c, we can construct defining formulas for the F-sections and F-sectors over c.

For the proofs of these theorems one should consult Sec. 2.5 of [ARN81].

The following abstract algorithm indicates how augmented projections are used in the cad algorithm, and generally serves to summarize the discussion of this section.

$CAD(r, A, k; S, F)$

[Cylindrical algebraic decomposition. A is a set of integral polynomials in r variables, $r \geq 1$. k satisfies $0 \leq k \leq r$. S is a list of sample points for an A-invariant cad D of $\mathbb{R}^r$. If $k \geq 1$, F is a list of defining formulas for the induced cad of $\mathbb{R}^k$, and if $k = 0$, F is the empty list.]

(1) [Initialize.] Set $B \leftarrow$ the finest squarefree basis for $prim(A)$. Set $S \leftarrow ()$ and $F \leftarrow ()$.

(2) [$r = 1$.] If $r > 1$ then go to 3. Isolate the real roots of B. Construct sample points for the cells of D and add them to S. If $k = 1$, then construct defining formulas for the cells of D and add them to F. Exit.

(3) [$r > 1$.] If $k < r$ then set $P \leftarrow PROJ(A)$ and $k' \leftarrow k$; otherwise set $P \leftarrow APROJ(A)$ and $k' \leftarrow k - 1$. Call CAD recursively with inputs $r - 1$, P, and k' to obtain outputs S' and F' which specify a P-invariant cad D' of $\mathbb{R}^{r-1}$. For each cell c of D', let α denote the sample point for c, and carry out the following sequence of steps: set $B^* \leftarrow$ the set of all $B_j(\alpha, x_r)$ such that $B_j \in B$ and $B_j(\alpha, x_r) \neq 0$; isolate the real roots of B^*; use α and the isolating intervals for the roots of B^* to construct sample points for the B-sections and B-sectors over c, adding them to S; if $k = r$, then, from the defining formula for c, construct defining formulas for the B-sections and B-sectors over c, adding them to F, and if $k < r$, set $F \leftarrow F'$. Exit □

3.2 A reduced projection map and new projection theorem

In this section we introduce a new projection map P which is a 'reduced' version of the map *PROJ* discussed in Section 3.1. We state a theorem analogous to Theorem 3.1.1 which implies that under certain assumptions on a given set A of polynomials, any cad of $\mathbb{R}^{r-1}$ such that every element of $P(A)$ has constant order (as opposed to sign - recall the definition of order given in Section 2.3) throughout every cell, can be lifted (or extended) to a cad of $\mathbb{R}^r$ such that every element of A has constant order throughout every cell. The mathematical result underlying this analogue of Theorem 3.1.1 will be termed *the lifting theorem*, and is the main contribution of this thesis. In this section we state the lifting theorem and derive the important consequences for cad construction from it. We postpone the proof of the lifting theorem to the next section of this chapter. In Chapter 5, we present algorithms for cad construction based upon the lifting theorem.

Before we can state the lifting theorem we need to make a few definitions.

Definition Let $K = \mathbb{R}$ or $\mathbb{C}$. Let U be an open subset of K^r and let $f : U \to K$ be an analytic function. We say that f is *order-invariant* in a subset S of U provided that the order of f is the same at every point of S.

Example. Let $f : \mathbb{R}^2 \to \mathbb{R}$ 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 ($\mathrm{ord}_{(0,0)} f = 2$).

Remark. Let U and V be open subsets of K^r, let $G : U \to V$ be an analytic isomorphism, and let $f : V \to K$ be an analytic function. By Theorem 2.1.5 the composite function $f \circ G$ is analytic in U. It follows from Theorem 2.3.1 that, for every point p of U,

$$\mathrm{ord}_{G(p)} f = \mathrm{ord}_p f \circ G.$$

Hence, if S is a subset of U, then f is order-invariant in $G(S)$ if and only if $f \circ G$ is order-invariant in S.

Throughout the remainder of this section and the next, let x denote the $(r-1)$-tuple $(x_1,\ldots,x_{r-1})$ and let (x, x_r) denote $(x_1,\ldots,x_{r-1},x_r)$.

We now introduce the concept of analytic delineability.

Definition. Let S be a connected submanifold of $\mathbb{R}^{r-1}$. We saw in Sec. 2.2 that one can define the notion of an analytic function from S into $\mathbb{R}$. If $f(x, x_r)$ is a real polynomial then we say f is *analytic delineable* on S if f is delineable on S by means of some $k \geq 0$ analytic functions $\theta_1 < \cdots < \theta_k$ from S into $\mathbb{R}$.

Remark. Suppose that $f(x, x_r)$ is analytic delineable on the connected s-submanifold S of $\mathbb{R}^{r-1}$. Then each f-section over S is a connected s-submanifold of $\mathbb{R}^r$ (Theorem 2.2.3) and each f-sector over S is a connected $(s+1)$-submanifold of $\mathbb{R}^r$ (Theorem 2.2.4).

We can now state our main mathematical result.

Theorem 3.2.1 (*Lifting theorem*). Let $f(x, x_r)$ be a squarefree polynomial

in $\mathbb{R}[x, x_r]$ of positive degree in x_r and with non-zero discriminant $D(x)$. Let S be a connected submanifold of $\mathbb{R}^{r-1}$ in which f is degree-invariant and of non-negative degree, and in which D is order-invariant. Then f is analytic delineable on S and is order-invariant in each f-section over S.

The proof of this theorem is quite long, and is supplied in the next section of this chapter. The theorem will enable us to show that our reduced projection map P, to be defined shortly, is essentially as good (for the purpose of cad construction) as its larger counterpart *PROJ*.

We now proceed to define the map P. Let A be a set of r-variate integral polynomials. Recall the definition of the coefficient set $coef f(A)$ from the previous section. We define the *discriminant set of* A, written $discr(A)$, to be the set

$$\{ discr(F) : F \in A, deg(F) \geq 2 \},$$

and the *resultant set of* A, written $res(A)$, to be the set

$$\{ res(F,G) : F,G \in A, F \neq G, deg(F), deg(G) \geq 1 \}.$$

We can now define P. Suppose first that A is a squarefree basis. We set

$$P(A) = coef f(A) \cup discr(A) \cup res(A).$$

Now let A be any set of r-variate polynomials. We set

$$P(A) = cont(A) \cup P(B),$$

where B is the finest squarefree basis for $prim(A)$.

Noting that the resultant of two polynomials F and G is equal to $subres_0(F,G)$, and that the discriminant of F is equal to $subdiscr_0(F)$, we

can compare the definitions of *PROJ* and P. It is clear that $P(A)$ is a subset of $PROJ(A)$. There are two respects in which *PROJ* and P differ. The first is that *PROJ* forms resultants, etc. of elements of the *reductum set* of B, whereas P forms resultants, etc. from just B itself. The second is that *PROJ* constructs full sequences of $subdiscr_j$'s and $subres_j$'s, whereas P constructs only the 0-th order *subdiscr*'s and *subres*'s (i.e. discriminants and resultants only).

Before deriving a counterpart of Theorem 3.1.1, we give a useful lemma.

Lemma 3.2.2 : Let $K = \mathbb{R}$ or $\mathbb{C}$. Let $F_1,...,F_n$ be nonconstant analytic functions defined in an open subset U of K^r, and let $f = F_1...F_n$. Let S be a connected subset of U. Then f is order-invariant in S if and only if each F_i is order-invariant in S.

The proof is straightforward. □

We now state our central result pertaining to P:

squarefree

Theorem 3.2.3 : Let A be a finite basis consisting of r-variate integral polynomials, $r \geq 2$, and let S be a connected submanifold of $\mathbb{R}^{r-1}$. Suppose that each element of A is not identically zero on S, and that each element of $P(A)$ is order-invariant in S. Then each element of A is degree-invariant and analytic-delineable on S, the sections of A over S are pairwise disjoint, and each element of A is order-invariant in every section of A over S.

Proof. Assume that some element of A is nonconstant (otherwise the theorem is trivial) and let $F_1,\ldots,F_n$ be the nonconstant elements of A. Let $f = \prod_{i=1}^{n} F_i$. Then f is squarefree, as the F_i are squarefree and pairwise relatively prime. Let $D(x)$ be the discriminant of $f(x,x_r)$. By Theorem 2.3.3

$$D = \prod_{i=1}^{n} discr(F_i).\prod_{i<j} res(F_i,F_j)^2.$$

By hypothesis, each $discr(F_i)$ and each $res(F_i,F_j)$ is order-invariant in S. Hence, by Lemma 3.2.2, D is order-invariant in S. Furthermore, f is not identically zero on S, and is degree-invariant on S. Hence, by the lifting theorem, f is analytic delineable on S, and is order-invariant in each f-section over S. By Lemma 3.2.2, each F_i is order-invariant in every such section. The conclusions of the theorem now follow. □

We shall also define a reduced augmented projection map AP, and establish a counterpart of Theorem 3.1.2. Let A be a squarefree basis of integral polynomials in $Z[x,x_r]$. We define a slight variant of the derivative set of A: where $gsfd(P)$ denotes the greatest squarefree divisor of the polynomial P, let

$$der^*(A) = \{gsfd(prim(F^{(j)})) : F \in A, 0 < j \leq deg(F)\}.$$

We set

$$AP(A) = discr(der^*(A)) \cup P(A).$$

For an arbitrary set A we set

$$AP(A) = cont(A) \cup AP(B),$$

where B is the finest squarefree basis for $prim(A)$.

The following result is our counterpart of Theorem 3.1.2:

Theorem 3.2.4 : Let A be a finite squarefree basis of integral polynomials in r variables, where $r \geq 2$, and let S be a connected submanifold of $\mathbb{R}^{r-1}$. Suppose that each element of A is not identically zero on S, and that each element of $AP(A)$ is order-invariant in S. Then, for each $F \in A$, F is degree-invariant on S, and $F^{(j)}$ is delineable on S, for every j, $0 \leq j \leq deg_S(F)$.

Proof : Let $F \in A$. The degree-invariance of F on S is obvious. Let $0 \leq j \leq deg_S(F)$. Then $F^{(j)}$ is degree-invariant and not identically zero on S (as F is). Let G be the greatest squarefree divisor of the primitive part of $F^{(j)}$. Then, as G is a divisor of $F^{(j)}$, G is degree-invariant and not identically zero on S. By hypothesis, the discriminant of G is order-invariant in S. Hence, by the lifting theorem, G is delineable on S. As the content of $F^{(j)}$ is non-zero in S, it follows that $F^{(j)}$ is delineable on S. □

3.3 Proof of the lifting theorem

The lifting theorem can be regarded as an adaptation to Euclidean space of certain aspects of O. Zariski's work on equisingularity over the complex field. In this section we give a straightforward proof of the lifting theorem based upon a recent result due to Zariski [ZAR75]. We do not, however, require the reader to consult Zariski's original paper and to attempt to see how the result stated therein is applicable. Instead, we provide in Chapter 4 a self-contained, and in some respects original, rendition of the relevant theorems due to Zariski.

The proof presented in this section is quite detailed, and hence rather long. The main thread of the proof can be gleaned from the first few pages.

Notation. We denote by $Z(S)$ the cylinder over a subset S of $\mathbb{R}^{r-1}$ (i.e. $Z(S) = S \times \mathbb{R}$).

Proof of 3.2.1 : Let the dimension of S be s, where $0 \leq s \leq r-1$. If $s = 0$ then the theorem is trivial. For $1 \leq s \leq r-1$, the theorem follows from the following assertion as to the "local delineability" of f :

Assertion 1. For each point p of S there is a neighborhood $N \subseteq \mathbb{R}^{r-1}$ of p such that f is analytic delineable on $S \cap N$ and f is order-invariant in each f -section over $S \cap N$.

We explain now how the theorem can be deduced from the above assertion. Let Assertion 1 hold. Then it follows by connectedness of S that the number, say $k \geq 0$, of distinct real roots of the univariate polynomial $f(p, x_r)$ does not depend upon the particular point p of S (that this number is locally constant is an immediate consequence of Assertion 1). If $k = 0$ then the theorem is vacuously true, so let $k \geq 1$. Then one can define k functions $\Theta_1, \cdots, \Theta_k$ from S into $\mathbb{R}$ by setting $\Theta_i(p)$ equal to the i-th real root of $f(p, x_r)$, for p in S and $1 \leq i \leq k$. Clearly the graphs of the Θ_i comprise the portion of the real variety of f lying in the cylinder over S . Let p be a point of S . Then by Assertion 1 there is a neighborhood $N \subseteq \mathbb{R}^{r-1}$ of p and k analytic functions from $S \cap N$ into $\mathbb{R}$, say $\theta_1 < \cdots < \theta_k$, whose graphs comprise the portion of the real variety of f which lies in $Z(S \cap N)$, and such that f is order-invariant in the graph of

each θ_i. Let $1 \leq i \leq k$. As $\Theta_i(x) = \theta_i(x)$ for all x in $S \bigcap N$ it follows that Θ_i is analytic near p, and hence in S. Thus f is analytic delineable on S. By connectedness of S, f is order-invariant in the graph of each Θ_i. The conclusions of the lifting theorem have been verified.

It remains to establish Assertion 1 (i.e., the local delineability of f). Let p be a point of S, and let the degree of $f(p, x_r)$ be l. Then $l \geq 0$ by hypothesis. If $l = 0$ then Assertion 1 follows immediately by the degree-invariance of f in S. Therefore, let us henceforth assume that $l > 0$. Let $\alpha_1 < \cdots < \alpha_k$, $k \geq 0$, be the distinct real roots of $f(p, x_r)$, let $\alpha_{k+1}, \cdots, \alpha_t$, $k \leq t$, be the distinct non-real roots of $f(p, x_r)$, and let m_i be the multiplicity of the root α_i, for $1 \leq i \leq t$. Then $\sum_{i=1}^{t} m_i = l$. Let κ be the minimum separation between the roots of $f(p, x_r)$: that is, $\kappa = \min\{ |\alpha_i - \alpha_j| : 1 \leq i < j \leq t \}$. Let $0 < \epsilon < \frac{\kappa}{2}$, and let C_i be the circle in the complex plane of radius ϵ centred at α_i. By the root continuity principle (Theorem 2.3.2) there is a neighborhood $N_0 \subseteq \mathbb{R}^{r-1}$ of p such that for every $x \in N_0$, each C_i contains exactly m_i roots (multiplicities counted) of $f(x, x_r)$. Consider the following assertion, which implies that if x is sufficiently close to p, *and belongs to* S, then all of the m_i roots of $f(x, x_r)$ inside C_i are coincident:

Assertion 2. For each i, $1 \leq i \leq k$, there is a neighborhood $N_i \subseteq N_0$ of p and an analytic function θ_i from $S \bigcap N_i$ into $(\alpha_i - \epsilon, \alpha_i + \epsilon)$ such that for every $x \in S \bigcap N_i$ and every $\alpha \in (\alpha_i - \epsilon, \alpha_i + \epsilon)$,

$$f(x, \alpha) = 0 \text{ if and only if } \alpha = \theta_i(x), \tag{3.3.1}$$

and such that f is order-invariant in the graph of θ_i.

We say that the above statement asserts the *nonsplitting* of the roots α_i, as x varies within S near p.

We shall now verify Assertion 1 on the strength of Assertion 2. Assume that Assertion 2 holds. Let $N = \bigcap_{i=0}^{k} N_i$, and consider the domain of each θ_i to be $S \bigcap N$. We shall show that the portion of the real variety of f (denoted by $V(f)$) which lies in the cylinder over $S \bigcap N$ is the union of the graphs of the θ_i: that is,

$$V(f) \bigcap Z(S \bigcap N) = \bigcup_{i=1}^{k} \text{graph}(\theta_i), \tag{3.3.2}$$

(where the right-hand side of the equation is understood to be the empty set in case $k = 0$). Let (x,α) be an element of the right-hand side of (3.3.2). Then $x \in S \bigcap N$ and $\alpha = \theta_i(x)$ for some i, $1 \leq i \leq k$. hence, as the range of θ_i is $(\alpha_i - \epsilon, \alpha_i + \epsilon)$, $\alpha \in (\alpha_i - \epsilon, \alpha_i + \epsilon)$. Therefore, by (3.3.1), $f(x,\alpha) = 0$, and so (x,α) is contained in the left-hand side of (3.3.2). Conversely, let (x,α) be an element of $V(f) \bigcap Z(S \bigcap N)$. Then $x \in S \bigcap N$, $\alpha \in \mathbb{R}$, and $f(x,\alpha) = 0$. As f is degree-invariant in S and the degree of $f(p,x_r)$ is l, the degree of $f(x,x_r)$ is also l. As $x \in N_0$, the interior of each C_i, $1 \leq i \leq t$, contains exactly m_i roots (multiplicities counted) of $f(x,x_r)$. Since $\sum_{i=1}^{t} m_i = l$, *every root of* $f(x,x_r)$ *is contained within one of the* C_i. Each C_i with $k+1 \leq i \leq t$ 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 $f(x,x_r)$, α must lie inside a C_i with

$1 \leq i \leq k$. Hence, by (3.3.1), $\alpha = \theta_i(x)$, so (x,α) is contained in the graph of θ_i. We have shown that (3.3.2) holds. This completes our proof of Assertion 1, on the strength of Assertion 2.

It therefore remains to establish Assertion 2 (i.e., the nonsplitting of the roots α_i as x varies within S near p). We now give a point-by-point summary of the steps involved in proving the nonsplitting of the roots.

1. We fix on a particular α_i, and observe that there is no loss of generality in assuming that $\alpha_i = 0$. We are able to dispose quite quickly of the case in which the dimension s of S is equal to $r-1$. In this case, S is just an open subset of $\mathbb{R}^{r-1}$, and so both the discriminant of f and the leading coefficient of f are nonzero in S. Hence, the nonsplitting of the roots is obvious (all roots are simple), and the analytic function θ_i of Assertion 2 is given by the implicit function theorem.

2. There remains the harder case $1 \leq s \leq r-2$. We choose coordinates $(y_1,\ldots,y_{r-1})$ about the point p, such that S is defined locally by the equations $y_{s+1} = 0,\ldots,y_{r-1} = 0$ in the new coordinate system (by Theorem 2.2.1). Let $g(y,y_r)$ denote the function $f(x,x_r)$ transformed into the new coordinates. Then $g(y,y_r)$ is a polynomial in y_r whose coefficients are analytic functions of y, defined near 0 (the analyticity here comes from the analyticity of the coordinate change map). The discriminant $E(y)$ of $g(y,y_r)$ is analytic near 0, and is order-invariant in the linear subspace T defined by $y_{s+1} = 0,\ldots,y_{r-1} = 0$, near 0 (as $D(x)$ is order-invariant in S).

3. Each coefficient of $g(y,y_r)$ can be expanded in a convergent power series

about 0 (by definition of analyticity). Each such power series can be regarded as a *complex* power series in the complex variables $(z_1,...,z_{r-1}) = z$, where $z_j = y_j + iv_j$, say. By the multivariate analogue (Theorem 2.1.2) of a well-known result on convergence, each of these power series is absolutely convergent in a neighborhood of 0 in complex $(r-1)$-space $\mathbb{C}^{r-1}$. In this way, each coefficient of $g(y,y_r)$, and hence also $g(y,y_r)$, can be extended (uniquely) to complex space. We write $g(z,z_r)$ to denote this extension of $g(y,y_r)$: $g(z,z_r)$ is a pseudopolynomial near 0 (see Section 2.1 for definition). We observe that the discriminant $E(z)$ of $g(z,z_r)$ is order-invariant in the complex linear subspace T^* defined by $z_{s+1} = 0,...,z_{r-1} = 0$, near 0.

4. The next step is to focus our attention on the structure of the complex variety $g(z,z_r) = 0$ in a neighborhood of the origin. We use the Weierstrass Preparation Theorem (Theorem 2.1.10) from the theory of several complex variables to do this. This theorem gives us a monic pseudopolynomial $h(z,z_r)$ which has the same locus as $g(z,z_r)$ near the origin. It is shown that the discriminant $F(z)$ of $h(z,z_r)$ is order-invariant in T^*, near 0.

5. We can now apply Zariski's theorem (Theorem 4.1.1) to h. This theorem implies the nonsplitting of the roots of $h(z,z_r)$, as z varies within T^*, near 0. In fact, the theorem yields an analytic function $\psi(z_1,...,z_s)$ defined near 0 which gives the unique distinct root α of $h(z,z_r)$, for $z = (z_1,...,z_s,0,...,0)$ in T^*, sufficiently close to 0. The theorem also assserts order-invariance of h along the locus of this root.

6. All that remains is to retrace our path. The nonsplitting of the roots of

$g(y,y_r)$, as y varies within T near 0, is immediate (as $T \subseteq T^*$). Taking the restriction of ψ to a neighborhood of 0 in real s-space $\mathbb{R}^s$ gives a real-valued analytic function $\eta(y_1,\ldots,y_s)$ which represents the i-th real root of $g(y,y_r)$ for y in T, near 0. Finally, transforming back to the (x,x_r)-variables, we deduce the nonsplitting of the roots of $f(x,x_r)$ as x varies within S, near p. We obtain an analytic function θ_i defined in S near p, which represents the i-th real root of $f(x,x_r)$, for x in S, near p. Order-invariance is preserved under the restriction and detransformation, and thus f is order-invariant in the graph of θ_i.

This concludes our summary of the proof of Assertion 2 (the nonsplitting of the roots).

We now fill in the details of the proof of Assertion 2 outlined above. Assume $k > 0$ (k the number of real roots of $f(p,x_r)$) and let $1 \leq i \leq k$. There is no loss of generality in assuming that $\alpha_i = 0$. (For if $\alpha_i \neq 0$ then we can use a translation of the x_r-coordinate to obtain a polynomial $f'(x,x_r') := f(x,x_r'+\alpha)$ such that (a) $f'(p,x_r')$ has a root of multiplicity m_i at $x_r' = 0$ and no other roots either inside or on the circle C of radius ϵ about 0; and (b) the discriminant of $f'(x,x_r')$ is the same as that of $f(x,x_r)$. Assuming that the required assertion has been proved for $\alpha_i = 0$, we obtain a neighborhood N_i of p and an analytic function $\theta_i' : S \cap N_i \to (-\epsilon, +\epsilon)$ corresponding to f'. We need simply "de-translate" θ_i' to find the desired

$$\theta_i : S \cap N_i \to (\alpha_i - \epsilon, \alpha_i + \epsilon)$$

corresponding to f .) Let $m = m_i$ and $C = C_i$: we seek a neighborhood $N = N_i$ of p and an analytic function $\theta = \theta_i$ satisfying the required properties.

Let us first dispose of the

Case $s = r - 1$.

By definition of submanifold there exists a neighborhood $U \subseteq N_0$ of p such that $U \subseteq S$. Let $f_0(x)$ be the leading coefficient of $f(x, x_r)$, and let $R(x)$ be the resultant of $f(x, x_r)$ and $\frac{\partial f}{\partial x_r}$. Recall that $D(x)$, the discriminant of $f(x, x_r)$, is defined by the equation

$$(-1)^{\frac{m(m-1)}{2}} R(x) = f_0(x) D(x) .$$

As f is degree-invariant and D is order-invariant in S, $f_0 \neq 0$ and $D \neq 0$ in U (since $f_0(x)$ and $D(x)$ are non-zero polynomials). Hence $R \neq 0$ in U and in particular $R(p) \neq 0$. As $f_0(p) \neq 0$, $R(p)$ is equal to the resultant of the univariate polynomials $f(p, x_r)$ and $\frac{\partial f}{\partial x_r}(p, x_r)$. (Although this may seem like a restatement of the definition of resultant, it actually depends crucially on the fact that $f_0(p) \neq 0$. Recall that $R(x)$ is defined to be a certain determinant in the coefficients of $f(x, x_r)$ and $\frac{\partial f}{\partial x_r}$. The only non-zero entries in the first column of this determinant are $f_0(x)$ and $df_0(x)$, where d is the degree of $f(x, x_r)$ (with respect to x_r). Hence if $f_0(q) = 0$ then $R(q) = 0$. However the resultant of the univariate polynomials $f(q, x_r)$ and $\frac{\partial f}{\partial x_r}(q, x_r)$ could be non-zero in spite of $f_0(q) = 0$.) Since $f(p, 0) = 0$, we

must therefore have $\frac{\partial f}{\partial x_r}(p,0) \neq 0$. Hence, by the implicit function theorem (obtained by taking $s = r-1$ in Theorem 2.1.7), there are neighborhoods $N' \subseteq U$ of p and $W \subseteq (-\epsilon, +\epsilon)$ of 0, and an analytic function $\theta : S \bigcap N' = N' \to \mathbb{R}$, such that for all $x \in N'$ and all $\alpha \in W$,

$$f(x,\alpha) = 0 \text{ if and only if } \alpha = \theta(x). \tag{3.3.3}$$

By continuity of θ, N' may be refined to a neighborhood $N \subseteq N'$ of p such that $\theta(N) \subseteq W$. Let $x \in S \bigcap N = N$ and let $\alpha \in (-\epsilon, +\epsilon)$. We shall check that (3.3.1) holds. Assume that $\alpha = \theta(x)$. Then $\alpha \in W$, so by (3.3.3), $f(x,\alpha) = 0$. Assume conversely that $f(x,\alpha) = 0$. Now $m = 1$ as $\frac{\partial f}{\partial x_r}(p,0) \neq 0$. Hence we must have $\alpha = \theta(x)$ (otherwise $f(x,x_r)$ would have at least two distinct roots, α and $\theta(x)$, inside C, contradicting $m = 1$). So (3.3.1) has been verified. Let $x \in N$ and let $\alpha = \theta(x)$. As $m = 1$, $x_r = \alpha$ is a simple root of $f(x,x_r)$. Thus $\frac{\partial f}{\partial x_r}(x,\alpha) \neq 0$, and so $\text{ord}_{(x,\alpha)} f = 1$. Hence f is order-invariant in the graph of θ. Assertion 2 has been established.

There remains the

Case $1 \leq s \leq r-2$.

It will be convenient for us to use a coordinate system about p with respect to which S is locally an s-dimensional linear subspace of $\mathbb{R}^{r-1}$. By Theorem 2.2.1 there exists a neighborhood $U \subseteq N_0$ of p and a coordinate system $\Phi : U \to V$ about p, $\Phi = (\phi_1, \cdots, \phi_{r-1})$, such that

$$S \cap U = \{ x \in U : \phi_{s+1}(x) = 0, \cdots, \phi_{r-1}(x) = 0 \} .$$

By replacing U by the connected component of U containing p we shall henceforth assume that U is connected. Let T be the s-dimensional linear subspace

$$\{ y = (y_1, \ldots, y_{r-1}) \in \mathbb{R}^{n-1} : y_{s+1} = 0, \cdots, y_{r-1} = 0 \}$$

of $\mathbb{R}^{r-1}$. Then the image of $S \cap U$ under Φ is $T \cap V$. Let

$$f(x, x_r) = f_0(x) x_r^d + f_1(x) x_r^{d-1} + \cdots + f_d(x)$$

where $f_0(x) \neq 0$. We shall denote by $g(y, y_r)$ the transform of $f(x, x_r)$ by Φ. That is, if $y \in V$, then $g_j(y) = f_j(\Phi^{-1}(y))$ for $0 \leq j \leq d$, and

$$g(y, y_r) = g_0(y) y_r^d + g_1(y) y_r^{d-1} + \cdots + g_d(y)$$

As the analytic map Φ^{-1} is not in general a polynomial map, $g(y, y_r)$ is not in general a polynomial in y and y_r. However we can regard $g(y, y_r)$ as a polynomial in y_r whose coefficients $g_j(y)$ are analytic functions of y, defined in V (so $g(y, y_r)$ is an instance of the real analogue of the pseudo-polynomials introduced in Sec. 2.1). Note that $y_r = 0$ is a root of multiplicity m of $g(0, y_r)$, that $g(0, \alpha) \neq 0$ for complex α satisfying $0 < |\alpha| \leq \epsilon$, and that, for each fixed $y \in V$, $g(y, y_r)$ has exactly m roots (multiplicities counted) inside C. Let $E(y)$ be the discriminant of $g(y, y_r)$. Then $E(y)$ is an analytic function in V and $E(y) = D(\Phi^{-1}(y))$ for every $y \in V$. Recall that D is order-invariant in S. Hence, by the remark following the definition of order-invariant in Section 3.2, E is order-invariant in $T \cap V$.

We should like to find a box $B = B(0;\delta) \subseteq V$ about 0 in $\mathbb{R}^{r-1}$, where $\delta = (\delta_1, \ldots, \delta_{r-1})$, and an analytic function $\eta(y_1,\ldots,y_{r-1})$ from $B^{(s)} = \{(y_1, \ldots, y_s) \in \mathbb{R}^s : |y_i| < \delta_i, 1 \leq i \leq s\}$ into $(-\epsilon, +\epsilon)$, such that for every $y = (y_1, \ldots, y_s, 0,\ldots,0) \in T \bigcap B$ and every $\alpha \in (-\epsilon, +\epsilon)$,

$$g(y,\alpha) = 0 \text{ if and only if } \alpha = \eta(y_1, \ldots, y_s) \tag{3.3.4}$$

and such that g is order-invariant in the set

$$G = \{(y,y_r) \in \mathbb{R}^n : y = (y_1, \ldots, y_s, 0,\ldots,0) \in T \bigcap B \text{ and } y_r = \eta(y_1, \ldots, y_s)\} \tag{3.3.5}$$

(Note that as $B^{(s)} \equiv T \bigcap B$ we can think of η as a map from $T \bigcap B$ into $(-\epsilon, +\epsilon)$, and the set G as the graph of η.) We shall make an excursion into the complex domain from which we shall return with the box B and the function η. Upon detransforming B and η via Φ we shall have our desired N and θ.

Choose $\rho = (\rho_1, \ldots, \rho_{n-1}) \in V$, with $\rho_i > 0$ for all i, such that $B_1 := B(0;\rho) \subseteq V$ and the power series expansion about 0 of every g_j is absolutely convergent at $y = \rho$. By Theorem 2.1.2, the power series expansion about 0 of every g_j, considered as a *complex* power series in the complex variables $z_1,\ldots,z_{r-1}$, is absolutely convergent in the polydisc $\Delta_1 := \Delta(0;\rho) \subseteq \mathbb{C}^{r-1}$ and the sum of the series, $g_j(z) = g_j(z_1, \ldots, z_{r-1})$, is holomorphic in Δ_1. For $z \in \Delta_1$, set

$$g(z,z_r) = g_0(z)z_r^d + g_1(z)z_r^{d-1} + \cdots + g_d(z)$$

(so $g(z,z_r)$ is a pseudopolynomial in Δ_1) and let $E(z)$ be the discriminant of $g(z,z_r)$. Let

$$\sum_{i_1, \ldots, i_{r-1} \geq 0}^{\infty} a_{i_1, \ldots, i_{r-1}} y_1^{i_1} \cdots y_{r-1}^{i_{r-1}} \tag{3.3.6}$$

be the power series expansion for $E(y)$ about 0. Then the power series expansion for $E(z)$ about 0, which is absolutely convergent in Δ_1, is obtained by substituting $z_1, \ldots, z_{r-1}$ for $y_1, \ldots, y_{r-1}$ in (3.3.6).

Let T^* be the s-dimensional linear subspace

$$\{ z = (z_1, \ldots, z_{r-1}) \in \mathbb{C}^{r-1} : z_{s+1} = 0, \cdots, z_{r-1} = 0 \}$$

of $\mathbb{C}^{r-1}$ (note that s is the dimension of T^* considered as a complex subspace of the complex vector space $\mathbb{C}^{r-1}$). We claim that, after refining Δ_1 suitably, we can assume that $E(z)$ is order-invariant in $T^* \bigcap \Delta_1$. We prove this claim now. Let $\mathrm{ord}_0 E = \mu$. Then every partial derivative of $E(z)$ of order less than μ vanishes at 0. Let

$$P(z) = \frac{\partial^{i_1 + \ldots + i_{r-1}} E}{\partial z_1^{i_1} \cdots \partial z_{r-1}^{i_{r-1}}}$$

be a partial derivative of $E(z)$ of order $\sum_{j=1}^{r-1} i_j < \mu$. By Theorem 2.1.2, $P(z)$ is holomorphic in Δ_1 and its power series expansion about 0, which is absolutely convergent in Δ_1, is obtained by differentiating (3.3.6) (with the y_i's replaced by z_i's) term-by-term. Let

$$Q(y) = \frac{\partial^{i_1 + \ldots + i_{r-1}} E}{\partial y_1^{i_1} \cdots \partial y_{r-1}^{i_{r-1}}} \quad .$$

By Theorem 2.1.2, $Q(y)$ is analytic in B_1 and its power series expansion about 0, which is absolutely convergent in B_1, is obtained by differentiating (3.3.6) term-by-term. Hence the power series for $P(z)$ can be obtained by substituting $z_1, \ldots, z_{r-1}$ for $y_1, \ldots, y_{r-1}$ in the power series for $Q(y)$. Recall that $E(y)$ is order-invariant in $T \bigcap V$. Hence, as $\mathrm{ord}_0 E = \mu$, $Q(y)$

vanishes throughout $T \bigcap B_1$. It follows that substituting $y_{s+1}=0, \cdots, y_{r-1}=0$ in the power series for $Q(y)$ yields the zero power series in $y_1, \ldots, y_s$. Hence substituting $z_{s+1}=0, \cdots, z_{r-1}=0$ in the power series for $P(z)$ yields the zero power series in $z_1, \ldots, z_s$. It follows that $P(z)$ vanishes throughout $T^* \bigcap \Delta_1$. We have shown that every partial derivative of $E(z)$ of order less than μ vanishes throughout $T^* \bigcap \Delta_1$. As $\mathrm{ord}_0 E = \mu$, some partial derivative of $E(z)$ of order μ, say $R(z)$, does not vanish at 0. Let $\Delta_2 \subseteq \Delta_1$ be a polydisc about 0 in which $R \neq 0$. Then $\mathrm{ord}_z E = \mu$ for every $z \in T^* \bigcap \Delta_2$, so $E(z)$ is order-invariant in $T^* \bigcap \Delta_2$. Replacing Δ_1 by Δ_2 we may assume that $E(z)$ is order-invariant in $T^* \bigcap \Delta_1$.

We wish to study the structure of the zero set of $g(z, z_r)$ near the origin. An application of the Weierstrass preparation theorem will facilitate this study. Recall that $g(z, z_r)$ is holomorphic in the polydisc $\Delta_1 \times \Delta(0;\epsilon)$, that $z_r = 0$ is a root of $g(0, z_r)$ of multiplicity m, and that $g(0, z_r) \neq 0$ for $0 < |z_r| \leq \epsilon$. By the Weierstrass preparation theorem (Theorem 2.1.10), there is a polydisc $\Delta_2 \subseteq \Delta_1$, a function $u(z, z_r)$ holomorphic and non-vanishing in $\Delta' := \Delta_2 \times \Delta(0;\epsilon)$, and a Weierstrass polynomial

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

in Δ_2, such that

$$g(z, z_r) = u(z, z_r) h(z, z_r) \tag{3.3.7}$$

for all $(z, z_r) \in \Delta'$, and such that for each fixed $z \in \Delta_2$, all the m roots of $h(z, z_r)$ are contained in the disc $\Delta(0;\epsilon)$. By (3.3.7), as $u \neq 0$ in Δ', the zero set of $g(z, z_r)$ is the same as that of $h(z, z_r)$, in Δ'.

We claim that $u(z,z_r)$ is in fact a pseudopolynomial in Δ_2. We prove this claim now. Let z be a fixed point of Δ_2. Let $z_r = \xi$ be a root of $h(z,z_r)$. Then $\xi \in \Delta(0;\epsilon)$. Hence, as (3.3.7) holds near $z_r = \xi$ in the z_r-plane, and as $u(z,z_r) \neq 0$ near $z_r = \xi$, $g(z,\xi) = 0$ and the multiplicity of the zero ξ of $h(z,z_r)$ is equal to the multiplicity of the zero ξ of $g(z,z_r)$. We have shown that every root of $h(z,z_r)$ is a root of $g(z,z_r)$, and moreover has the same multiplicity in $g(z,z_r)$ as it has in $h(z,z_r)$. Thus $h(z,z_r) \mid g(z,z_r)$ in $\mathbb{C}[z_r]$ and the quotient of $g(z,z_r)$ by $h(z,z_r)$ is clearly equal to $u(z,z_r)$. Let l be the degree of $g(z,z_r)$. Then $m \leq l \leq d$, and the degree of $u(z,z_r)$ is $l-m$. Let us write

$$u(z,z_r) = u_0(z)z_r^{d-m} + u_1(z)z_r^{d-m-1} + \cdots + u_{d-m}(z),$$

where $u_0(z) = \cdots = u_{d-l-1}(z) = 0$, and $u_{d-l}(z) \neq 0$. Letting z now be a variable point of Δ_2, the coefficients $u_j(z)$ of $u(z,z_r)$ can be regarded as functions defined in Δ_2. That these functions are in fact holomorphic in Δ_2 is seen by equating coefficients in (3.3.7). We have established our claim that $u(z,z_r)$ is a pseudopolynomial in Δ_2.

Let $F(z)$ be the discriminant of $h(z,z_r)$. We shall find a function $Q(z)$ holomorphic in Δ_2 such that

$$E(z) = Q(z)F(z) \tag{3.3.8}$$

for all z in Δ_2. If $d > m$ in which case $u(z,z_r)$ has positive degree in z_r then set

$$Q(z) = G(z)(R(z))^2$$

where $G(z)$ is the discriminant of $u(z,z_r)$ and $R(z)$ is the resultant of

$u(z,z_r)$ and $h(z,z_r)$. Equation (3.3.8) holds by Theorem 2.3.3. If $d=m$ in which case $u(z,z_r)$ has degree zero in z_r then set

$$Q(z) = (u_0(z))^{2m-2}.$$

Equation (3.3.8) holds by Equation (2.3.6).

By Lemma 3.2.2, $F(z)$ is order-invariant in $T^* \bigcap \Delta_2$. Hence, by Zariski's 1975 theorem (Theorem 4.1.1), there exists a polydisc $\Delta_3 \subseteq \Delta_2$ about 0, and a holomorphic function $\psi(z_1, \ldots, z_s)$ from $\Delta_3^{(s)}$ into $\Delta(0;\epsilon)$ such that for all $z=(z_1, \ldots, z_s, 0, \ldots, 0) \in T^* \bigcap \Delta_3$ and all $\alpha \in \Delta(0;\epsilon)$,

$$h(z,\alpha) = 0 \text{ if and only if } \alpha = \psi(z_1, \ldots, z_s) \tag{3.3.9}$$

and such that h is order-invariant in the set

$$G^* = \{(z,z_r) \in \mathbb{C}^n : z=(z_1, \ldots, z_s, 0, \ldots, 0) \in T^* \bigcap \Delta_3 \text{ and } z_r = \psi(z_1, \ldots, z_s)\}.$$

As remarked following the statement of Zariski's theorem in Sec. 4.1, $\Delta_3^{(s)}$ can be identified with $T^* \bigcap \Delta_3$, and ψ regarded as a map from $T^* \bigcap \Delta_3$ into $\Delta(0;\epsilon)$, with graph G^*.

Let the power series expansion for $\psi(z_1, \ldots, z_s)$ about 0 be absolutely convergent at the point $(z_1, \ldots, z_s) = (\delta_1, \ldots, \delta_s)$ of $\Delta_3^{(s)}$, where $\delta_i > 0$ for each i. Choose $\delta_{s+1}, \ldots, \delta_{r-1} > 0$ so that, if $\delta = (\delta_1, \ldots, \delta_s, \delta_{s+1}, \ldots, \delta_{r-1})$, then the polydisc $\Delta_4 := \Delta(0;\delta)$ in $\mathbb{C}^{r-1}$ is contained in Δ_3. Let $B = B(0;\delta)$ in $\mathbb{R}^{r-1}$ and let η be the restriction of ψ to $B^{(s)}$. Then $B \subseteq V$ and we claim that η is a real-valued analytic function, that for every $y=(y_1, \ldots, y_s, 0, \ldots, 0) \in T \bigcap B$ and every $\alpha \in (-\epsilon, +\epsilon)$ (3.3.4) holds, and that $g(y,y_r)$ is order-invariant in "the graph of η" (i.e., strictly speaking, in the set G defined by (3.3.5)). We prove these claims

now. Let $(y_1, \ldots, y_s) \in B^{(s)}$ and let $y = (y_1, \ldots, y_s, 0, \ldots, 0)$ be the corresponding element of $T \bigcap B$. By (3.3.9), $\alpha := \psi(y_1, \ldots, y_s)$ is a root of $h(y, y_r)$ inside $\Delta(0;\epsilon)$. Hence, by (3.3.7), α is a root of $g(y, y_r)$ inside $\Delta(0;\epsilon)$. But $g(y, y_r)$ is a *real* polynomial in y_r. Hence $\bar{\alpha}$ is a root of $g(y, y_r)$ inside $\Delta(0;\epsilon)$, and so by (3.3.7), $h(y, \bar{\alpha}) = 0$. But (3.3.9) implies that $\alpha = \bar{\alpha}$, and hence α is a real number. Thus η is a real-valued function, and $\eta : B^{(s)} \to (-\epsilon, +\epsilon)$. Let

$$\sum_{j \geq 0} d_j z_1^{j_1} \cdots z_s^{j_s} \quad , \tag{3.3.10}$$

where j denotes the multi-index $(j_1, \ldots, j_s)$, be the power series expansion for $\psi(z_1, \ldots, z_s)$ about 0. Then (3.3.10) is absolutely convergent in $\Delta_4^{(s)}$, by Theorem 2.1.2. Let $d_j = b_j + ic_j$, where b_j and c_j are real numbers, for each multi-index j. By Theorem 48 of Chap. 6, [KAP52],

$$\psi(\delta_1, \ldots, \delta_s) = \sum_{j \geq 0} b_j \delta_1^{j_1} \cdots \delta_s^{j_s} + i\left(\sum_{j \geq 0} c_j \delta_1^{j_1} \cdots \delta_s^{j_s}\right) ,$$

where both the real and imaginary parts of the right-hand side are absolutely convergent. By Theorem 2.1.2, each of the series

$$\sum_{j \geq 0} b_j y_1^{j_1} \ldots y_s^{j_s} \quad , \quad \sum_{j \geq 0} c_j y_1^{j_1} \ldots y_s^{j_s}$$

is absolutely convergent in $B^{(s)}$, and the sum of each series is an analytic function in $B^{(s)}$. But for $(y_1, \ldots, y_s) \in B^{(s)}$,

$$\begin{aligned} \eta(y_1, \ldots, y_s) = \psi(y_1, \ldots, y_s) &= \sum_{j \geq 0} d_j y_1^{j_1} \ldots y_s^{j_s} \\ &= \sum_{j \geq 0} b_j y_1^{j_1} \ldots y_s^{j_s} + i\left(\sum_{j \geq 0} c_j y_1^{j_1} \ldots y_s^{j_s}\right) \\ &= \sum_{j \geq 0} b_j y_1^{j_1} \ldots y_s^{j_s} \quad , \text{ as } \eta \text{ is real-valued.} \end{aligned}$$

Hence η is analytic in $B^{(s)}$. It is straightforward to verify the remaining claims about η.

Finally, set $N = \Phi^{-1}(B)$ and define $\theta : S \bigcap N \to (-\epsilon, +\epsilon)$ by $\theta(x) = (\eta_0\phi)(x)$, where $\phi : S \bigcap N \to B^{(s)}$ is the chart for S corresponding to Φ. As $\theta_0\phi^{-1} = \eta$ is analytic in $B^{(s)}$, θ is analytic in $S \bigcap N$. Clearly (3.3.1) holds for every $x \in S \bigcap N$ and every $\alpha \in (-\epsilon, +\epsilon)$, and the order-invariance of f in the graph of θ follows from that of g in the graph of η, by the remark following the definition of order-invariance in Section 3.2. This completes the proof of Assertion 2 and hence of the lifting theorem. □

Chapter Four

The Zariski Theorem

This chapter presents an exposition of Zariski's 1975 theorem on equisingularity over the complex field [ZAR75]. Our presentation of this result is self-contained and in many respects quite different from Zariski's. Our basic tools are analytic functions of several complex variables, and elementary topology (covering spaces in particular). Puiseux series (or fractional power series) enter into one aspect of the argument.

The proof is divided into two cases: the codimension one case, and the remaining case. The codimension one case was established by Zariski in 1965 [ZAR65] (the essential ideas were known earlier [ZAR35]). Section 2 contains an exposition of this result. The remaining case is proved by reduction to the codimension one case. This reduction is the essential content of [ZAR75]. Section 1 provides our version of the reduction.

Throughout this chapter we shall denote the $(n-1)$-tuple $(z_1,...,z_{n-1})$ by z.

4.1. The general theorem

The following theorem is an adaptation of a result published by Zariski in 1975 [ZAR75]:

Theorem 4.1.1. Let $h(z,z_n)$ be a Weierstrass polynomial of positive degree in the polydisc Δ_1 about 0 in $\mathbb{C}^{n-1}$, and assume that for every fixed z in Δ_1, all the roots of $h(z,z_n)$ are contained in the disc $\Delta(0;\epsilon)$ about 0 in $\mathbb{C}$. Let $F(z)$ be the discriminant of $h(z,z_n)$ and assume that $F(z)$ does not vanish identically. Let $1 \leq s \leq n-2$, let

$$T^* = \{ z = (z_1,\ldots,z_{n-1}) \in \mathbb{C}^{n-1} : z_{s+1} = 0,\ldots,z_{n-1} = 0 \},$$

and assume that F is order-invariant in $T^* \cap \Delta_1$. Then there exists a polydisc $\Delta_2 \subseteq \Delta_1$ about 0, and a holomorphic function $\psi(z_1,\ldots,z_s)$ from $\Delta_2^{(s)}$ into $\Delta(0;\epsilon)$, such that for all $z = (z_1,\ldots,z_s,0,\ldots,0)$ in $T^* \cap \Delta_2$ and all α in $\Delta(0;\epsilon)$,

$$h(z,\alpha) = 0 \text{ if and only if } \alpha = \psi(z_1,\ldots,z_s),$$

and such that h is order-invariant in the set

$$G^* = \{ (z,z_n) \in \mathbb{C}^{n-1} \times \mathbb{C} : z = (z_1,\ldots,z_s,0,\ldots,0) \in T^* \cap \Delta_2 \ \&\ z_n = \psi(z_1,\ldots,z_s) \}.$$

Remark 1. As $\Delta_2^{(s)}$ can be identified with $T^* \cap \Delta_2$ under the mapping $\iota(z_1,\ldots,z_s) = (z_1,\ldots,z_s,0,\ldots,0)$, we can think of ψ as a map from $T^* \cap \Delta_2$ into $\Delta(0;\epsilon)$, and the set G^* as the graph of ψ.

Remark 2. Zariski's theorem itself actually allows in place of the particular s-dimensional linear subspace T^* of $\mathbb{C}^{n-1}$ an arbitrary s-dimensional submanifold S^* of $\mathbb{C}^{n-1}$ (containing 0). We shall not need to formulate this slightly more general theorem here, however.

Proof of 4.1.1. Our proof of the theorem is given in numbered stages.

1. Let $\operatorname{ord}_0 F = r$. We may assume without loss of generality that $\frac{\partial^r F}{\partial z_{n-1}^r}(0) \neq 0$. (If this is not the case then we can find an invertible linear

transformation L of $\mathbb{C}^{n-1}$ fixing $T*$ pointwise such that if $\overline{F} := F_o L^{-1}$ is the transform of F by L then $\dfrac{\partial^r \overline{F}}{\partial z_{n-1}^r}(0) \neq 0$.)

2. For the remainder of this section we shall denote the s-tuple of variables $(v_1,\ldots,v_s)$ by $\mathbf{v}$. Let the power series expansion for $F(z)$ about 0 be

$$\sum_{i_1,\ldots,i_{n-1}\geq 0} f_{i_1,\ldots,i_{n-1}} z_1^{i_1} \cdots z_{n-1}^{i_{n-1}} \tag{4.1.1}$$

Then $f_{i_1,\ldots,i_{n-1}} = 0$ for all $(i_1,\ldots,i_{n-1})$ with $\sum_{j=1}^{n-1} i_j < r$, and $f_{0,\ldots,0,r} \neq 0$ (by (1)). The series is absolutely convergent in Δ_1.

3. The series (4.1.1) can be arranged as an iterated series thus:

$$\sum_{i_{s+1},\ldots,i_{n-1}\geq 0} \Big(\sum_{i\geq 0} f_{i,i_{s+1},\ldots,i_{n-1}} z_1^{i_1} \cdots z_s^{i_s}\Big) z_{s+1}^{i_{s+1}} \cdots z_{n-1}^{i_{n-1}}. \tag{4.1.2}$$

For each fixed $i_{s+1},\ldots,i_{n-1} \geq 0$, the inner series in (4.1.2) is absolutely convergent in $\Delta_1{}^{(s)}$. Let $p_{i_{s+1},\ldots,i_{n-1}}(\mathbf{z})$ denote the sum of this inner series. Let $\delta = (\delta,\delta_{s+1},\ldots,\delta_{n-1})$ be the polyradius of Δ_1. Then the outer series

$$\sum_{i_{s+1},\ldots,i_{n-1}\geq 0} p_{i_{s+1},\ldots,i_{n-1}}(\mathbf{z}) z_{s+1}^{i_{s+1}} \cdots z_{n-1}^{i_{n-1}} \tag{4.1.3}$$

is absolutely convergent in the polydisc $|z_{s+1}| < \delta_{s+1}, \ldots, |z_{n-1}| < \delta_{n-1}$.

4. For $\mathbf{z} \in \Delta_1{}^{(s)}$ and $k \geq 0$, let

$$P_k(\mathbf{z},z_{s+1},\ldots,z_{n-1}) = \sum_{i_{s+1}+\ldots+i_{n-1}=k} p_{i_{s+1},\ldots,i_{n-1}}(\mathbf{z}) z_{s+1}^{i_{s+1}} \cdots z_{n-1}^{i_{n-1}}.$$

Then $P_0 \equiv \cdots \equiv P_{r-1} \equiv 0$, by order-invariance of F in $T* \bigcap \Delta_1$. Hence,

for each fixed $z \in \Delta_1^{(s)}$, and for $|z_{s+1}| < \delta_{s+1}, \ldots, |z_{n-1}| < \delta_{n-1}$,

$$F(z,z_{s+1},\ldots,z_{n-1}) = P_r(z,z_{s+1},\ldots,z_{n-1}) + P_{r+1}(z,z_{s+1},\ldots,z_{n-1}) + \cdots$$

(grouping terms in the series (4.1.3)).

5. *Case I*: $s = n-2$.

We have

$$F(z,z_{n-1}) = p_r(z)z_{n-1}^r + p_{r+1}(z)z_{n-1}^{r+1} + \cdots.$$

Hence $F(z,z_{n-1}) = z_{n-1}^r N(z,z_{n-1})$, where

$$N(z,z_{n-1}) = p_r(z) + p_{r+1}(z)z_{n-1} + \cdots,$$

for $(z,z_{n-1}) \in \Delta_1$. It can be shown that N is holomorphic. Now $N(0,0) = p_r(0) = f_{0,r} \neq 0$ (from (2)). Hence, there exists $\Delta_2 \subseteq \Delta_1$ such that $N \neq 0$ in Δ_2. We can therefore apply Theorem 4.2.1 to obtain the required function ψ.

6. Case II: $1 \leq s \leq n-2$.

Our essential strategy is to reduce Case II to Case I. We use a quadratic transformation (or "blowing-up map") to bring about the reduction to the codimension 1 case. Define the map $Q : \mathbb{C}^{n-1} \to \mathbb{C}^{n-1}$ by

$$Q(Z,Z_{s+1},\ldots,Z_{n-1}) = (Z,Z_{s+1}Z_{n-1},\ldots,Z_{n-2}Z_{n-1},Z_{n-1}).$$

Q is called a *quadratic transformation*, as each of its components has degree at most two, and some component has degree exactly two. Q maps the entire hyperplane $H^*: Z_{n-1} = 0$ to the s-dimensional linear subspace T^* of $\mathbb{C}^{n-1}$. Even though strictly speaking Q^{-1} does not exist, one can think of a "map" Q^{-1} which sends a point $z = (z,z_{s+1},\ldots,z_{n-1})$, with $z_{n-1} \neq 0$, to the point

$$Z = (z, \frac{z_{s+1}}{z_{n-1}}, \ldots, \frac{z_{n-2}}{z_{n-1}}, z_{n-1})$$

(for which $Q(Z) = z$), and which sends a point $z \in T^*$ to the *set* of points $Z \in \mathbb{C}^{n-1}$ for which $Q(Z) = z$. Points in $\{z_{n-1} = 0\} - T^*$ would have no image under Q^{-1}, however. We say that T^* is *blown-up* by Q^{-1} to H^*, and call Q^{-1} a *blowing-up map*.

Where $\delta_i' = \delta_i$ for $1 \leq i \leq s$ and $i = n-1$, and $\delta_i' = \frac{\delta_i}{\delta_{n-1}}$ for $s+1 \leq i \leq n-2$, and $\delta' = (\delta_1', \ldots, \delta_{n-1}')$, let $\Delta_1' = \Delta(0;\delta')$. We have that $Q(\Delta_1') \subseteq \Delta_1$. Hence if we set $h'(Z, Z_n) = h(Q(Z), Z_n)$ for $Z \in \Delta_1'$, then h' is a Weierstrass polynomial in Δ_1'. Let $F'(Z)$ be the discriminant of $h'(Z, Z_n)$.

7. Case II (continued).

We show that F' satisfies the hypotheses of Theorem 4.2.1 (and equivalently that F' is order-invariant in H^*, near 0). Let $Z = (Z, Z_{s+1}, \ldots, Z_{n-1})$ be an element of Δ_1', and let

$$N(Z) = P_r(Z, Z_{s+1}, \ldots, Z_{n-2}, 1) + Z_{n-1} P_{r+1}(Z, Z_{s+1}, \ldots, Z_{n-2}, 1) + \cdots .$$

Then

$$\begin{aligned} F'(Z) = F(Q(Z)) &= F(Z, Z_{s+1}Z_{n-1}, \ldots, Z_{n-2}Z_{n-1}, Z_{n-1}) \\ &= P_r(Z, Z_{s+1}Z_{n-1}, \ldots, Z_{n-2}Z_{n-1}, Z_{n-1}) \\ &\quad + P_{r+1}(Z, Z_{s+1}Z_{n-1}, \ldots, Z_{n-2}Z_{n-1}, Z_{n-1}) + \cdots \\ &= Z_{n-1}^r N(Z), \end{aligned}$$

as

$$P_k(Z, Z_{s+1}Z_{n-1}, \ldots, Z_{n-2}Z_{n-1}, Z_{n-1}) = Z_{n-1}^k P_k(Z, Z_{s+1}, \ldots, Z_{n-1}, 1).$$

It can be shown that N is holomorphic; further, we have

$N(0) = P_r(0,0,...,0,1) = p_{0,...,0,r}(0) = f_{0,...,0,r} \neq 0$, by (2).

Hence there exists $\Delta_2' \subseteq \Delta_1'$ such that $N \neq 0$ in Δ_2'.

8. Case II (conclusion).

By Theorem 4.2.1, there exists a polydisc Δ_3' contained in Δ_2' and a holomorphic function $\psi'(Z_1,...,Z_{n-2})$ from $\Delta_3'^{(n-2)}$ into $\Delta(0;\epsilon)$ such that for all $Z = (Z_1,...,Z_{n-2},0)$ in $H^* \bigcap \Delta_3'$ and all Z_n in $\Delta(0;\epsilon)$,

$$h'(Z,Z_n) = 0 \text{ if and only if } Z_n = \psi'(Z_1,...,Z_{n-2})$$

and such that h' is order-invariant in the set

$$K^* = \{(Z,Z_n) \in \mathbb{C}^n : Z = (Z_1,...,Z_{n-2},0) \in H^* \bigcap \Delta_3' \text{ and } Z_n = \psi'(Z_1,...,Z_{n-2})\}.$$

Let ν' be the polyradius of Δ_3', let $\nu = Q(\nu')$, and let $\Delta_3 = \Delta(0;\nu)$. Define $\psi : \Delta_3^{(s)} \to \Delta(0;\epsilon)$ by $\psi(z) = \psi'(z,0,...,0)$. We shall show that ψ satisfies the properties asserted of it in the conclusion of Theorem 4.1.1.

It is clearly the case that for all $z = (z,0,...,0)$ in $T^* \bigcap \Delta_3$ and all z_n in $\Delta(0;\epsilon)$,

$$h(z,z_n) = 0 \text{ if and only if } z_n = \psi(z).$$

It remains to show that h is order-invariant in the set G^* defined in the statement of the theorem (with 'Δ_2' replaced by 'Δ_3').

Let $(w,w_n) \in G^*$ and let $t = \text{ord}_{(w,w_n)} h$. We shall prove that $t = \text{ord}_{(w,w_n)} h'$. The order-invariance of h in G^* will then follow by the order-invariance of h' in K^*. We have $t \leq \text{ord}_{(w,w_n)} h'$, by Theorem 2.3.2. We shall prove that there exists a point $(w',w_n) \in K^*$, with $w' = (w,w_{s+1}', \ldots, w_{n-2}',0)$ an element of $H^* \bigcap \Delta_3'$, such that

$t \geq \mathrm{ord}_{(w',w_n)} h'$. This will show, by order-invariance of h' in $K*$, that $t \geq \mathrm{ord}_{(w,w_n)} h'$.

Now w is an element of $T* \bigcap \Delta_3$, and so $w = (\mathbf{w},0,\ldots,0)$, where $\mathbf{w} \in \Delta_3^{(s)}$. As $\mathrm{ord}_{(w,w_n)} h = t$, there is a term

$$c(z_1-w_1)^{e_1} \cdots (z_s-w_s)^{e_s} z_{s+1}^{e_{s+1}} \cdots z_{n-1}^{e_{n-1}} (z_n-w_n)^{e_n} ,$$

with $\sum_{j=1}^{n} e_j = t$ and $c \neq 0$, in the power series expansion of h about (w,w_n). This term gives rise to the non-zero term

$$c(Z_1-w_1)^{e_1} \cdots (Z_s-w_s)^{e_s} Z_{s+1}^{e_{s+1}} \cdots Z_{n-2}^{e_{n-2}} Z_{n-1}^{m} (Z_n-w_n)^{e_n}$$

where $m = \sum_{j=s+1}^{n-1} e_j$, in the power series expansion of h' about (w,w_n) (since $h'(Z,Z_n) = h(Q(Z),Z_n)$).

Let the power series expansion of h' about (w,w_n) be arranged as an iterated series thus:

$$\sum_{i,i_{n-1},i_n \geq 0} q_{i,i_{n-1},i_n}(Z_{s+1},\ldots,Z_{n-2}) \cdot (Z_1-w_1)^{i_1} \cdots (Z_s-w_s)^{i_s} Z_{n-1}^{i_{n-1}} (Z_n-w_n)^{i_n}$$

(cf. stage 3 of the proof of Theorem 4.1.1). Now q_{e,m,e_n} is not identically zero, as it contains the non-zero term $cZ_{s+1}^{e_{s+1}} \cdots Z_{n-2}^{e_{n-2}}$. Hence, there exist $w_{s+1}', \ldots, w_{n-2}'$, with $w' := (\mathbf{w},w_{s+1}', \ldots, w_{n-2}',0)$ an element of $H* \bigcap \Delta_3'$, such that

$$q := q_{e,m,e_n}(w_{s+1}', \ldots, w_{n-2}')$$

is non-zero.

Now the power series expansion of h' about (w',w_n) contains the term

$$q(Z_1-w_1)^{e_1}\cdots(Z_s-w_s)^{e_s}(Z_{s+1}-w_{s+1})^0\cdots(Z_{n-2}-w_{n-2})^0 Z_{n-1}^m (Z_n-w_n)^{e_n} .$$

Hence, as $q \neq 0$ and the total degree of this term is

$$e_1+\cdots+e_s+m+e_n = t ,$$

we have $t \geq \mathrm{ord}_{(w',w_n)}h'$. Hence, by the order-invariance of h' in K^*, we have $t \geq \mathrm{ord}_{(w,w_n)}h'$.

We have now shown that $t = \mathrm{ord}_{(w,w_n)}h'$. The order-invariance of h in G^* now follows by the order-invariance of h' in K^*. □

4.2. Special Case (codimension one)

We present in this section a theorem established by Zariski in 1965 [ZAR65]. This theorem is essentially the special case $s = n-2$ of Theorem 4.1.1. Our formulation of the result is adapted to our needs and is somewhat different from Zariski's formulation. Our proof is also different from the one Zariski gave. Throughout this section we shall adopt the notational convention that $\mathbf{z} = (z_1,\ldots,z_{n-2})$: thus $z = (\mathbf{z},z_{n-1})$. Let H^* be the hyperplane $\{ z = (\mathbf{z},z_{n-1}) \in \mathbb{C}^{n-1} : z_{n-1} = 0 \}$ in $\mathbb{C}^{n-1}$. The theorem can be stated as follows:

Theorem 4.2.1 (*Zariski*) : Let $n \geq 3$ and let $h(z,z_n)$ be a Weierstrass polynomial of positive degree in the polydisc Δ_1 about 0 in $\mathbb{C}^{n-1}$, and assume that for every fixed z in Δ_1, all the roots of $h(z,z_n)$ are contained in the disc $\Delta(0;\epsilon)$ about 0 in $\mathbb{C}$. Let $F(z)$ be the discriminant of $h(z,z_n)$ and suppose that there exists a function $N(z)$, holomorphic and non-vanishing in Δ_1, and

an integer $r \geq 0$, such that

$$F(z) = z_{n-1}^{r} N(z)$$

for all $z = (z,z_{n-1})$ in Δ_1. Then there exists a polydisc $\Delta_2 \subseteq \Delta_1$ about 0, and a holomorphic function $\psi(z)$ from $\Delta_2^{(n-2)}$ into $\Delta(0;\epsilon)$, such that for every fixed $z = (z,0)$ in $H^* \bigcap \Delta_2$ and every z_n in $\Delta(0;\epsilon)$,

$$h(z,z_n) = 0 \text{ if and only if } z_n = \psi(z),$$

and such that h is order-invariant in the set

$$G^* = \{ (z,0,z_n) \in \mathbb{C}^n : z \in \Delta_2^{(n-2)} \text{ and } z_n = \psi(z) \}. \qquad (4.2.1)$$

Note that the hypotheses on $F(z)$ that it be associated to the function z_{n-1}^{r} is essentially equivalent to the hypothesis that $F(z)$ be order-invariant in H^*, near the origin. Thus the above theorem is essentially the special case $s = n-2$ of Theorem 4.1.1: that is, the case in which the linear subspace T^* of $\mathbb{C}^{n-1}$ has codimension one.

This result of Zariski is equivalent to the following two theorems taken together. The first theorem (4.2.2) asserts the "nonsplitting" of the locus G^* of h over H^*, and the second (4.2.3) asserts the order- invariance of h in G^*.

Theorem 4.2.2 : Let $h(z,z_n)$ be a Weiersrass polynomial of positive degree in the polydisc Δ_1 about 0 in $\mathbb{C}^{n-1}$, and assume that h satisfies the hypotheses of Theorem 4.2.1. (In particular, assume that for every fixed z in Δ_1, all the roots of $h(z,z_n)$ are contained in the disc $\Delta(0;\epsilon)$ in $\mathbb{C}$.) Then there exists a holomorphic function $\psi(z)$ from $\Delta_1^{(n-2)}$ into $\Delta(0;\epsilon)$ such that for

every fixed $z = (\mathbf{z},0) \in H^* \bigcap \Delta_1$ and every $z_n \in \Delta(0;\epsilon)$,

$$h(z,z_n) = 0 \text{ if and only if } z_n = \psi(\mathbf{z}).$$

Theorem 4.2.3 : Let $h(z,z_n)$ be a Weierstrass polynomial of degree $m \geq 1$ in the polydisc Δ_1 about 0 in $\mathbb{C}^{n-1}$, and assume that h satisfies the hypotheses of Theorem 4.2.1. Assume further that $h(\mathbf{z},0,z_n) = z_n^m$ for all $\mathbf{z} \in \Delta_1^{(n-2)}$.Then there exists a polydisc $\Delta_2 \subseteq \Delta_1$ about 0 such that h is order-invariant in the set $\Delta_2^{(n-2)} \times \{ (0,0) \}$.

Proof that 4.2.1 <=> (4.2.2 & 4.2.3) : Clearly 4.2.1 implies 4.2.2 and 4.2.3. Assume conversely that 4.2.2 and 4.2.3 hold. Let $h(z,z_n)$ be a Weierstrass polynomial of degree $m \geq 1$ in the polydisc Δ_1 about 0 in $\mathbb{C}^{n-1}$, and assume that h satisfies the hypotheses of Theorem 4.2.1. Theorem 4.2.2 gives us the required function ψ, defined in $\Delta_1^{(n-2)}$. It remains to establish that there is a polydisc $\Delta_2 \subseteq \Delta_1$ about 0 such that h is order-invariant in the set G^* defined by equation (4.2.1). For $z = (\mathbf{z},z_{n-1}) \in \Delta_1$, let $h'(z,z_n) = h(z,z_n + \psi(\mathbf{z}))$. Then $h'(z,z_n)$ is a Weierstrass polynomial in Δ_1 and $h'(\mathbf{z},0,z_n) = z_n^m$ for $\mathbf{z} \in \Delta_1^{(n-2)}$. Moreover, by root continuity, there exists a polydisc $\Delta_1' \subseteq \Delta_1$ about 0 such that for every fixed $z \in \Delta_1'$, all the roots of $h'(z,z_n)$ are contained in $\Delta(0;\epsilon)$. Hence, by Theorem 4.2.3, there exists a polydisc $\Delta_2 \subseteq \Delta_1'$ about 0 such that h' is order-invariant in $\Delta_2^{(n-2)} \times \{(0,0)\}$. Now the map $(z,z_n) \rightarrow (z,z_n + \psi(\mathbf{z}))$ is an analytic isomorphism of $\Delta_2 \times \mathbb{C}$ onto itself. Hence, by Theorem 2.3.1, the order of h' at $(\mathbf{z},0,0)$ is equal to the order of h at $(\mathbf{z},0,\psi(\mathbf{z}))$, for every $\mathbf{z} \in \Delta_2^{(n-2)}$. Therefore h is order-invariant in the set G^* defined by equation (4.2.1). We have shown that Theorem 4.2.1 holds. □

It remains, therefore, to establish Theorems 4.2.2 and 4.2.3. We will first need to study irreducible Weierstrass polynomials and factorization. Let R be an integral domain. A non-constant element of the polynomial ring $R[z_n]$ is said to be *reducible* if it is a product of non-constant polynomials of lower degree, and is otherwise said to be *irreducible*. Let R now be the ring of all holomorphic functions in the polydisc Δ_1 about 0 in $\mathbb{C}^{n-1}$. As Δ_1 is connected, R is an integral domain (by the identity theorem, Theorem 2.1.4). Let $h(z,z_n)$ be a Weierstrass polynomial in Δ_1. Then h can be regarded as a polynomial in z_n over the ring R, i.e. as an element of $R[z_n]$. It follows by induction on the degree of h that h may be factored as a product of irreducible Weierstrass polynomials thus:

$$h = h_1 \cdots h_k .$$

It will follow from Lemma 4.2.5 below that the h_i are uniquely determined, provided that the discriminant of h does not vanish identically.

Let U be an open subset of $\mathbb{C}^n$. A continuous function $\Gamma : [0,1] \to U$, with $\Gamma(0) = w_0$ and $\Gamma(1) = w_1$, is called a *path* in U from w_0 to w_1. Let Γ and Γ' be paths in U, from w_0 to w_1, and from w_1 to w_2, respectively. Then the *composite path* $\Gamma' * \Gamma$ from w_0 to w_2 is defined as follows:

$$(\Gamma' * \Gamma)(t) = \begin{cases} \Gamma(2t) & \text{if } 0 \le t \le 1/2 \\ \Gamma'(2t-1) & \text{if } 1/2 \le t \le 1 \end{cases}$$

The *reverse path* Γ^r of Γ is defined by $\Gamma^r(t) = \Gamma(1-t)$, $0 \le t \le 1$.

Lemma 4.2.4 : Let Δ_1 be a polydisc about 0 in $\mathbb{C}^{n-1}$ and let $h(z,z_n)$ be a Weierstrass polynomial of positive degree in Δ_1. Let U be an open subset of

Δ_1 in which the discriminant of h does not vanish. Let w and w' be points of U, not necessarily distinct, and let Γ be a path in U from w to w'. Let α be a root of $h(w,z_n)$. Then there is 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 $m \geq 1$, let $V = \{ (z,z_n) \in U \times \mathbb{C} : h(z,z_n) = 0 \}$, and let w_0 be a point of U. By m applications of the implicit function theorem, there exists a neighbourhood $W \subseteq U$ of w_0 such that the portion of V contained in $W \times \mathbb{C}$ consists of the disjoint graphs of m holomorphic functions from W into $\mathbb{C}$. Hence ([MUN75], 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 then follows by the path lifting property (Lemma 4.1 in Ch. 8 of [MUN75]). □

Remark. With the notations of the above lemma, we set $\Gamma_h[\alpha] := \phi(1)$ and say Γ *carries* α *into* $\phi(1)$ (*via* h).

The following is an important lemma about irreducible Weierstrass polynomials:

Lemma 4.2.5 : Let Δ_1 be a polydisc about 0 in $\mathbb{C}^{n-1}$ and let $h(z,z_n)$ be n irreducible Weierstrass polynomial in Δ_1. Let $G(z)$ be the discriminant of $h(z,z_n)$, let $F(z)$ be a holomorphic function in Δ_1, not identically zero, such that $G(z) = 0 \Rightarrow F(z) = 0$ for all z in Δ_1, and let $U = \{ z \in \Delta_1 : F(z) \neq 0 \}$. Let $w \in U$ and let α be a root of $h(w,z_n)$. Then for every $w' \in U$ and every root α' of $h(w',z_n)$, 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 in [BMA48], Ch. 9, Sec. 3, pp 194-198. □

Remark. The above lemma implies that the irreducible factors of a Weierstrass polynomial whose discriminant does not vanish identically are uniquely determined.

We can now give the

Proof of Theorem 4.2.2 : Factor h into a product of irreducible Weierstrass polynomials $h_1 \cdots h_k$. Let $1 \leq i \leq k$, and let $G(z)$ be the discriminant of $h_i(z, z_n)$. Recall that the discriminant $F(z)$ of $h(z, z_n)$ has the form $F(z) = z_{n-1}^r N(z)$ for all $z \in \Delta_1$, where $N(z)$ is holomorphic and non-vanishing in Δ_1. Now the zero set of G is contained in that of F by Lemma 2.3.4, and is hence a subset of $H^* \cap \Delta_1$. But if $G(\mathbf{w},0) = 0$ for some $\mathbf{w} \in \Delta_1^{(n-2)}$, then $G(\mathbf{z},0) = 0$ for all $\mathbf{z} \in \Delta_1^{(n-2)}$ by zero system continuity (see [WHI72], Ch. 1, Lemma 5E). Hence the zero set of G is either empty, or the entire region $H^* \cap \Delta_1$.

We shall show that, for each point $w = (\mathbf{w},0)$ in $H^* \cap \Delta_1$, there exists exactly one distinct root of $h_i(w, z_n)$. This is clearly true if $G \neq 0$ in Δ_1, as in this case the degree of h_i is 1. Suppose, on the other hand, that $G = 0$ in $H^* \cap \Delta_1$, and that, for some $w = (\mathbf{w},0) \in H^* \cap \Delta_1$, $h_i(w, z_n)$ has some $l \geq 2$ distinct roots, say $\alpha_1, \ldots, \alpha_l$, with multiplicities $m_1, \ldots, m_l$ respectively. Choose disjoint open discs $D_1, \ldots, D_l$ about $\alpha_1, \ldots, \alpha_l$, respectively. By root continuity of the bivariate Weierstrass polynomial $h_i(\mathbf{w}, z_{n-1}, z_n)$, there exists a disc D' about 0 in the plane of the z_{n-1}-coordinate such that

$\Delta_1^{(n-2)} \times D' \subseteq \Delta_1$ and such that, for every fixed w_{n-1} in D', there are exactly m_j roots (counted according to multiplicity) of $h_i(\mathbf{w},w_{n-1},z_n)$ in D_j, $1 \leq j \leq l$.

Let w_{n-1}' be a non-zero point of D', let $w' = (\mathbf{w},w_{n-1}')$ and let α and β be roots of $h_i(w',z_n)$ in D_1 and D_2 respectively. Let $U = \{ z \in \Delta_1 : G(z) \neq 0 \}$. Then $U = \Delta_1 H^*$. By Lemma 4.2.5, there is a path $\Gamma(t) = (\Gamma(t),\Gamma_{n-1}(t))$ in U from w' to itself such that $\Gamma_{h_i}[\alpha] = \beta$. Let $r = (\mathbf{r},r_{n-1})$ be the polyradius of Δ_1. We can deform Γ in U to a path Γ' in the set defined by $\mathbf{z} = \mathbf{w}$, $|z_{n-1}| < r_{n-1}$, by means of the path homotopy ([MUN75], Ch. 8)

$$H(s,t) = ((1-s)\Gamma(t) + s\,\mathbf{w},\Gamma_{n-1}(t))$$

(for which $H(0,t) = \Gamma(t)$ and $H(1,t) = (\mathbf{w},\Gamma_{n-1}(t))$). Furthermore, we can deform Γ' in U to a path Γ'' along the circle defined by $\mathbf{z} = \mathbf{w}$, $|z_{n-1}| = |w_{n-1}'|$ by means of the path homotopy

$$K(s,t) = \left(\mathbf{w},(1-s)\Gamma_{n-1}(t) + \frac{s\,\Gamma_{n-1}(t)\,|w_{n-1}'|}{|\Gamma_{n-1}(t)|}\right).$$

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 4.2.4. By Theorem 4.3 of Ch. 8 of [MUN75], $\phi''(1) = \beta$ (which implies $\Gamma_{h_i}''[\alpha] = \beta$). Yet, as $\phi''(t)$ is a root of $h_i(\Gamma''(t),z_n)$, we must have that $\phi''(t) \in \bigcup_{j=1}^{l} D_j$, for all t. 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 all t. This contradicts $\phi''(1) = \beta$, as β is an element of D_2. Hence our assumption that $h_i(w,z_n)$ has more than one distinct root must be

false. Thus $h_i(w,z_n)$ has exactly one distinct root, for each fixed w in the set $H^* \bigcap \Delta_1$.

We can now show that $h(w,z_n)$ has exactly one distinct root, for each fixed $w \in H^* \bigcap \Delta_1$. There is nothing further to prove if $k = 1$, so assume $k > 1$. Let $w \in H^* \bigcap \Delta_1$, let $1 \leq i < j \leq k$, and let α_i and α_j be the roots of $h_i(w,z_n)$ and $h_j(w,z_n)$ respectively, and assume that $\alpha_i \neq \alpha_j$. Then the resultant $R(z)$ of $h_i(z,z_n)$ and $h_j(z,z_n)$ does not vanish at $z = w$. However, the zero set of R contains 0, is contained in $H^* \bigcap \Delta_1$ (as $R(z) = 0 \Rightarrow F(z) = 0$), and is hence equal to the entire region $H^* \bigcap \Delta_1$ (by zero system continuity), contradicting $R(w) \neq 0$. Therefore, we must have $\alpha_i = \alpha_j$ after all. Hence $h(w,z_n)$ has exactly one distinct root, say α.

For $\mathrm{w} \in \Delta_1^{(n-2)}$, let $\psi(\mathrm{w})$ denote the unique root α of $h(\mathrm{w},0,z_n)$. Then, where m is the degree of h, we have

$$h(\mathrm{w},0,z_n) = (z_n - \psi(\mathrm{w}))^m .$$

Thus, where $a_1(z)$ is the coefficient of z_n^{m-1} in $h(z,z_n)$, we have

$$a_1(\mathrm{w},0) = -m\,\psi(\mathrm{w}).$$

Hence ψ is holomorphic in $\Delta_1^{(n-2)}$. □

We turn now to establishing Theorem 4.2.3. The theorem will follow from three lemmas on parametrizing an irreducible Weierstrass polynomial which satisfies the hypotheses of the theorem. The first lemma asserts the existence of a parametrization for such a Weierstrass polynomial.

Lemma 4.2.6 : Let $h(z,z_n)$ be an irreducible Weierstrass polynomial of

degree $M \geq 1$ in the polydisc $\Delta_1 = \Delta(0;\delta)$ in $\mathbb{C}^{n-1}$, and assume that h satisfies the hypotheses of Theorem 4.2.3. (In particular, assume that for every fixed z in Δ_1, all the roots of $h(z,z_n)$ are contained in the disc $\Delta(0;\epsilon)$ in $\mathbb{C}$.) Let $\rho = \delta$, let $\rho_{n-1} = \delta_{n-1}^{1/m}$, let $\rho = (\rho,\rho_{n-1})$, and let $\Delta_1' = \Delta(0;\rho)$. Then there is a holomorphic function $\phi : \Delta_1' \to \Delta(0;\epsilon)$ such that for every fixed $z = (z,z_{n-1}) \in \Delta_1$ and every z_n in $\Delta(0;\epsilon)$,

$$h(z,z_n) = 0 \text{ if and only if there exists u, } |u| < \rho_{n-1}, \text{ such that } \begin{cases} z_{n-1} = u^m \\ z_n = \phi(z,u) \end{cases}.$$

Proof. Even though the hypotheses of Theorem 4.2.1 specify $n \geq 3$, the hypotheses of the theorem, as indeed the present lemma, can be stated for $n = 2$ as well. The case $n = 2$ of the present lemma is Theorem 10A of [WHI72], Ch. 1. The hypotheses of Theorem 4.2.1 permit the extension of the result to higher dimensions. □

With the notation of the above lemma, we shall say that the pair of equations

$$\begin{cases} z_{n-1} = u^m \\ z_n = \phi(z,u) \end{cases}$$

defines a *parametrization* for h (in Δ_1). In such a parametrization let m_1 denote the order of ϕ at 0 in u. Then we shall see (Lemma 4.2.8 below) that for all z sufficiently close to 0,

$$\text{ord}_{(z,0,0)} h = \min(m,m_1).$$

That h is order-invariant in the set $\Delta_1^{(n-2)} \times \{(0,0)\}$ (near the origin) will fol-

low from this. The next result will be used in proving Lemma 4.2.8.

Let K be an algebraically closed field of characteristic zero. We shall denote by $K\{x\}$ the field of all fractional power series in the indeterminate x with coefficients in K; (see [WAL50],Ch. 4, Sec. 3, in which the notation $K(x)^*$ is used). That is, $K\{x\}$ consists of all elements θ of the form

$$\theta = a_h x^{h/m} + a_{h+1} x^{h+1/m} + \cdots \tag{4.2.2}$$

where $m \geq 1$ and h is an integer (possibly negative).

If θ is an element of $K\{x\}$ given by (4.2.2) and $a_h \neq 0$, then we define the *order* of θ, denoted by $O(\theta)$, to be h/m. Puiseux' theorem (Theorem 3.1 of [WAL50], Ch. 4) states that the field $K\{x\}$ is algebraically closed. Thus every nonconstant polynomial $g(x,y)$ over $K\{x\}$ can be factored into linear factors over $K\{x\}$ thus:

$$g(x,y) = \prod_{i=1}^{d} (y - \theta_i) ;$$

$\{\theta_1, \ldots, \theta_d\}$ is called the set of Puiseux roots of $g(x,y)$. We can now state and prove our next result.

Lemma 4.2.7 : Let $h(z,z_n)$ be an irreducible Weierstrass polynomial of degree $m \geq 1$ in the polydisc Δ_1 about 0 (in $\mathbb{C}^{n-1}$), and assume that h satisfies the hypotheses of Theorem 4.2.3. Let

$$\begin{cases} z_{n-1} &= u^m \\ z_n &= \phi(z,u) \end{cases}$$

be a parametrization for h and assume that ϕ is not identically zero. Assume that the power series expansion for ϕ about 0 is absolutely convergent in Δ_1' (using the notation of the previous lemma) and let this power series be

arranged as follows:

$$c_1(\mathbf{z})u^{m_1} + c_2(\mathbf{z})u^{m_2} + \cdots$$

where $0 < m_1 < m_2 < \cdots$ and the c_i are not identically zero. Assume $m > m_1$. Then there is a polydisc $\Delta_2 \subseteq \Delta_1$ about 0 such that $c_1(\mathbf{z}) \neq 0$ for all $\mathbf{z} \in \Delta_2^{(n-2)}$.

Proof. Let $\mathbf{z}$ be a fixed element of $\Delta_1^{(n-2)}$ and set $g_{\mathbf{z}}(z_{n-1},z_n) = h(\mathbf{z},z_{n-1},z_n)$. Regard $g_{\mathbf{z}}$ as a polynomial in z_n over the field $\mathbb{C}\{z_{n-1}\}$ by replacing each coefficient of $g_{\mathbf{z}}$ by its power series expansion about 0. Let ζ be a primitive m-th root of unity and for $1 \leq i \leq m$, let $\theta_i(\mathbf{z})$ denote the element

$$c_1(\mathbf{z})\zeta^{(i-1)m_1} z_{n-1}^{m_1/m} + c_2(\mathbf{z})\zeta^{(i-1)m_2} z_{n-1}^{m_2/m} + \cdots$$

of $\mathbb{C}\{z_{n-1}\}$. As the power series in u obtained by expanding

$$g_{\mathbf{z}}(u^m, c_1(\mathbf{z})u^{m_1} + c_2(\mathbf{z})u^{m_2} + \ldots)$$

is identically zero, we have, setting $u = \zeta^{(i-1)} z_{n-1}^{1/m}$, that $g_{\mathbf{z}}(z_{n-1},\theta_i(\mathbf{z})) = 0$. Thus $\theta_i(\mathbf{z})$ is a Puiseux root of $g_{\mathbf{z}}(z_{n-1},z_n)$. But the $\theta_i(\mathbf{z})$, $1 \leq i \leq m$, are distinct. (For suppose $1 \leq i < j \leq m$, and $\zeta^{(i-1)m_k} = \zeta^{(j-1)m_k}$, $k = 1,2,\ldots$. Let $|u_1| < \rho_{n-1}$, $u_1 \neq 0$. Then the m distinct roots of $h(\mathbf{z},u_1^m,z_n)$ are the numbers

$$\phi(\mathbf{z},u_1), \phi(\mathbf{z},\zeta u_1), \ldots, \phi(\mathbf{z},\zeta^{m-1}u_1).$$

However,

$$\begin{aligned}\phi(\mathbf{z},\zeta^{i-1}u_1) &= c_1(\mathbf{z})\zeta^{(i-1)m_1}u_1^{m_1} + c_2(\mathbf{z})\zeta^{(i-1)m_2}u_1^{m_2} + \cdots \\ &= c_1(\mathbf{z})\zeta^{(j-1)m_1}u_1^{m_1} + c_2(\mathbf{z})\zeta^{(j-1)m_2}u_1^{m_2} + \cdots\end{aligned}$$

$$= \phi(z, \zeta^{j-1} u_1) ,$$

a contradiction.) Hence the $\theta_i(z)$, $1 \leq i \leq m$, constitute the complete set of Puiseux roots of $g_z(z_{n-1}, z_n)$. For $1 \leq i < j \leq m$, let $\eta_{i,j}(z) = \theta_i(z) - \theta_j(z)$. Then

$$\eta_{i,j}(z) = d_1^{(i,j)}(z) z_{n-1}^{m_1/m} + d_2^{(i,j)}(z) z_{n-1}^{m_2/m} + \cdots ,$$

where

$$d_k^{(i,j)}(z) = c_k(z) \zeta^{(i-1)m_k} - c_k(z) \zeta^{(j-1)m_k} = c_k(z)(\zeta^{(i-1)m_k} - \zeta^{(j-1)m_k}) .$$

Let $1 \leq i < j \leq m$, and let $k_{i,j}$ be the least positive integer k such that $d_k^{(i,j)}(0) \neq 0$; (the number $k_{i,j}$ certainly exists as $\theta_i(0) \neq \theta_j(0)$, and hence $\eta_{i,j}(0) \neq 0$). Then $O(\eta_{i,j}(0)) = m_{k_{i,j}}/m$. By continuity of the functions $d_{k_{i,j}}^{(i,j)}$, there exists a polydisc $\Delta_2 \subseteq \Delta_1$ about 0 such that for every pair (i,j) with $1 \leq i < j \leq m$,

$$d_{k_{i,j}}^{(i,j)}(z) \neq 0$$

for every $z \in \Delta_2^{(n-2)}$. Thus, for all (i,j),

$$O(\eta_{i,j}(z)) \leq m_{k_{i,j}}/m ,$$

for every z in $\Delta_2^{(n-2)}$. We shall show that in fact we have equality here.

For fixed z in $\Delta_2^{(n-2)}$, let $D_z(z_{n-1}) = F(z, z_{n-1})$ (F the discriminant of h). Then as $F(z, z_{n-1} = z_{n-1}^r . N(z, z_{n-1})$ by hypothesis,

$$\operatorname{ord}_0 D_z = r . \tag{4.2.3}$$

On the other hand, $D_z(z_{n-1})$ can be regarded as the discriminant of the polynomial

$$g_z(z_{n-1}, z_n) \in \mathbb{C}\{z_{n-1}\}[z_n]$$

and hence as an element of $\mathbb{C}\{z_{n-1}\}$. As $\theta_1(z), \ldots, \theta_m(z)$ are the roots of $g_z(z_{n-1}, z_n)$ in $\mathbb{C}\{z_{n-1}\}$, we have

$$D_z = \prod_{1 \le i < j \le m} (\theta_i(z) - \theta_j(z))^2 = \prod_{1 \le i < j \le m} \eta_{i,j}(z)^2 \ .$$

Hence, by (4.2.3), we have

$$r = 2 \sum_{1 \le i < j \le m} O(\eta_{i,j}(z)) \ . \tag{4.2.4}$$

As (4.2.4) holds with $z = 0$, and as $O(\eta_{i,j}(z)) \le O(\eta_{i,j}(0))$ for all (i,j), it follows that

$$O(\eta_{i,j}(z)) = O(\eta_{i,j}(0)) \ , \tag{4.2.5}$$

for all (i,j).

Now there exists some z' in $\Delta_2^{(n-2)}$ such that $c_1(z') \neq 0$, as c_1 is not identically zero. Note that $\zeta^{m_1} \neq 1$, as $0 < m_1 < m$ and ζ is a primitive m-th root of 1. Thus $\zeta^{0.m_1} - \zeta^{1.m_1} \neq 0$ and hence by (4.2.5), $O(\eta_{1,2}(0)) = m_1/m$. Therefore, by (4.2.5), $O(\eta_{1,2}(z)) = m_1/m$, for all z in the polydisc $\Delta_2^{(n-2)}$: that is, $d_1^{1,2}(z) \neq 0$, for all $z \in \Delta_2^{(n-2)}$. As

$$d_1^{1,2}(z) = c_1(z)(\zeta^{0.m_1} - \zeta^{1.m_1}) \ ,$$

it follows that $c_1(z) \neq 0$ for all $z \in \Delta_2^{(n-2)}$. This completes the proof of the lemma. □

Lemma 4.2.8 : Let $h(z, z_n)$ be an irreducible Weierstrass polynomial of degree $m \ge 1$ in the polydisc Δ_1 about 0 (in complex $(n-1)$-space), and assume that h satisfies the hypotheses of Theorem 4.2.3. Let

$$\begin{cases} z_{n-1} &= u^m \\ z_n &= \phi(\mathbf{z},u) \end{cases}$$

be a parametrization for h, and let m_1 be the order of ϕ at 0 in u. Then there is a polydisc $\Delta_2 \subseteq \Delta_1$ about 0 such that

$$\operatorname{ord}_{(\mathbf{z},0,0)} h = \min(m, m_1)$$

for all $\mathbf{z} \in \Delta_2^{(n-2)}$.

Proof. Suppose first of all that $\phi \equiv 0$. Then $m = 1$ and $h(z, z_n) = z_n$. Thus $\operatorname{ord}_{(\mathbf{z},0,0)} h = 1$ for all $\mathbf{z} \in \Delta_1^{(n-2)}$. Suppose on the other hand that ϕ is not identically zero. Using the notation of Lemma 4.2.6 we may assume, by refining Δ_1' suitably, that the power series expansion for ϕ about 0 is absolutely convergent in Δ_1'. Let this power series be arranged as follows:

$$c_1(\mathbf{z})u^{m_1} + c_2(\mathbf{z})u^{m_2} + \cdots$$

where $0 < m_1 < m_2 < \cdots$ and the c_i are not identically zero. Let $\mathbb{C}\{\mathbf{z}\}$ be the field of all fractional power series in $z_1, \ldots, z_{n-2}$. That is, inductively, $\mathbb{C}\{\mathbf{z}\}$ consists of all elements of the form

$$a_h(z_1,\ldots,z_{n-3}) z_{n-2}^{h/m} + a_{h+1}(z_1, \ldots, z_{n-3}) z_{n-2}^{(h+1)/m} + \cdots$$

where $m \geq 1$, h is an integer (possibly negative), and

$$a_k(z_1,\ldots,z_{n-3}) \in \mathbb{C}\{z_1,\ldots,z_{n-3}\}.$$

We can show by induction on $n-2$, using Puiseux' theorem, that $\mathbb{C}\{\mathbf{z}\}$ is algebraically closed. Let $K = \mathbb{C}\{\mathbf{z}\}$, and regard $h(\mathbf{z}, z_{n-1}, z_n)$ as a polynomial in z_n over the field $K\{z_{n-1}\}$ by replacing each coefficient of h by its power series expansion about the origin (suitably arranged). Let ζ be a prim-

itive m-th root of unity and for $1 \leq i \leq m$, let θ_i be the element

$$c_1(\mathbf{z})\zeta^{(i-1)m_1} z_{n-1}^{m_1/m} + c_2(\mathbf{z})\zeta^{(i-1)m_2} z_{n-1}^{m_2/m} + \cdots$$

of $K\{z_{n-1}\}$. Now the power series in $\mathbf{z}$ and u obtained by expanding

$$h(\mathbf{z}, u^m, c_1(\mathbf{z})u^{m_1} + c_2(\mathbf{z})u^{m_2} + \cdots)$$

is identically zero. Hence, setting $u = \zeta^{(i-1)} z_{n-1}^{1/m}$, we obtain $h(\mathbf{z}, z_{n-1}, \theta_i) = 0$. Thus θ_i is a Puiseux root of $h(\mathbf{z}, z_{n-1}, z_n)$. But the θ_i are distinct (cf. proof of Lemma 4.2.7) and hence constitute the complete set of Puiseux roots of $h(\mathbf{z}, z_{n-1}, z_n)$. Thus

$$h(\mathbf{z}, z_{n-1}, z_n) = \prod_{i=1}^{m} (z_n - \theta_i)$$

and so, where

$$h(\mathbf{z}, z_{n-1}, z_n) = z_n^m + a_1(\mathbf{z}, z_{n-1}) z_n^{m-1} + \cdots + a_m(\mathbf{z}, z_{n-1}),$$

we have

$$\begin{aligned}
a_1(\mathbf{z}, z_{n-1}) &= -(\theta_1 + \cdots + \theta_m) \\
a_2(\mathbf{z}, z_{n-1}) &= + \sum_{1 \leq i < j \leq m} \theta_i \theta_j \\
&\cdots \\
a_m(\mathbf{z}, z_{n-1}) &= (-1)^m \theta_1 \cdots \theta_m \ .
\end{aligned}$$

We shall consider separately the two cases $m \leq m_1$ and $m > m_1$.

Case I : $m \leq m_1$

We have $O(\theta_i) = m_1/m \geq 1$, for $1 \leq i \leq m$. Hence $O(a_j) \geq j$, for $1 \leq j \leq m$. This impies that, for $1 \leq j \leq m$, the order (say t_1) in z_{n-1} of the holomorphic functions a_j at the origin is at least j. Let $\Delta_2 \subseteq \Delta_1$ be a

polydisc about 0 in which the power series expansion about 0 of each a_j is absolutely convergent. Then it follows that, for each point z' in $\Delta_2^{(n-2)}$, the order in z_{n-1} of a_j at $(z',0)$ is at least j. (This is clearly true if $a_j \equiv 0$, so assume that a_j is not identically zero, and let the power series expansion for a_j about (0,0) be arranged thus:

$$\alpha_1(z) z_n^{t_1-1} + \alpha_2(z) z_n^{t_2-1} + \cdots$$

where the α_i are not identically zero. Then, where $\alpha_i'(z-z')$ denotes the power series expansion for α_i about z', we have that

$$\alpha_1'(z-z') z_n^{t_1-1} + \alpha_2'(z-z') z_n^{t_2-1} + \cdots$$

is the power series expansion for a_j about $(z',0)$. Thus the order in z_{n-1} of a_j is t_1 ($\geq j$) at $(z',0)$.) Therefore, for each point z' of $\Delta_2^{(n-2)}$, we have $\operatorname{ord}_{(z',0)} a_j \geq j$, hence

$$\operatorname{ord}_{(z',0,0)} (a_j(z,z_{n-1}) z_n^{m-j}) \geq j + m - j = m .$$

It follows that

$$\operatorname{ord}_{(z',0,0)} h = m = \min(m, m_1)$$

for every $z' \in \Delta_2^{(n-2)}$.

Case II : $m > m_1$.

By Lemma 4.2.7, there is a polydisc $\Delta_2 \subseteq \Delta_1$ about 0 such that $c_1(z) \neq 0$ for all $z \in \Delta_2^{(n-2)}$. As in Case I, $O(\theta_i) = m_1/m$. Thus $O(a_j) \geq jm_1/m$, for $1 \leq j \leq m$. Therefore, for $1 \leq j \leq m$, the order in z_{n-1} of the holomorphic function a_j at the origin is greater than or equal to jm_1/m. Assume, by refining Δ_2 if necessary, that the power series expansion about

0 of each a_j is absolutely convergent. Then it follows that, for $1 \leq j \leq m$, and for each point $z' \in \Delta_2^{(n-2)}$, the order in z_{n-1} of a_j at $(z',0)$ is greater than or equal to jm_1/m. Therefore, for $1 \leq j < m$ and for $z' \in \Delta_2^{(n-2)}$, we have $\operatorname{ord}_{(z',0)} a_j \geq jm_1/m$, hence

$$\begin{aligned} \operatorname{ord}_{(z',0,0)} (a_j (z,z_{n-1}) z_n^{m-j}) &\geq jm_1/m + m - j \\ &= m - j(1 - m_1/m) \\ &> m - m(1 - m_1/m) \\ &= m_1 . \end{aligned}$$

Now $a_m(z,z_{n-1}) = (-1)^m \theta_1 \cdots \theta_m$ and

$$\theta_1 \cdots \theta_m = d_1(z) z_{n-1}^{m_1} + d_2(z) z_{n-1}^{m_1+1} + \cdots ,$$

where $d_1(z) = (-1)^{(m+1)m_1} c_1(z)^m$. Thus, as $c_1(z') \neq 0$ for each $z' \in \Delta_2^{(n-2)}$, we have that $\operatorname{ord}_{(z',0)} a_m = m_1$ for each $z' \in \Delta_2^{(n-2)}$. Hence

$$\operatorname{ord}_{(z',0,0)} h = m_1 = \min(m, m_1)$$

for every $z' \in \Delta_2^{(n-2)}$. □

We can give at last the

Proof of Theorem 4.2.3 : Factor h into a product of irreducible Weierstrass polynomials $h_1 \cdots h_k$. Let $1 \leq i \leq k$ and let $G(z)$ be the discriminant of $h_i(z, z_n)$. Recall that the discriminant $F(z)$ of $h(z, z_n)$ has the form

$$F(z) = z_{n-1}^r N(z) ,$$

where $N(z)$ is holomorphic and non-vanishing in Δ_1. Let $\delta = (\delta_1, \ldots, \delta_{n-1})$ be the polyradius of Δ_1. Now $F(z) = G(z)H(z)$, for

some holomorphic $H(z)$, by *Theorem 2.3.3.* Hence, for every fixed $\mathbf{z} \in \Delta_1^{(n-2)}$, we must have

$$G(\mathbf{z},z_{n-1}) = z_{n-1}^{s} U(\mathbf{z},z_{n-1}) ,$$

for some s, $0 \leq s \leq r$, and some $U(\mathbf{z},z_{n-1})$, holomorphic and non-vanishing in the disc $|z_{n-1}| < \delta_{n-1}$. By zero system continuity, s does not depend on $\mathbf{z}$. In fact, $U(\mathbf{z},z_{n-1})$ is holomorphic in the variables $z_1, \ldots, z_{n-2}$, as well as z_{n-1}, as the expression

$$U(\mathbf{z},z_{n-1}) = \frac{1}{2\pi i} \int_C \frac{U(\mathbf{z},\zeta)\, d\zeta}{\zeta - z_{n-1}}$$

holds for $\mathbf{z} \in \Delta_1^{(n-2)}$ and z_{n-1} inside C, for any circle C about 0 in the disc $|z_{n-1}| < \delta_{n-1}$. Thus h_i satisfies the hypotheses of Theorem 4.2.3. Let p be the degree of h_i. By Lemma 4.2.6 there exists a parametrization

$$\begin{cases} z_{n-1} &= u^p \\ z_n &= \phi(\mathbf{z},u) \end{cases}$$

for h_i in Δ_1. Let p_1 be the order of ϕ at 0 in u. By Lemma 4.2.8 there exists a polydisc $\Delta_i' \subseteq \Delta_1$ about 0 such that

$$\operatorname{ord}_{(\mathbf{z},0,0)} h_i = \min(p, p_1)$$

for all $\mathbf{z}$ in $\Delta_i'^{(n-2)}$. Thus h_i is order-invariant in $\Delta_i'^{(n-2)} \times \{(0,0)\}$.

Let $\Delta_2 = \bigcap_{i=1}^{k} \Delta_i'$. Then $h \left(= \prod_{i=1}^{k} h_i \right)$ is order-invariant in $\Delta_2^{(n-2)} \times \{(0,0)\}$. □

Chapter Five

Cad Construction Using Reduced Projection

This chapter presents algorithms for cad construction which use the reduced projection operation studied in Chapter 3.

Section 1 develops an algorithm for computing cad's when the input polynomials are oriented favourably in a certain sense. The algorithm presented resembles the algorithm *CAD* from Section 3.1 closely, except that the reduced projection is used in place of the original.

Section 2 presents a cad algorithm which can be used on quite general sets of polynomials. The algorithm has to work harder to provide order-invariant decompositions over nullifying cells (where some polynomial vanishes identically) in each dimension.

Section 3 provides clustering cad algorithms for the plane and 3-space. These algorithms yield smooth, order-invariant clusters of cells.

5.1 Cad computation for well-oriented polynomials

In this section we shall endeavour to formulate a cad construction algorithm using the reduced projection operation introduced in Chapter 3, which resembles the fundamental algorithm *CAD* reviewed in Section 3.1 as closely as possible. In attempting to keep the algorithm as simple as possible, at

least for the time being, we will be required to impose certain assumptions on the input set of polynomials. These assumptions have their origin in the hypothesis of Theorem 3.2.3 that each polynomial of the given basis not vanish identically on the submanifold in question. It will be argued that many sets of polynomials satisfy the required assumptions, and a partial test for determining whether or not the assumptions are satisfied will be given. Furthermore, it will be shown that any set of polynomials can be transformed into a set for which the assumptions hold. In the next section we shall relax the assumptions on the input polynomials, and show how to deal with the general case.

We now state precisely the assumptions referred to above.

Definition. A set A of non-zero r-variate integral polynomials is said to be *well-oriented* if $r = 1$, or, if $r > 1$, then

(1) for every $F \in prim(A)$, $F(a, x_r) \equiv 0$ for at most finitely-many $a \in \mathbb{R}^{r-1}$, and

(2) $P(A)$ is well-oriented.

Thus, if A is a well-oriented set of polynomials, then no element of $prim(A)$ vanishes identically on any submanifold of $\mathbb{R}^{r-1}$ of positive dimension. Moreover, this property holds recursively for $P(A)$.

It is not hard to see that if $r = 1,2,3$ then *every* set A of non-zero r-variate polynomials is well-oriented. A random polynomial in four variables of degree at least two in the main variable is likely to be well-oriented, as there are not likely to be more than a finite number of simultaneous solutions of the coefficients. Let F be a random polynomial in five variables of

degree at least three in the main variable. Then it is probable that condition (1) of the definition of well-oriented shall hold, as the set of 4-variate coefficients of F (a set containing at least 4 elements) probably has only finitely-many common zeros. If, further, the degree of each 4-variate coefficient in its main variable is at least two, then it is probable that condition (2) of the definition of well-oriented shall also hold. More generally, it would be reasonable to suggest that a finite set A of random polynomials $F(x_1,...,x_r)$ such that the degree of F in the i-th variable is at least $i-2$ is probably well-oriented.

The cad algorithm that we shall shortly present accepts as input a set A of well-oriented polynomials. The question thus arises as to how one determines whether a given set of polynomials is well-oriented or not. When the number of variables does not exceed three, the set is always well-oriented. In the case of four variables one needs to examine the primitive part of each input polynomial to determine whether its coefficients vanish simultaneously at at most finitely many points in three-space. In general, one must examine not only the input set A, but also $P(A)$, $P(P(A))$, and so on. In the next paragraph we consider the problem of determining whether the coefficients of a polynomial have only finitely many simultaneous solutions.

It is sometimes easy to see whether the coefficients of a polynomial $F(x_1,...,x_r)$ have at most finitely many common zeros (for example, whenever a coefficient is a non-zero constant). Computation of successive resultants of some or all of the pairs of the coefficients (eliminating $x_{r-1},...,x_2$ in that order) may reveal that the common zeros of the coefficients have only finitely many distinct x_1- coordinates. If it can be determined in a similar

way that, for each i, $1 \leq i \leq r-1$, the common zeros have only finitely many distinct x_i-coordinates, then there are only finitely many common zeros. A finitely many common zeros test based upon resultant computation has been implemented in the SAC-2 computer algebra system: the name of the algorithm is *IPFZT* ("Integral Polynomial Finitely Many Common Zeros Test"). For details of the method one should consult the listing of *IPFZT*. For most cases in which there are only finitely many common zeros, the test *IPFZT* will indicate this. However, there are some exceptional cases in which *IPFZT* cannot distinguish the well-oriented from the non well-oriented case. Whenever the "well-oriented" property has not been determined to hold, one can apply the more general cad algorithm given in the next section.

We now present a simplified cad construction algorithm *CADRW* which can be applied to a well-oriented set A of polynomials in r variables, yielding a list of sample points for an A-invariant cad D of $\mathbb{R}^r$. The algorithm *CADRW* is modelled on its counterpart from Section 3.1, *CAD*. The main difference between the two algorithms is that in *CADRW*, the map P is used in place of the map *PROJ*. Defining formula construction is possible in this setting, although requires a somewhat generalized notion of "well-oriented" (see remarks following the abstract algorithm *CADRW*, presented later in this section).

A cad constructed by the new algorithm *CADRW* has certain additional properties: each cell is smooth, and every polynomial in the input set A is order-invariant in each cell. A cad which has these properties is thus termed a smooth, *A-order-invariant* cad. The additional properties are bought

quite cheaply. Theorem 3.2.3 guarantees that they will hold except where the primitive part of some input polynomial vanishes identically. But the number of such nullifying points is finite, by the well-oriented condition. To take account of the nullifying points we introduce the following terminology: for a smooth cell c in $\mathbb{R}^{r-1}$ with sample point α, and basis $B = \{B_1,...,B_n\}$, the *delineating set* $\hat{B}_c$ for B on c is defined to be the set $\{ \hat{B}_j : 1 \leq j \leq n \}$, where $\hat{B}_j$ is the "least" partial derivative (with respect to the standard lexicographic ordering of partial derivatives) of B_j such that $\hat{B}_j(\alpha,x_r)$ is not identically zero. Thus, if A is a finite well-oriented set of polynomials and B is a squarefree basis for $prim(A)$, then we have

$$\hat{B}_c = B$$

for every $P(A)$-invariant cell c of $\mathbb{R}^{r-1}$ of positive dimension. The algorithm *CADRW* below uses the delineating set to obtain an order-invariant decomposition of the cylinder over any nullifying 0-cell.

CADRW $(r, A; S)$

[Cylindrical algebraic decomposition, reduced projection, well-oriented polynomials. A is a well-oriented set of integral polynomials in r variables, $r \geq 1$. S is a list of sample points for a smooth, A-order-invariant cad D of $\mathbb{R}^r$.]

(1) [Initialize.] Set $B \leftarrow$ the finest squarefree basis for $prim(A)$. Set $S \leftarrow ()$.

(2) [$r = 1$.] If $r > 1$ then go to 3. Isolate the real roots of B. Construct sample points for the cells of D and add them to S. Exit.

(3) [$r > 1$.] Set $P \leftarrow P(A)$. [Recall $P(A) = cont(A) \cup P(B)$.] Call

CADRW recursively with inputs $r-1$ & P to obtain a list S' of sample points for a smooth, P-order-invariant cad D' of $\mathbb{R}^{r-1}$. For each cell c of D', let α denote the sample point for c, and carry out the following sequence of steps: set $\hat{B} \leftarrow$ the delineating set for B over c; set

$$B^* = \{\hat{B}_j(\alpha, x_r) : \hat{B}_j \in \hat{B}\};$$

isolate the real roots of B^*; use α and the isolating intervals for the roots of B^* to construct sample points for the $\hat{B}$-sections and $\hat{B}$-sectors over c, adding them to S. Exit □

It is straightforward to prove the validity of *CADRW* using Theorem 3.2.3.

The above algorithm could be modified so as to yield defining formulas as well as sample points. The modified algorithm, like the algorithm *CAD* of Section 3.1, would accept as input a triple (r, A, k), $0 \leq k \leq r$, and would yield as output lists S and F (F the list of defining formulas). In the modified algorithm the first instruction of Step 3 would be the following:

If $k < r$ then set $P \leftarrow P(A)$ and $k' \leftarrow k$, and otherwise set $P \leftarrow AP(A)$ and $k' \leftarrow k-1$.

The next instruction would be a recursive call to the algorithm with inputs $(r-1, P, k')$. There would be a restriction on the allowed inputs (r, A, k) comparable to the well-oriented condition: an input (r, A, k) would have to be well-oriented in the sense that:

(1) for every $F \in prim(A)$, $F(a, x_r) \equiv 0$ for at most finitely many $a \in \mathbb{R}^{r-1}$; and

(2) if $k < r$ then $(r-1, P(A), k)$ is well-oriented, and otherwise $(r-1, AP(A), k-1)$ is well-oriented.

We shall show that any set A of r-variate non-zero integral polynomials can be transformed by means of an invertible linear transformation into a well-oriented set A'. The coordinate transformation we shall use will yield an even stronger property for A':

Definition. A set A of non-zero r-variate real polynomials is said to be *very-well-oriented* (*vwo*) if $r = 1$ or, if $r > 1$, then
(1) for every $F \in A$, the degree of F in x_r is equal to the total degree of F; and
(2) $P(A)$ is vwo.

We will need the following lemma:

Lemma 5.1.1. Let $H(x_1,\ldots,x_r)$ be a non-zero homogeneous polynomial with integer coefficients. One can determine integers $\lambda_1, \ldots, \lambda_{r-1}$ such that $H(\lambda_1, \ldots, \lambda_{r-1}, 1) \neq 0$.

Proof. Now $H(x_1,\ldots,x_{r-1},1) \neq 0$, and hence $H(\lambda,x_2,\ldots,x_{r-1},1)$ reduces to the zero polynomial for only finitely many $\lambda \in \mathbb{C}$. Test $\lambda = 0, +1, -1, +2, -2, \ldots$ until an integer λ_1 is found such that $H(\lambda_1,x_2,\ldots,x_{r-1},1) \neq 0$. Similarly, find an integer λ_2 such that $H(\lambda_1,\lambda_2,x_3,\ldots,x_{r-1},1) \neq 0$. Continuing in this manner, obtain $\lambda_1, \ldots, \lambda_{r-1}$ such that $H(\lambda_1, \ldots, \lambda_{r-1}, 1) \neq 0$. □

Recall that a linear transformation T of $\mathbb{R}^r$ corresponds to an $r \times r$ matrix

(α_{ij}). We say that T is an *integral* linear transformation if every entry of the corresponding matrix is an integer. If $F(x_1,...,x_r)$ is a real polynomial then the *transform* of F by T, denoted F_oT, is the polynomial $F(T(x_1,...,x_r))$. If A is a set of real polynomials then the transform of A by T, denoted A_oT, is the set of all F_oT, with $F \in A$.

Theorem 5.1.2. Let A be a finite set of non-zero integral polynomials in $x_1,...,x_r$. Then one can construct an invertible integral linear transformation T of $\mathbb{R}^r$ such that the transform of A by T is vwo.

Proof. We proceed by induction on r. If $r = 1$, then A is vwo. Assume that the theorem is true for $r-1$. Let $A = \{F_1,...,F_n\}$ be a set of non-zero integral polynomials in $x_1,...,x_r$. Let d_i be the total degree of F_i, and let H_i be the homogeneous part of F_i of degree d_i. Let $d = \sum d_i$ and let $H = \prod H_i$. Then by Lemma 5.1.1, we can determine integers $\lambda_1, \ldots, \lambda_{r-1}$ such that $H(\lambda_1, \ldots, \lambda_{r-1},1) \neq 0$.

Let

$$S(x_1,...,x_r) = (x_1 + \lambda_1 x_r, \ldots, x_{r-1} + \lambda_{r-1} x_r, x_r).$$

Then the transform of F_i by S has the property that the degree in x_r equals d_i. By induction hypothesis, we can construct an invertible integral linear transformation T_{r-1} of $\mathbb{R}^{r-1}$ such that the transform of $P(A_oS)$ by T_{r-1} is vwo. With $x = (x_1,...,x_{r-1})$, let $\bar{T}_{r-1}(x, x_r) = (T_{r-1}(x), x_r)$, $T_r = S_o\bar{T}_{r-1}$, and $A' = A_oT_r$.

We shall now prove that A' is vwo. Let $F \in A'$. Then $F' = F_{i\,o}T_r$, for some i. Now

$$F'(0,x_r) = F_i(T_r(0,x_r)) = F_i(S(T_{r-1}(0),x_r))$$
$$= F_i(S(0,x_r)) = (F_i \circ S)(0,x_r) .$$

Hence the degree of F' in x_r equals d_i, (which is equal to the total degree of F'.) Hence condition (1) of the definition of vwo is satisfied. Suppose that $r > 2$. Now $A_o S$ consists entirely of primitive polynomials (as the coefficient of $x_r^{d_i}$ in $F_i \circ S$ is a constant). Hence, where B is the coarsest squarefree basis for $A_o S$, we have $P(A_o S) = P(B)$. As $A' = (A_o S)_o \bar{T}_{r-1}$, $B_o \bar{T}_{r-1}$ is the coarsest squarefree basis for A'. Now a moment's thought will convince one that $P(B)_o T_{r-1} = P(B_o \bar{T}_{r-1})$. Therefore, $P(A_o S)_o T_{r-1} = P(A')$. Hence $P(A')$ is vwo. This establishes condition (2) of the definition of vwo. □

5.2 Cad computation in general

In case an input set of polynomials is known to be well-oriented, we may use the algorithm *CADRW* from the previous section. What to do when the input set is not known to be well-oriented? This section contains a cad algorithm using the reduced projection that may be applied in the general case.

Definition. Let A be a set of r-variate integral polynomials. The cell c in $(r-1)$-space is said to be a *nullifying cell (for A)* if some element of $prim(A)$ vanishes identically on c.

If a set A of r-variate polynomials is not known to be well-oriented, then there could be a nullifying cell c for A of positive-dimension in $(r-1)$-space. If we wish to obtain a cad of r-space, *sign*-invariant with respect to

the polynomials in A, then this situation presents no difficulties. However our use of the reduced projection operator is based upon the construction of *order*-invariant cad's. Unfortunately, Theorem 3.2.3, with its hypothesis that the cell in question is not a nullifying cell, is of no help in determining an order-invariant decomposition of the cylinder over c.

The strategy of our general algorithm is to examine each polynomial of $prim(A)$ in turn, to determine whether the coefficients have only finitely-many common zeros: we use the SAC-2 algorithm *IPFZT* for this purpose. If a polynomial F could have a nullifying cell of positive dimension (as determined by *IPFZT*), then we enlarge the set A by adding to it all of the non-constant partial derivatives of F of all positive orders. Let us denote this enlarged set containing A by $\bar{A}$. We form the reduced projection of $\bar{A}$, and inductively construct a cad D' of $(r-1)$-space consisting of smooth cells, order-invariant with respect to the projection. Let c be a cell of D'. Theorem 3.2.3 implies that the cylinder over c is partitioned by the zeros of $\bar{A}$ into a finite number of disjoint smooth sections and sectors, in each of which the polynomials in $\bar{A}$ are sign-invariant. By definition of $\bar{A}$, this partitioning of the cylinder over c is sign-invariant with respect to the partial derivatives of any $F \in prim(A)$ vanishing identically on c, and is hence order-invariant with respect to any such F.

We now present our general cad algorithm that uses reduced projection.

$$CADR(r, A, k; S, F)$$

[Cylindrical algebraic decomposition, reduced projection. A is a finite set of integral polynomials in r variables, $r \geq 1$. k satisfies $0 \leq k \leq r$. S is a list of

sample points for a smooth, A-order-invariant cad D of $\mathbb{R}^r$. If $k \geq 1$, F is a list of defining formulas for the induced cad of $\mathbb{R}^k$, and if $k = 0$, F is the empty list.]

(1) [Initialize.] If $r > 1$ then, for each polynomial F in $prim(A)$, apply the test *IPFZT* to the coefficients of F and, if the test reports a zero, enlarge A by adding to it all of the nonconstant partial derivatives of positive order of F. Denote this enlargement of A by $\bar{A}$. Set $B \leftarrow$ the finest squarefree basis for $prim(\bar{A})$. Set $S \leftarrow$ () and $F \leftarrow$ ().

(2) [$r = 1$.] If $r > 1$ then go to 3. Isolate the real roots of B. Construct sample points for the cells of D and add them to S. If $k = 1$, then construct defining formulas for the cells of D and add them to F. Exit.

(3) [$r > 1$.] If $k < r$ then set $P \leftarrow P(\bar{A})$ & $k' \leftarrow k$; otherwise set $P \leftarrow AP(\bar{A})$ and $k' \leftarrow k-1$. Call *CADR* recursively with inputs $r-1$, P, and k' to obtain lists S' and F' which specify a smooth, P-order-invariant cad D' of $\mathbb{R}^{r-1}$. For each cell c of D', let α denote the sample point for c, and carry out the following sequence of instructions: set $B* \leftarrow$ the set of $B_j(\alpha,x_r)$ such that $B_j \in B$ and $B_j(\alpha,x_r)$ is not the zero polynomial; isolate the real roots of $B*$; use α and the isolating intervals for the roots of $B*$ to construct sample points for the B-sections and B-sectors over c, adding them to S; if $k = r$, then construct defining formulas for the B-sections and B-sectors over c, adding them to F, and if $k < r$, then set $F < F'$. Exit □

We mention a couple of refinements that one could make to this cad

algorithm. First, an improvement that could be made to both the above algorithm and the algorithm *CADRW* from the last section. Let A be a squarefree basis of r-variate integral polynomials. In general, it is not necessary to include in $P(A)$ every coefficient of every polynomial in A. Suppose that we discover using *IPFZT* that the first k coefficients of some $F \in A$ vanish simultaneously at only a finite number of points of $\mathbb{R}^{r-1}$. Then the rest of the coefficients of F can be excluded from $P(A)$. Thus, in general, we would expect to have to include in $P(A)$ at most $r-1$ coefficients of each polynomial in A.

Second, a refinement to the general algorithm *CADR*. We can sometimes do better than including in the set $\bar{A}$ the entire set of non-constant partial derivatives of a polynomial likely to have a nullifying cell of positive dimension. Suppose that F is such a polynomial, with nullifying cell c, and that some partial derivative of F of order t is a non-zero constant. Then it suffices to place into $\bar{A}$ only those partial derivatives of F of order less than t. For a decomposition of the cylinder over c into sections and sectors that are sign-invariant with respect to the partial derivatives of F of order less than t will be an F-order-invariant decomposition of this cylinder.

The inclusion of partial derivatives in the set $\bar{A}$ in algorithm *CADR* increases the size of the projection set of A. However, this inclusion of "extra" polynomials may not in fact be necessary. It would seem plausible, since the reduced projection $P(A)$ suffices to determine an order-invariant decomposition of $\mathbb{R}^r$ with respect to A whenever A is well-oriented, that $P(A)$ should also suffice to produce such a decomposition in the non-well-oriented case. The author had hoped for some time that the following

conjecture (cf. Theorem 3.2.3) would be true, but it is now known to be false:

Conjecture 1: Let A be a finite basis of r-variate integral polynomials, $r \geq 2$, and let S be a connected submanifold of $\mathbb{R}^{r-1}$. Suppose that each element of $P(A)$ is order-invariant in S. Then the cylinder over S can be partitioned into a finite number of smooth sections and sectors over S, in each of which every polynomial in A is order-invariant.

Note that this conjecture resembles Theorem 3.2.3 closely, but differs from it in that the hypothesis that S not be a nullifying cell for A has been relaxed. Unfortunately, the following counter-example disproves the conjecture:

Counter-example to Conjecture 1: Let A consist of the single squarefree polynomial in four variables $F(x,y,z,w) = zw + xy - z$. Let S be the x-axis in $\mathbb{R}^3$. Now $P(A)$ consists of the polynomials z, and $xy - z$. Hence each element of $P(A)$ is order-invariant in S. However, the order of F throughout the entire cylinder over S is equal to one, except at the point (0,0,0,1), where the order of F is two. (This can be seen by writing down the partial derivatives of F.) Hence no partitioning of the cylinder over S of the kind asserted in Conjecture 1 can exist.

The set S in the above counter-example would not in fact be a cell constructed by the cad algorithm. The algorithm would yield the origin as a 0-cell, and the positive and negative portions of the x-axis as 1-cells. We shall state a modification of Conjecture 1 whose hypotheses exclude sets S of the

kind used in the counter-example. First some terminology.

Definition . Let S be a connected subset of $\mathbb{R}^r$, order-invariant with respect to a set of polynomials P. The *order-variety of S with respect to P* is the set of all points of $\mathbb{R}^r$ at which the order of each element of P is the same as it is on S.

Conjecture 2. Let A be a squarefree basis of r-variate integral polynomials, $r \geq 2$, and let S be a connected submanifold of $\mathbb{R}^{r-1}$. Suppose that each element of $P(A)$ is order-invariant in S, and that the order-variety of S with respect to $P(A)$ is identical with S, near each point of S. Then the cylinder over S can be partitioned into a finite number of smooth sections and sectors over S, in each of which every polynomial in A is order-invariant, and such that the order-variety of each section or sector s with respect to A is locally identical with s.

5.3 Clustering cad algorithms

The original cad algorithm proposed by Collins did not yield the adjacency relationships between cells of a cad. Thus the original algorithm has limited application to investigation of the topological properties of semi-algebraic sets. Moreover, it was observed that the cad algorithm tends to decompose a semi-algebraic set into a great deal more cells than seems to be necessary. In 1980 cell adjacency algorithms for 2-space and 3-space were devised by Arnon, Collins and McCallum. Arnon [ARN81] subsequently used these adjacency algorithms to develop what he termed the *clustering* cad algorithm. The clustering algorithm attempts to combine adjacent cells

that have the same sign pattern for elements of the input set A together to form larger units that correspond to the A-invariant components of the appropriate Euclidean space.

A *cluster* is a collection of cells of D whose union is connected. In this section we give procedures based upon the algorithms and theorems from Chapter 4 of [ARN81] for producing smooth, A-order-invariant clusters in 2-space and 3-space (given an input set A). In 2-space the clusters produced correspond to the maximal connected, smooth, A-order-invariant regions of the plane. In 3-space, however, the clusters obtained are not necessarily maximal.

The clustering algorithm for 2-space given here uses the order pattern on adjacent cells, instead of the sign pattern, as a basis for combining cells. Fortunately, the connected components of the A-order-invariant regions of the plane are smooth:

Theorem 5.3.1. Let A be a set of bivariate polynomials with real coefficients. Let S be a maximal connected, A-order-invariant subset of $\mathbb{R}^2$. Then S is a submanifold of $\mathbb{R}^2$.

Proof . Let $F(x,y)$ be the product of the irreducible factors in $\mathbb{R}[x,y]$ of the elements of A (so $F(x,y)$ has no repeated nonconstant factors in $\mathbb{R}[x,y]$). Then S is a maximal connected, F-order-invariant subset of $\mathbb{R}^2$. (For if T is a connected, F-order-invariant set containing S, then by Lemma 3.2.2, each factor of F is order-invariant in T, hence each element of A is order-invariant in T, again by Lemma 3.2.2. By maximality of S for A, we must have $T = S$.) Now the set of points P in the plane for which

$\text{ord}_P F = 0$ comprises an open subset, or a 2-submanifold, of the plane. Also, the set of points P for which $\text{ord}_P F = 1$ comprises a 1-submanifold of the plane (see definition of 1-submanifold). The singular points of F (i.e. the points P for which $\text{ord}_P F > 1$) are isolated, as F is squarefree with respect to x and y. Hence, the singular points of F comprise a 0-submanifold of $\mathbb{R}^2$. The above observations imply that S is a connected component of *some* submanifold of the plane. It follows that S is itself a submanifold of $\mathbb{R}^2$. □

We define some technical terms used in our 2-space clustering algorithm. An *adjacency* of a cad D is a pair of cells of D that are adjacent. A *clustering* of D is a partitioning of the cells of D into clusters. Let C be a clustering of D. An adjacency (c, d) of D is said to be an *outer-adjacency* (with respect to C) if c and d belong to different clusters of C. A *representative cell* of a cluster of C is a cell of maximum dimension belonging to the cluster. Every cluster manipulated by the algorithms given below has a specially designated representative cell.

We now give the 2-space algorithm, *CLCSO*2.

*CLCSO*2$(A, k; C, I, S, F)$

[Clustered cad of the plane, smooth, order-invariant clusters. A is a set of bivariate integral polynomials. k satisfies $0 \leq k \leq 2$. C is a list of smooth, A-order-invariant clusters for a smooth, A-order-invariant cad D of the plane. I is the list of all adjacencies of D. S is a list of sample points for certain cells of D, such that S contains a sample point for the representative

cell of every cluster in C, and S contains a sample point for the lower-dimensional cell of each outer-adjacency in I. If $k \geq 1$, then F is a list of defining formulas for the cad of k-dimensional space induced by D. If $k = 0$, then F is the null list.]

(1) [Initialize.] Set $B \leftarrow$ the finest squarefree basis for $prim(A)$.

(2) [Determine D', the induced cad of 1-space.] If $k < 2$ then set $P \leftarrow P(A)$ and $k' \leftarrow k$; otherwise set $P \leftarrow AP(A)$ and $k' \leftarrow k-1$. Isolate the real roots of P. Construct sample points for the cells of D', recording these in S'. If $k' = 1$, then construct defining formulas for the cells of D', recording them in F'; otherwise set $F' \leftarrow ()$.

(3) [Determine D and the order of each element of A on its cells.] For each cell c of D', let α denote the sample point for c, and carry out the following sequence of steps: set $B* \leftarrow$ the set of all $B_j(\alpha,x_2)$ such that $B_j \in B$ and $B_j(\alpha,x_2) \not\equiv 0$; isolate the real roots of $B*$, thereby determining the number of sections and sectors of A over c; determine the order of each element of A on each section and sector and save for use in Step 6 below.

(4) [Construct defining formulas for D, if desired.] If $k = 2$ then for each cell c of D', construct defining formulas for the sections and sectors of A over c (using F') and record them in F; otherwise set $F \leftarrow F'$.

(5) [Determine adjacencies of D.] For each pair c,d of adjacent cells in D', use the box adjacency algorithm SSADJ2 from [ACM84b] to determine all adjacencies between (possibly infinite) sections of A over c and (possibly infinite) sections of A over d. Infer all other adjacencies

of D from these. Record the adjacencies in I.

(6) [Determine clusters.] Let $c_1,...,c_m$ be the cells of D' in increasing (left-to-right) order. Initialize C to the set of clusters each of which consists of a single section or sector over c_1. For $i = 1,...,m-1$ do the remaining actions of this step: add the (sets containing single) sections and sectors over c_{i+1} to C; for each adjacency (s,t) in I, where s is over c_i and t is over c_{i+1}, use the order information from Step 3 to determine whether the polynomials in A have the same order on s as they have on t; if so, then combine the cluster containing s with the cluster containing t.

(7) [Sample point construction.] Construct a sample point for the representative cell of each cluster. Construct a sample point for the lower-dimensional cell of any outer-adjacency of D. Record these sample points in S. Exit □

That *CLCSO*2 produce a sample point for the lower-dimensional cell of each outer-adjacency of a cad of the plane is required by the 3-space clustering algorithm, to which we now turn.

Let A be a set of trivariate polynomials, let P be the reduced projection $P(A)$ of A, and let S be (the underlying region of) a smooth, P-order-invariant, positive-dimensional cluster in the plane, as produced by the above algorithm. Then, by Theorem 3.2.3, every element of $prim(A)$ is delineable on S, and moreover the sections and sectors of A over S are smooth and A-order-invariant. Now the cad algorithm applied to A yields, amongst the cells in 3-space that it produces, the sections and sectors of A

over each cell comprising the cluster S. Hence, the sections and sectors over all the cells of S may be grouped into "large" sections and sectors extending over the whole of S; and furthermore, these large sections and sectors are smooth and order-invariant for A. The large sections and sectors over S are known as the *initial* clusters over S. The question thus arises as to how the initial clusters over adjacent clusters in the plane may be further combined, ideally to form the largest possible smooth, order-invariant clusters in 3-space.

Unfortunately, clustering on the basis of the same pattern of orders of the elements of A (as was done for the plane) does not necessarily produce smooth clusters in 3-space:

Example. Let A consist of the single polynomial

$$F(x,y,z) = z^2 - x^2y^2,$$

and let S be the union of the x-axis and the y-axis. Then S is the set of all points at which the order of F equals 2. However S is not a submanifold of $\mathbb{R}^3$.

The connected components of the nonsingular portion of the variety of the product of the elements of A are smooth; strictly speaking, we have the following

Theorem 5.3.2. Let A be a set of trivariate polynomials with real coefficients and let F be the product of the irreducible factors in $\mathbb{R}[x,y,z]$ of the elements of A. Let S be a maximal connected, A-order-invariant subset of $\mathbb{R}^3$, in which the order of F is 1. Then S is a 2-submanifold of $\mathbb{R}^3$.

Proof. Straightforward.

We must be more careful in clustering the singular portions of the variety of the product of elements of A. We do not have a general method for producing maximal smooth, order-invariant clusters within the singular set. However, we do have a method that appears to yield the maximal such clusters in many special cases (including the case in which the variety of each element of A has at worst isolated singularities, and intersects the variety of every other element of A transversally). We give the definition and the theorem underlying this method, and proceed to describe the 3-space clustering algorithm.

Definition. Let A be a set of trivariate polynomials with real coefficients and let c be either a 0-cell or a 1-cell in $\mathbb{R}^3$. We say that c is *A-Jacobian-regular* if either c is a 1-cell or, if c is a 0-cell, then there exist exactly two distinct irreducible factors of elements of A, say G and H, that vanish on c, and, where $M(x,y,z) = (G(x,y,z),H(x,y,z))$ and $c = \{P\}$, the Jacobian matrix of the map M at P, $J_M(P)$, is non-singular.

Theorem 5.3.3. Let A be a set of trivariate polynomials with real coefficients and let F be the product of the irreducible factors in $\mathbb{R}[x,y,z]$ of the elements of A. Let S be a maximal connected, A-order-invariant, union of A-Jacobian-regular 0-cells and 1-cells of a smooth, A-order-invariant cad D of $\mathbb{R}^3$, such that the order of F is greater than 1 throughout S. Then S is a 1-submanifold of $\mathbb{R}^3$.

Proof. Let P be a point of S. Then P is either a 0-cell, or P is contained

in a 1-cell, say c. In the latter case, S is identical with c in a neighborhood of P, by the boundary property (see [ARN81]: Sec. 3.1 and Theorem 3.6.22). Hence, in this case S is a 1-submanifold near P (as c is). Suppose, on the other hand, that P is a 0-cell. Then, by the Jacobian-regularity at P, there exist exactly two irreducible factors of elements of A which vanish at P, say G and H; moreover, the Jacobian matrix of G and H at P is non-singular. Hence, by definition of submanifold, the variety of the two polynomials G and H is a 1-submanifold near P. We shall show that S is identical with this variety near P. Let Q be a point of S. Then $G(Q) = H(Q) = 0$, so Q belongs to the variety of G and H. Let N be a neighborhood of P in which every irreducible factor of the elements of A except for G and H is nonzero, in which some first-order partial derivative of each of G and H is nonzero, and which meets no other 0- or 1-cells of D except for those adjacent to P. Let Q be a point (other than P) of the variety of G and H, contained in N. Now the polynomials in A have the same order pattern at Q as they have at P (by definition of N); further, $\mathrm{ord}_Q F > 1$. Thus Q belongs to some 1-cell, say c, of the cad D; and further, c is adjacent to P (by definition of N). Hence, by definition of S, we must have $c \subseteq S$. Therefore, Q is a point of S. We have now shown that $S \cap N$ is identical with the portion of the variety of G and H contained in N, and hence that S is a 1-submanifold near P. □

We now present the 3-space clustering algorithm.

$$CLCSO3(A,k;C,I,S,F)$$

[Clustered cad of 3-space, smooth, order-invariant clusters. A is a list of trivariate integral polynomials. k satisfies $0 \leq k \leq 3$. C is a list of smooth, A-order-invariant clusters formed from a smooth, A-order-invariant cad D of $\mathbb{R}^3$. I is a list of certain of the adjacencies of D. S is a list of sample points for certain cells of D, such that S contains a sample point for the representative cell of every cluster in C. If $k \geq 1$, then F is a list of defining formulas for the cad of k-dimensional space induced by D. If $k = 0$, then F is the null list.]

(1) [Initialize.] Set $B \leftarrow$ the finest squarefree basis for $prim(A)$.

(2) [Determine D' and a clustering for it.] If $k < 3$ then set $P \leftarrow P(A)$ and $k' = k$; otherwise set $P \leftarrow AP(A)$ and $k' = k-1$. Call $CLCSO2$ with inputs P and k' to obtain outputs C', I', S', and F'.

(3) [Determine the list L of cells of D.] Set L = (). For each cluster K of C', let c denote the representative cell for K, and α the sample point for c; perform the following sequence of instructions: set $B^* \leftarrow$ the set of all $B_j(\alpha,z)$, where $B_j \in B$ and $B_j(\alpha,z) \neq 0$; if c is a nullifying 0-cell, add additional elements of $Q(\alpha)[z]$ to B^* as described in [ARN81], Section 4.8, so that D will be "cylindricity- refined" (the 3-space adjacency algorithm, to be called in Step 6, requires D to have this property); isolate the real roots of B^*, thereby determining the number of sections and sectors over c, and hence the number of sections and sectors over any cell d in K. Add the set of all sections and sectors over every cell of K to the list L.

(4) [Determine vanishing information for the cells of D.] Let $G(x,y,z)$ be

the product of the elements of B, together with the nonconstant irreducible factors in $Z[x,y]$ of the elements of $cont(A)$. For each cluster K of C', with representative cell say c, and each section or sector s over c, do the following: determine the order of each element of A on s; if some element of A vanishes on s, then determine whether or not the order of G on s is 1; if the order of G on s is greater than one, then determine whether s is A-Jacobian-regular. Save all this information for use in Step 8 below.

(5) [Construct defining formulas for D, if desired.] If $k = 3$, then for each cluster K of C', with representative cell say c, construct defining formulas for the sections and sectors over c (using F'), and from these infer the defining formulas for the sections and sectors over each cell of K (as described in Section 4.7 of [ARN81]); record these defining formulas in F. Otherwise set $F \leftarrow F'$.

(6) [Determine the set of adjacencies of D.] Adjacencies within a cylinder over (the underlying region of) a cluster are clear. Use the 3-space adjacency algorithm from [ARN81], *SBAA*3, to determine, for each outer-adjacency (c,d) of I', with $dim(c) < dim(d)$, the boundary of every section over d in the extended cylinder over c. All adjacencies of D can be inferred from this information.

(7) [Determine smooth, A-order-invariant clusters, as large as possible.] Initialize $C \leftarrow ()$. For each outer-adjacency (c,d) of I' do the following: if not previously done, add the initial clusters over J, K to C (J,K the cluster of C' containing c,d resp.); for each adjacency (s,t) from Step 6, with s a cell over c and t a cell over d, determine

whether the information saved from Step 4 is the same for s as for t; if so, then combine the cluster containing s with the cluster containing t.

(8) [Sample point construction.] Construct a sample point for the representative cell of each cluster in C. Exit □

Chapter Six

Evaluation of the modified cad algorithms

We present in this chapter both theoretical analysis of and empirical observations about the cad algorithms from Chapter Five. An analysis of the algorithm *CADRW* from Section 5.1 is the subject of the first section of this chapter. Our analysis parallels that presented by Collins in [COL75]. We are able to derive an improved computing time bound for the cad algorithm, which nevertheless remains super-exponential in the number of variables r.

Both the two- and three-space clustering algorithms from Section 5.3 were implemented in the *SAC* −2 computer algebra system. Several examples of the application of these algorithms are presented in Section 6.2.

6.1 Algorithm analysis

We present here a fairly detailed analysis of the cad algorithm *CADRW* from Section 5.1. We follow the basic structure of the analysis in Section 4 of [COL75] quite closely. The first step of *CADRW* calls for the construction of the finest squarefree basis of $prim(A)$, where A is the (well-oriented) input set of r-variate polynomials. To simplify the analysis, however, we will assume that a *coarsest* squarefree basis is computed instead. The theorems of Chapter Three which support the validity of *CADRW* remain

true if one uses a coarsest, rather than a finest, squarefree basis in the definition of the reduced projection P. (From a practical point of view, it is advantageous to use the finest squarefree basis, even though more work is required to compute it.)

A little terminology first of all. Recall that the *norm* of an integral polynomial A in r variables, denoted by $|A|_1$, is the sum of the absolute values of the integer coefficients of A. The *length* of an integer a, denoted by $L(a)$, is the number of bits in the binary representation of a. We shall make use of the basic properties $L(ab) \leq L(a)+L(b)$, and $L(a) \leq a$ (if $a > 0$) in our analysis.

The three basic parameters used in Collins' analysis are the number m of polynomials contained in A, a bound n for the degree of each polynomial in A in each variable, and a norm-length bound d for the elements of A. Our analysis will be facilitated by assigning somewhat different meanings to the parameters m and n. We shall say that a set A of r-variate polynomials has the (m,n)*-property* if the set A can be partitioned into at most m disjoint subsets, such that the product of the polynomials in each subset has degree at most n (in any variable). It is clear that if A has the (m,n)-property then so does any squarefree basis B for $prim(A)$.

Lemma 6.1.1 : Let A be a finite set of integral polynomials, in r variables, $r \geq 2$, and let $A*$ be the reduced projection $P(A)$. Suppose that A has the (m,n)-property, and that d is a norm-length bound for the elements of A. Then $A*$ has the $(m*,n*)$-property, and norm-length bound $d*$, where

$$m* \leq 2m^2n \ , \tag{6.1.1}$$

$$n* \leq 2n^2 , \tag{6.1.2}$$

$$d* \leq 7rn^2 + 2nd. \tag{6.1.3}$$

Proof : Recall that $A*$ is equal to

$$cont(A) \cup coeff(B) \cup discr(B) \cup res(B) ,$$

where B is the coarsest squarefree basis for $prim(A)$. Now as A has the (m,n)-property, A can be partitioned into m disjoint subsets, $S_1,...,S_m$, such that the product of the elements of each subset has degree no more than n. Let T_1 be the set of basis elements which divide some element of S_1; for $i > 1$, let T_i be the set of basis elements which divide some element of S_i, and which do not already occur in some T_j, $j < i$. Then, where *ldcf* is short for "leading coefficient", we claim that the product of all elements of the set

$$cont(S_i) \cup ldcf(T_i) \cup discr(T_i) \cup res(T_i) \tag{6.1.4}$$

has degree no more than $2n^2$ (in any variable). For if c is the product of the elements of $cont(S_i)$, and $T_i = \{F_1,...,F_t\}$, then the polynomial $F := cF_1...F_t$ divides the product of the elements of S_i, and hence has degree less than or equal to n. Hence the resultant of F and F' has degree at most $2n^2$ (in any variable), as it is the determinant of a matrix with at most $2n$ rows and columns, whose entries have degree at most n (in any variable). But this resultant is equal to a power of c multiplied by the following:

$$\prod_{j=1}^{t} ldcf(F_j) \prod_{j=1}^{t} discr(F_j) \prod_{j<k} res(F_j,F_k)^2.$$

Our claim follows from this.

There are at most m sets of the form (6.1.4). The remaining elements of A^* are of two kinds: coefficients of elements of B other than leading coefficients, and resultants of the form $res(F_j,G_k)$, with F_j an element of some T_j and G_k an element of some T_k. The set of these remaining coefficients of elements of B clearly has the (mn,n)-property, while the set of all these remaining resultants clearly has the $(\frac{m^2-m}{2},2n^2)$-property. All told, A^* can be partitioned into no more than

$$m + mn + \frac{m^2-m}{2} = \frac{m}{2} + mn + \frac{m^2}{2} \leq 2m^2n$$

sets, such that the degree of the product of all the elements from any set is not greater than $2n^2$. This establishes (6.1.1) and (6.1.2).

Let c be the maximum norm of the elements of B, and let e be the length of c. Then $e \leq 3rn + d$, by Corollary 2.3.5 (to Gelfond's theorem). Let F and G be elements of B. Then, by Theorem 2 in [COH74],

$$| res(F,G) |_1 \leq |F|_1^n |G|_1^n \leq c^{2n} .$$

Now $|F'|_1 \leq n|F|_1$. Hence, by Theorem 1 in [COH74], (recalling the definition of discriminant,)

$$| discr(F) |_1 \leq |F|_1^{n-1} n^n |F|_1^n \leq n^n c^{2n-1} .$$

Therefore, if P is any element of $P(B)$, then the length of the norm of P is at most $nL(n)+2ne$, hence at most $7rn^2+2nd$. □

In the projection phase of algorithm *CADRW* we compute the successive projections $P(A)$, $P(P(A))$,... . We can obtain by induction, using Lemma 6.1.1, corresponding bounds for all these projections.

Lemma 6.1.2: Let A be as in Lemma 1, and assume that A has the (m,n)-property, and has norm length bound d. Let $A_1 = A$ and, for $1 \leq k < r$, let A_{k+1} be the reduced projection $P(A_k)$ of A_k. Then, for $1 \leq k \leq r$, A_k has the (m_k, n_k)-property, and has norm-length bound d_k, where

$$m_k \leq (2n)^{(k-1)2^{k-2}} m^{2^{k-1}}, \tag{6.1.5}$$

$$n_k \leq \frac{1}{2}(2n)^{2^{k-1}}, \tag{6.1.6}$$

$$d_k \leq r(2n)^{2^k} d. \tag{6.1.7}$$

Proof : Inequalities (6.1.5) and (6.1.6) are easily established by induction. Note that (6.1.7) holds for $k = 1,2$. Assuming (6.1.7) holds for $k \geq 2$, we have by (6.1.3) and (6.1.6)

$$\begin{aligned} d_{k+1} &\leq 7rn_k^2 + 2n_k d_k \\ &\leq \frac{7}{4} r(2n)^{2k} + (2n)^{2k-1} r(2n)^{2k} d \\ &\leq 2r(2n)^{3.2^{k-1}} d \\ &\leq r(2n)^{2^{k+1}} d \end{aligned}$$

As basis computation is an integral part of the projection process, we need to know how long how long a basis computation takes.

Lemma 6.1.3: Let A be a set of r-variate integral polynomials which has the (m,n)-property and suppose that the factors of elements of A have norm-length bound $3rn+d$. Then the time to compute a coarsest squarefree basis for A is dominated by $r^2 m^3 n^{2r+6} d^2$.

Proof : Now A can be partitioned into m subsets S_i, such that the degree of

the product of the elements of S_i in any variable is at most n. We can compute a coarsest squarefree basis for A in two stages. In the first stage we compute a squarefree basis for each of the subsets S_i. We use an algorithm due to Loos that is described on page 147 of [COL75]. This algorithm requires polynomial greatest common divisor computation, the time for which [LOO82b] is $e^{2r+1}l^2$ (e a degree bound, l a norm-length bound for the r-variate input polynomials). As described on page 147 of [COL75], we employ Loos' algorithm and Musser's squarefree factorization algorithm [MUS71] alternately, at most n times each. In each of the (at most) n applications of Loos algorithm, each input set will contain at most n polynomials, with degrees and norm-lengths bounded by n and $3rn+d$ respectively. Thus the time for all applications of Loos' algorithm will be dominated by $nn^2n^{2r+1}(3rn+d)^2$, hence by $r^2n^{2r+6}d^2$. As the time for squarefree factorization of a polynomial P is $e^{2r+4}l^2$ (e a degree bound for P, $3re+l$ a norm-length bound for the factors of P), the time for the (at most) n squarefree factorizations is dominated by $n^{2r+5}d^2$. The total time to compute bases for each of $S_1,\ldots,S_m$ is thus $r^2n^{2r+6}m\,d^2$.

In the second stage, we successively combine, using Loos' algorithm, the bases obtained for the S_i to obtain, finally, a basis for A. In each of the m applications of Loos' algorithm, each input basis set will contain at most mn polynomials, with degrees bounded by n, and norm-lengths by $3rn+d$. Hence, the time for the second stage is dominated by $m\,(mn)^2n^{2r+1}(2rn+d)^2$, hence by $r^2n^{2r+5}m^3d^2$. The theorem now follows. □

Using the previous two lemmas we can now bound the total time spent in the projection phase of the algorithm.

Theorem 6.1.4: The total time spent in the projection phase of algorithm *CADRW* is dominated by $(2n)^{r\cdot 2^{r+3}} m^{2^r} d^2$.

Proof . The resultant of two polynomials in r variables, with degrees not greater than e, and with norms of length l or less can be computed in time $e^{2r+2} l^2$ (see [COL71]). Let A_k, $1 \le k \le r$, be as in Lemma 6.1.2. Now the norm-length of any polynomial in a basis for the set A_k is at most $3rn_k + d_k$; and the norm-length of the derivative of any such polynomial is at most $4rn_k + d_k$. Since the elements of A_k have $r-k+1$ variables, a resultant or a discriminant of A_{k+1} can be computed in time $n_k^{2(r-k+2)}(4rn_k + d_k)^2$, and there are no more than $n_k^2 m_k^2$ such resultants and discriminants to be computed. Thus the time to compute all resultants and discriminants of A_{k+1} is dominated by $r^2 n_k^{8+2(r-k)} m_k^2 d_k^2$, hence by $(2n)^{r\cdot 2^{r+2}} m^{2^{r-1}} d^2$ (using the inequality $2(r-k) \le 2^{r-k}$). It follows that the total time spent on resultant and discriminant computation in the projection phase is dominated by $(2n)^{r\cdot 2^{r+3}} m^{2^{r-1}} d^2$.

Before calculating the resultants and discriminants of A_{k+1} we compute a coarsest squarefree basis for $prim(A_k)$. By Lemma 6.1.3, the time for this is $r^2 m_k^3 n_k^{2(r-k+1)+6} d_k^2$. This expression is dominated by $r^2 n_k^{10+2(r-k)} m_k^3 d_k^2$, hence by $r^4 (2n)^{r\cdot 2^{r+2}} m^{2^r} d^2$. Thus the time for r such basis computations is dominated by $(2n)^{r\cdot 2^{r+3}} m^{2^r} d^2$.

We can neglect the relatively insignificant time to compute contents, coefficients and derivatives. The theorem now follows. □

Let D be the cad of $\mathbb{R}^k$ computed by *CADRW* and let D_k be the cad of $\mathbb{R}^k$ induced by D, for $1 \leq k \leq r$. Let c_k be the number of cells in D_k. We can establish the following bound for c_k:

Theorem 6.1.5: For $1 \leq k \leq r$, c_k is less than $(2n)^{r \cdot 2^r} m^{2^r}$.

Proof : The cells of D_1 are determined by the real roots of not more than m_r groups of polynomials, such that the product of the elements of each group has degree at most n_r. There are thus at most $m_r n_r$ such roots, and hence $c_1 \leq 2m_r n_r + 1$. For each value of k, $2 \leq k \leq r$, and each cell c of D_k, Step 3 of *CADRW* substitutes the $k-1$ coordinates of the sample point for c for the first $k-1$ variables of the k-variable polynomials in A_{r-k+1}, thereby obtaining a set of univariate polynomials with real algebraic number coefficients, which has the (m_{r-k+1}, n_{r-k+1})-property. Hence $c_k \leq c_{k-1}(2m_{r-k+1}n_{r-k+1} + 1)$. Now the inequalities for c_1 and c_k we have derived imply that $c_1 \leq 4m_r n_r$ and $c_k \leq 4m_{r-k+1}n_{r-k+1}c_{k-1}$, for $2 \leq k \leq r$. By induction on k, we thus have $c_k \leq \prod_{i=r-k+1}^{r} 4m_i n_i$, hence $c_k \leq \prod_{i=1}^{r} 4m_i n_i$. Now $4m_i n_i \leq 2(2n)^{(i-1)2^{i-2}+2^{i-1}} m^{2^{i-1}}$. Therefore, $c_k \leq 2^{r-1}.(2n)^{(r-1)2^{r-1}+2^r} m^{2^r}$ $\leq (2n)^a m^{2^r}$, where $a = (r-1)(2^{r-1}+1) + 2^r \leq r.2^r$. □

We next bound the time to compute the cad D_1 of the real line, invariant with respect to the polynomials in A_r.

Theorem 6.1.6: The time spent in the base phase of the algorithm is dominated by $(2n)^{r \cdot 2^{r+4}} m^{2^r} d^2$.

Proof : The time to compute a coarsest squarefree basis of the set A_r is dominated by $m_r^3 n_r^8 d_r^2$ (setting $r = 1$ in Lemma 6.1.3). Now the time to isolate the real roots of a set of p squarefree, pairwise relatively prime polynomials, with a degree bound of e and a norm-length bound of l is dominated by $pe^8 + p^7 e^7 l^3$ (see p 165 of [COL75]). There are at most $m_r n_r$ polynomials in the basis for A_r, each having degree at most n_r, and norm-length at most $n_r + d_r$ (by Mignotte's theorem). Hence the time to isolate the real roots of the basis polynomials is dominated by

$$(m_r n_r) n_r^8 + (m_r n_r)^7 (n_r + d_r)^3,$$

hence by $m_r^7 n_r^{17} d^3$. By Lemma 6.1.2, this expression is less than or equal to $(2n)^a m^b d^3$, where $a = 7(r-1)2^{r-2} + 17.2^{r-1} + 3.2^r$ $\leq r.2^{r+1} + 2^{r+3} + 2^{r-1} + 2^{r+2} \leq r.2^{r+4}$, and $b = 7.2^{r-1} < 2^{r+2}$. □

We now discuss the extension phase of the algorithm. In this last phase of the algorithm, computations with real algebraic numbers are performed. These computations are expensive, and it will turn out that the time for the last phase dominates the time for the preceding phases.

We need to have a measure of the sizes of the algebraic numbers that arise in the algorithm. As two different representations of real algebraic numbers are used, there are two different characterizations of size. Regarded as an element of the field of all real algebraic numbers, a real algebraic number α is represented by its integral minimal polynomial $M(x)$ and an interval I with rational endpoints such that α is the unique root of M in I. As discussed on pages 165 and 166 of [COL75], the size of α can be characterized by the degree of M and the norm-length of M.

Regarded as an element of the real algebraic number field $Q(\alpha)$, the real algebraic number β is represented by a polynomial $B(x) \in Q[x]$, with the degree of B less than that of M. The rational polynomial $B(x)$ is itself represented in the form $B(x) = b^{-1}\bar{B}(x)$, where b is an integer, $\bar{B}(x)$ is an integral polynomial, and b and $\bar{B}$ are relatively prime. In this case the size of β is characterized by the length of b and the norm-length of $\bar{B}$.

For each cell c in the cad D_k of $\mathbb{R}^k$, there is computed a real algebraic number α that is a primitive element for the sample point of c: that is, if $\beta = (\beta_1, \ldots, \beta_k)$ is the sample point of c, then $Q(\beta_1, \ldots, \beta_k) = Q(\alpha)$. A pair (M, I) which represents α is also computed. Let $A_k{}^*$ be the set of all such polynomials M. Let $n_k{}^*$ be the maximum degree of the elements of $A_k{}^*$ and let $d_k{}^*$ be the maximum norm-length of the elements of $A_k{}^*$.

For each coordinate β_i of a sample point β in $\mathbb{R}^k$, *CADRW* computes a rational polynomial $B_i = b_i{}^{-1}\bar{B}_i$ which represents β_i as an element of $Q(\alpha)$. Let $B_k{}'$ be the set of all such rational polynomials B_i associated in this way with sample points β in $\mathbb{R}^k$, and let $d_k{}'$ be the maximum of the set of all b-lengths and $\bar{B}$-norm-lengths, taken over all $B = b^{-1}\bar{B} \in B_k{}'$.

We will be able to improve the bounds for $n_k{}^*$, $d_k{}^*$, and $d_k{}'$ given in Theorems 14 and 15 of [COL75]. Our present goal is to set down recurrence relations for these quantities. We extract bounds for the case $k = 1$ directly from [COL75] (see equations 8,9 and 10):

$$n_1{}^* \leq n_r, \tag{6.1.8}$$

$$d_1{}^* \leq n_r + d_r, \tag{6.1.9}$$

$$d_1' \leq 4m_r^2 n_r^2 (n_r + d_r). \tag{6.1.10}$$

Let $\beta = (\beta_1, \ldots, \beta_k)$ be a sample point in $\mathbb{R}^k$, with primitive element α. Let $C(x_1,\ldots,x_{k+1})$ be a polynomial in the basis for A_{r-k}, and let β_{k+1} be a root of $C(\beta_1, \ldots, \beta_k, x_{k+1}) =: C^*(x_{k+1})$. We apply the algorithm *SIMPLE* described in [LOO82a] to α and β_{k+1}, producing α' such that $Q(\alpha,\beta_{k+1}) = Q(\alpha')$. Now the degree of the field $Q(\alpha)$ over Q is at most n_k^*, and the degree of β_{k+1} over $Q(\alpha)$ is at most n_{r-k}. Hence the degree of $Q(\alpha')$ over Q is at most $n_k^* n_{r-k}$. We have shown that

$$n_{k+1}^* \leq n_k^* n_{r-k}. \tag{6.1.11}$$

This improves the recurrence relation for n_k^* given in [COL75] (see equation 11). The improvement stems from our use of the *minimal* polynomial to represent an algebraic number: Collins was not able to use the minimal polynomial as no polynomial-time polynomial factorization algorithm was available in 1975.

We extract from [COL75] (equations 12 and 13) the recurrence relations for d_k^* and d_k' (there is a small error in equation 12, which does not affect any subsequent results, which we correct):

$$\begin{aligned} d_{k+1}^* \leq\ & (d_k^* n_{r-k}) n_k^* + (3n_{r-k}^2 + d_{r-k} + d_k^* + k n_{r-k} d_k') n_k^{*2} + \\ & (k+2) n_{r-k} d_k^* n_k^{*3}, \end{aligned}$$

$$\begin{aligned} d_{k+1}' \leq\ & d_k' + 2n_k^* n_{k+1}^{*2} + 5n_k^* n_{k+1}^* d_{k+1}^* + \\ & 2\{k n_{r-k} d_k' + n_{r-k} d_{r-k} + (k+4) n_k^* n_{r-k}^2 d_k^*\} n_k^{*2} m_{r-k}^2 . \end{aligned}$$

We can now prove a counterpart to Theorems 14 and 15 in [COL75].

Theorem 6.1.7: With n_k^*, d_k^* and d_k' as defined above,

$$n_k^* \leq (2n)^{2^r}, \tag{6.1.14}$$

$$d_k^*, d_k' \leq (2n)^{k.2^{r+3}} (2n)^{r.2^{r+2}} m^{2^{r+1}} d. \tag{6.1.15}$$

Thus,

$$d_k^*, d_k' \leq (2n)^{r.2^{r+4}} m^{2^{r+1}} d \ . \tag{6.1.16}$$

Proof : Using induction, we can establish by (6.1.8), (6.1.11), and (6.1.6) that $n_k^* \leq (2n)^{s_k}$, where $s_k = 2^{r-1} + \cdots + 2^{r-k}$. As $s_k < 2^r$, (6.1.14) follows.

We can now use (6.1.14) to simplify the recurrence relation (6.1.12). Now $k+2 \leq 2^{2^k}$, from which it follows by (6.1.6) that $(k+2)n_{r-k} \leq \frac{1}{2}(2n)^{2^r}$. Using this inequality, and (6.1.6), (6.1.7) and (6.1.14), we can then derive the following:

$$d_{k+1}^* \leq r\,(2n)^{2^{r+2}}(d + d_k^* + d_k'). \tag{6.1.17}$$

Similarly, we can simplify (6.1.13) using (6.1.5), (6.1.6), (6.1.7) and (6.1.14), obtaining:

$$d_{k+1}' \leq (2n)^{2^{r+2}} (2n)^{(r-k)2^{r-k-1}} m^{2^{r-k}} (rd + d_k^* + d_{k+1}^* + d_k'). \tag{6.1.18}$$

Substituting (6.1.17) into (6.1.18), and simplifying, yields:

$$d_{k+1}' \leq 2r\,(2n)^{2^{r+3}} (2n)^{(r-k)2^{r-k-1}} m^{2^{r-k}} (d + d_k^* + d_k'). \tag{6.1.19}$$

Let $D_k = d + d_k^* + d_k'$. Using (6.1.17) and (6.1.19) we find that

$$D_{k+1} \leq (2n)^{2^{r+3}} (2n)^{r.2^{r-k+1}} m^{2^{r-k}} D_k. \tag{6.1.20}$$

From (6.1.9) and (6.1.10) we obtain the following bound for D_1.

$$D_1 \leq (2n)^{2^{r+3}} (2n)^{r.2^{r+1}} m^{2^r} d \ . \tag{6.1.21}$$

Using (6.1.21) and the recurrence relation (6.1.20), it is then clear by induction that

$$D_k \leq (2n)^{k.2^{r+3}} (2n)^{2rs_k} m^{s_k} d , \qquad (6.1.22)$$

where $s_k = 2^r + \cdots + 2^{r-k+1}$. The inequalities (6.1.15) and (6.1.16) follow immediately. □

The main subalgorithms used in the extension phase of *CADRW* are *ABASIS* (univariate algebraic polynomial coarsest squarefree basis), *ISOL* (algebraic polynomial real root isolation), *NORMAL*, *SIMPLE*, and *IPFAC* (univariate integral polynomial factorization). Specifications for the first four of these algorithms are given in Sec. 2 of [COL75] (pp 147-149). A polynomial factorization algorithm was not used in [COL75], as no polynomial time algorithm for polynomial factorization was known in 1975. *IPFAC* is used in our scheme to determine the minimal polynomial of each primitive element computed by *SIMPLE*.

It is shown in [COL75] (p 168) that one can in fact use the basis and root isolation algorithms for *integral* polynomials (*IPBASIS* and *IPRRI* respectively) in place of *ABASIS* and *ISOL* respectively. This alternative strategy requires an algorithm *APGCD* (algebraic polynomial gcd). We shall henceforth assume that this alternative method is adopted.

Let us assume that the computing time of each of the subalgorithms used in the extension phase is dominated by

$$\mu^J \nu^K \delta^L ,$$

where μ is the number of input polynomials, and ν and δ are the maximum

degree and maximum norm-length respectively of the input polynomials. (Integer values of J, K and L exist since all the subalgorithms used have polynomial computing time bounds [LOO82a], [KAL82]).

We shall find bounds B_1, B_2, and B_3 for μ, ν, and δ respectively. Let us consider the extension from $\mathbb{R}^k$ to $\mathbb{R}^{k+1}$. A study of page 168 of [COL75] reveals that the number of polynomials input to the root isolation algorithm is at most

$$(m_{r-k}\, n_{r-k})(n_k * n_{r-k}) \ .$$

In fact this bound also applies to the other algorithms, hence serves as a bound for μ. Using (6.1.5), (6.1.6), and the derivation of (6.1.14), we thus obtain the following bound $B_1(r,m,n)$ for μ:

$$B_1(r,m,n) = (2n)^{r.2^{r+1}} m^{2^{r-1}} \ .$$

It can be seen that the right-hand sides of equations (11) and (13) from [COL75] bound ν and δ respectively. It follows that we have the following bounds $B_2(r,n)$, and $B_3(r,m,n,d)$ for ν and δ respectively:

$$B_2(r,n) = (2n)^{2^{r+1}}$$

$$B_3(r,m,n,d) = (2n)^{r.2^{r+4}} m^{2^{r+1}} d \ .$$

The time for one application of any of the algorithms in the extension phase is dominated by

$$B_1^J\, B_2^K\, B_3^L \ ,$$

hence by

$$(2n)^{r.2^{r+1}(J+K+8L)} m^{2^{r-1}(J+4L)} d^L \ .$$

The basis and root isolation algorithms are each applied c_k times (during the extension from $\mathbb{R}^k$ to $\mathbb{R}^{k+1}$), and *SIMPLE* and *IPFAC* are each applied at most c_{k+1} times. *NORMAL* is applied at most $c_k\,(m_{r-k}\,n_{r-k})$ times. Hence, using Theorem 6.1.5 (and its proof), it is straightforward to show that the total number of applications of each subalgorithm during the extension phase is at most

$$(2n)^{r\cdot 2^{r+1}}\,m^{2^r}\quad .$$

Hence the total time for the extension phase is dominated by

$$(2n)^{r\cdot 2^{r+1}(J+K+8L+1)}\,m^{2^{r-1}(J+4L+2)}\,d^L\quad .$$

Let E and F be the lengths of $2(J+K+8L+1)$ and (the ceiling of) $\frac{1}{2}(J+4L+2)$ respectively. We thus have:

Theorem 6.1.8: The total time for the extension phase of *CADRW* is dominated by

$$(2n)^{r\cdot 2^{r+E}}\,m^{2^{r+F}}\,d^L\quad .$$

As J, K, and L are positive integers, $E \geq 5$ and $F \geq 3$. Hence, comparing Theorem 6.1.8 with Theorems 6.1.4 and 6.1.6, we obtain the following:

Theorem 6.1.9: The total time for *CADRW* is dominated by

$$(2n)^{r\cdot 2^{r+E}}\,m^{2^{r+F}}\,d^L\quad .$$

What can be said about the values of J, K, and L? Table 6.1.1 lists computing time bounds for the main subalgorithms used in the extension phase of *CADRW*. A reference is provided for every bound listed, except for the bounds for *NORMAL* and *SIMPLE* (derived by the author). Our

algorithm *NORMAL* is based upon the algorithm outlined on p. 168 of [COL75], and does not correspond exactly with the algorithm *NORMAL* in [LOO82a]. The major component of our *NORMAL* algorithm is a resultant computation. The bound given for *SIMPLE* [LOO82a] is actually a bound for Step 4 of the algorithm only. However, it is stated in [LOO82a] that empirical evidence suggests Step 4 is the most time-consuming step.

Theorem 6.1.10: Assume $J = 7$, $K = 21$, and $L = 3$. Then the total time for the extension phase of *CADRW* is dominated by

$$(2n)^{r.2^{r+7}} m^{2^{r+4}} d^3 \ .$$

Theorem 6.1.11: Assume $J = 7$, $K = 21$, and $L = 3$. Then the total time for *CADRW* is dominated by

$$(2n)^{r.2^{r+7}} m^{2^{r+4}} d^3 \ .$$

We can compare our computing time bound for *CADRW* with that obtained for the algorithm *DECOMP* of [COL75] (see Theorem 16 of this reference). The exponents of m and d are (almost) the same in both cases, but the exponent of $2n$ in regard to *CADRW* is $r.2^{r+7}$, compared with an exponent of 2^{2r+8} in regard to *DECOMP*. Setting $u = 2^r$ and ignoring constant factors, the former exponent is $u \log u$, while the latter is u^2.

Algorithm	Bound	Source
APGCD	$\nu^9\delta^2$	[RUB73], Sec. 5.2
IPBASIS	$\mu^3\nu^8\delta^2$	Lemma 6.1.3
IPFAC	$\nu^{12}\delta^3$	[KAL82]
IPRRI	$\mu^7\nu^8\delta^3$	[COL75], p. 165
NORMAL	$\nu^8\delta^2$	
SIMPLE	$\nu^{21}\delta^2$	

Table 6.1.1. Computing time bounds
for algebraic algorithms

6.2 Empirical observations

In this section we discuss the performance of the new clustering cad algorithms presented in Section 5.3. The modified clustering cad algorithms for the plane and for three-space, *CLCSO* 2 and *CLCSO* 3, have been implemented in the SAC-2 computer algebra system. We have applied the SAC-2 versions of *CLCSO* 2 and *CLCSO* 3 to a number of examples, and present here some observations relating to four of the more interesting examples. The four subsections *A* to *D* that follow each contain a discussion of one example.

The computing times reported in this section were measured on a VAX 11/780 computer running the UNIX operating system. For convenience, we will not distinguish, throughout this section, between an algorithm and its SAC-2 implementation.

A. The tacnode

The following equation defines a *tacnode* ([WAL50], p.58):

$$F(x,y) = y^4 - 2y^3 + y^2 - 3x^2y + 2x^4 = 0.$$

Figure 6.2.1 is a sketch of the curve. Figure 3.1.1 illustrates a cad D of the plane which is sign-invariant with respect to F. Arnon [ARN81] reports that the ordinary cad algorithm (i.e. the algorithm *CAD* from Section 3.1 of this thesis) takes 1508 seconds to construct D, whereas the *sign*-invariant clustering cad algorithm (i.e. the algorithm *CLCAD*2 of [ARN81]) takes 107 seconds to construct D and to form sign-invariant clusters. The clustering algorithm takes less time than the ordinary algorithm because it does not construct a sample point for every cell of D. The sign-invariant clusters produced by the clustering algorithm are the curve itself and the connected components of its complement (Fig. 6.2.1).

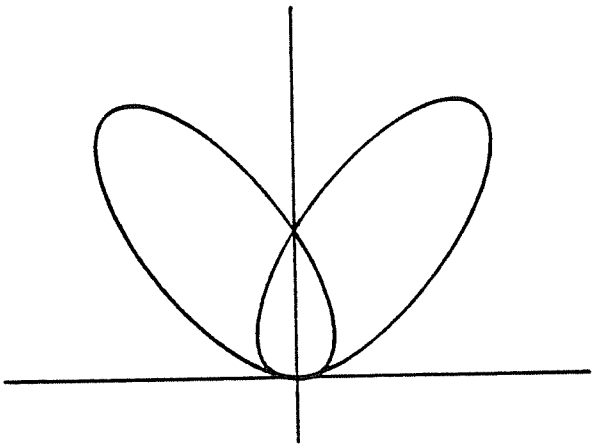

Fig. 6.2.1. Tacnode.

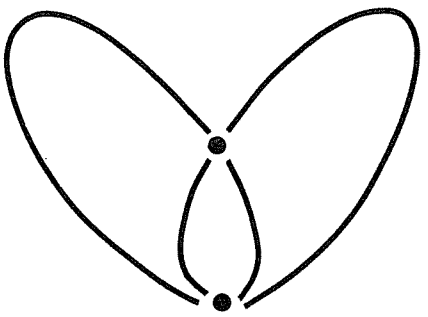

Fig. 6.2.2. Smooth, order-invariant clusters for tacnode.

The order-invariant clustering cad algorithm *CLCSO*2 takes approximately 156 seconds (on average) to construct D and to form smooth, order-invariant clusters. The clusters produced by this algorithm are depicted in Figure 6.2.2.

B. *The Whitney umbrella*

The equation $F(x,y,z) = z^2 - xy^2 = 0$ defines a surface in 3-space known as the Whitney umbrella. Figure 6.2.3 is a sketch of the surface. Note that the entire x-axis is contained in the surface: the negative portion of the x-axis forms the "handle" of the umbrella.

The order-invariant clustering algorithm *CLCSO*3 takes approximately 24 seconds to construct smooth, order-invariant clusters in 3-space. These clusters are depicted in Figure 6.2.4: there is one 0-cluster, two 1-clusters,

two 2-clusters, and three 3-clusters, a total of eight clusters. Note that these clusters are not maximal, as the entire x-axis is a smooth, connected set in which the order of F is everywhere two.

Arnon's algorithm takes about 17 seconds to construct sign-invariant clusters in 3-space. The entire surface is such a cluster: thus, the number of sign-invariant clusters is four. As the full projection of the input set $\{F\}$ is essentially the same as the reduced projection of $\{F\}$, it is not surprising that the order-invariant clustering algorithm runs no faster than Arnon's clustering algorithm.

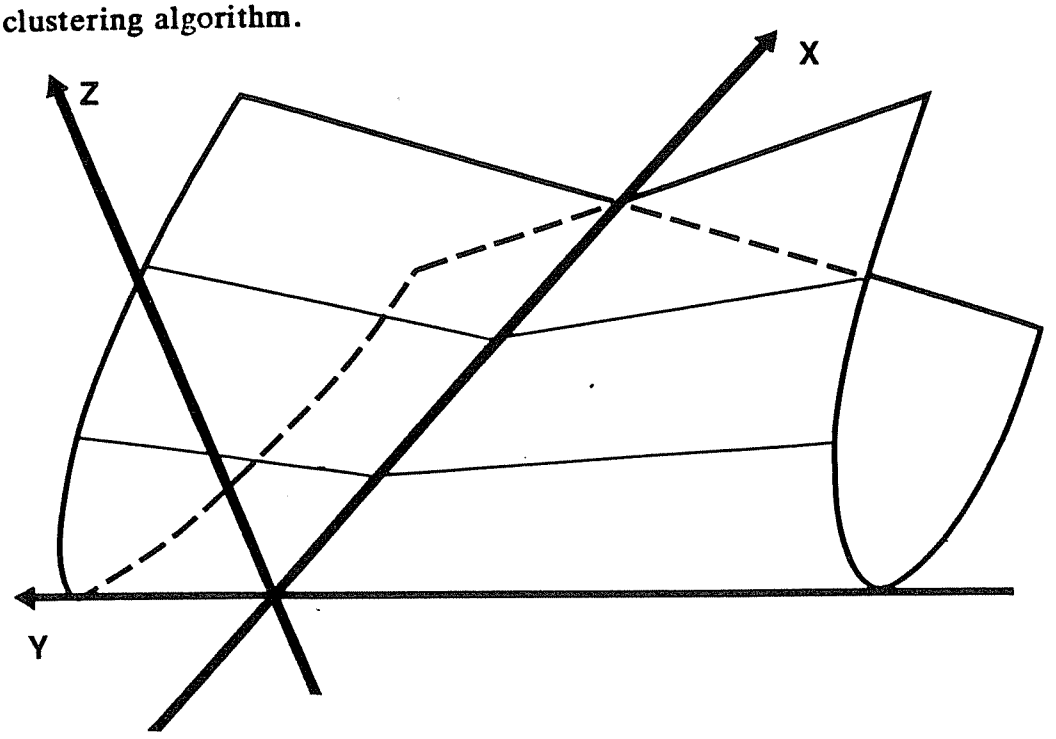

Fig. 6.2.3. Whitney umbrella.

C. *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

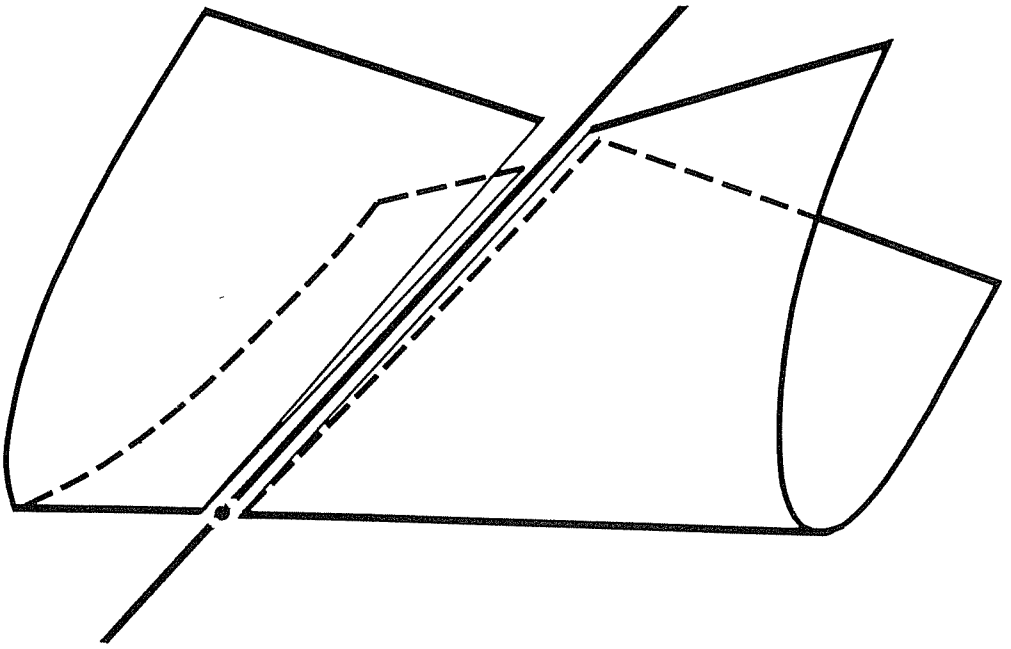

Fig. 6.2.4. Smooth, order-invariant clusters
for Whitney umbrella.

trivial application of the cad algorithm. However, we can make an interesting example for the algorithm by taking the two surfaces together (that is, taking the input set to be $A = \{F, G\}$).

The reduced projection of A consists of the following bivariate polynomials: the discriminant of F (a quadratic polynomial), the discriminant of G (a cubic), and the resultant of F and G (a sextic). The three curves defined by these equations are depicted in Figure 6.2.5 (curve 1 is $discr(F) = 0$, curve 2 is $discr(G) = 0$, and curve 3 is $res(F, G) = 0$; note that curve 3 has an isolated point on the x-axis). The order-invariant clustering algorithm takes 1,170 seconds, or about 20 minutes, to construct a smooth, order-invariant cad of the plane, and to form smooth, order-invariant clusters in the plane. The clusters formed are depicted in Figure 6.2.6: there are 11 0-clusters, 20 1-clusters, and 11 2-clusters, a total of 42. The 0-clusters are

presisely the singular points of the product of the bivariate polynomials (which defines the union of the curves 1,2 and 3).

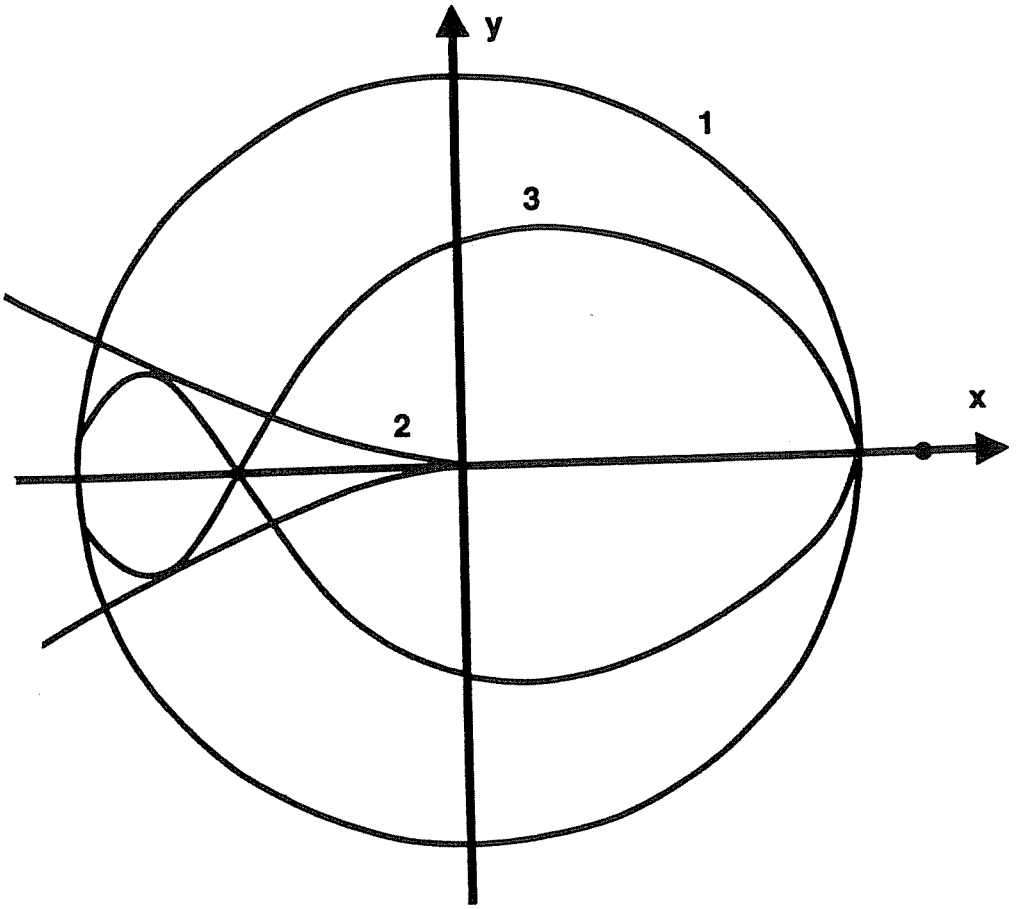

Fig. 6.2.5.
Let $F(x,y,z) = z^2+y^2+x^2-1$
and $G(x,y,z) = z^3+xz+y$. Then:
curve 1 is $discr(F) = 0$,
curve 2 is $discr(G) = 0$,
curve 3 is $res(F,G) = 0$.

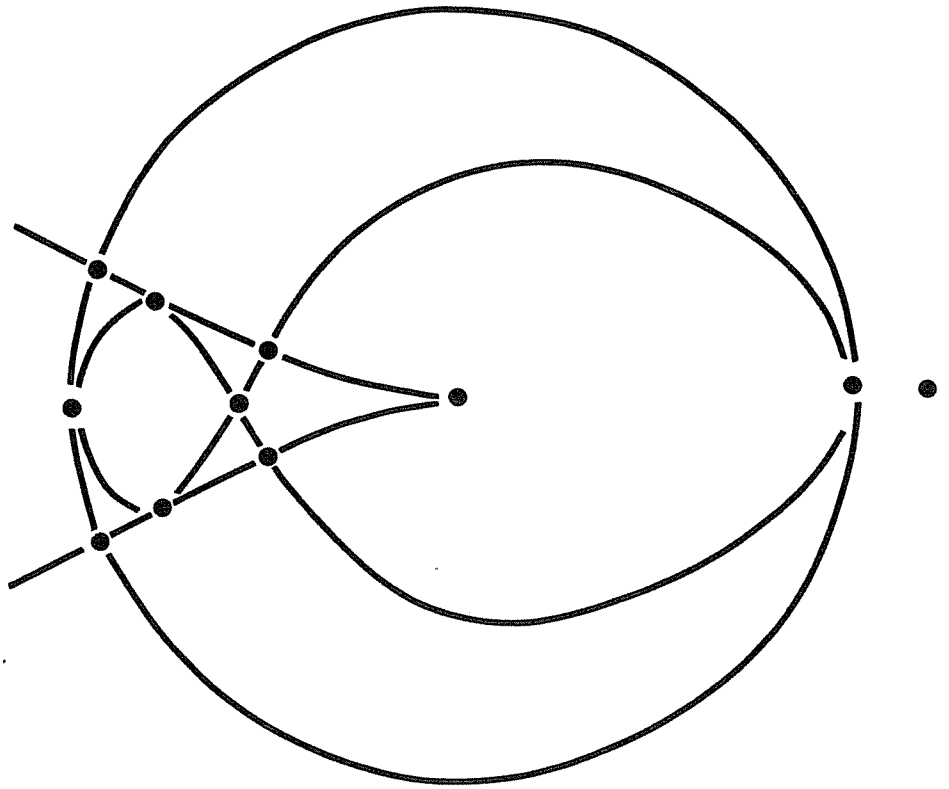

Fig. 6.2.6. Smooth, order-invariant clusters
for curves of Fig. 6.2.5.

The algorithm takes just under 9 hours in total to compute a smooth, A-order-invariant cad of 3-space, together with smooth, A-order-invariant clusters. There are 9 clusters altogether: a 1-cluster corresponding to the intersection of the sphere and the catastrophe surface, two 2-clusters comprising the rest of the sphere, two 2-clusters comprising the rest of the catastrophe surface, and four 3-clusters. These clusters are maximal, as expected (see remarks preceding Theorem 5.3.3). We can infer from the information provided by the algorithm that the intersection of the two surfaces is a compact, connected, 1-dimensional submanifold of $\mathbb{R}^3$ whose projection onto the x,y-plane (i.e., the 1-dimensional part of curve 3) is (topologically) a figure eight.

About 8 hours is spent on adjacency calculations in 3-space. This is perhaps not too surprising, when one considers that there are actually about 1,000 *cells* in the decomposition of 3-space (these cells are partitioned by the algorithm into just 9 clusters), and that an essentially complete list of all adjacencies between cells in 3-space is determined. We believe that there are at least two ways in which the time for the adjacency determination can be reduced. The first way is to reduce the number of pieces in the 3-space decomposition. It is plausible that one way this could be accomplished is by using sections and sectors over *clusters* in 2-space, as opposed to cells in 2-space, as the components of the clusters in 3-space. The second way is to use a more efficient 3-space adjacency algorithm. There is an adjacency algorithm in [MCC79] which only works over non-nullifying cells in the plane, but which we believe would run faster than the algorithm in use at the present time.

D. *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 between -2 and +2 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 algorithms *CLCAD* 3 and *CLCSO* 3. The full projection of A, as computed by *CLCAD* 3, is the set

$$P_1 = \{ldcf(F), discr(F), subdiscr_1(F), subdiscr_2(F), ldcf(G), discr(G)\},$$

where G is the reductum of F. The characteristics of these polynomials are summarized in Table 6.2.1. *CLCAD* 3 forms the univariate projection of P_1, and then performs a squarefree basis computation. The set U_1 of univariate basis polynomials obtained is described in Table 6.2.2. Note that U_1 contains 17 polynomials, the "worst" of which has degree 22, and maximum coefficient length (in decimal digits) 16:

$$4096\,X^{22} - 356096\,X^{21} + 14041856\,X^{20}$$

$$- 330249664\,X^{19} + 5114803328\,X^{18}$$

$$- 54149113904\,X^{17} + 390611881536\,X^{16} + \ldots$$

CLCAD 3 isolates the real roots of the polynomials in U_1. A total of 31 real roots is found, yielding an induced decomposition of the real line into

$2 \times 31 + 1 = 63$ cells. The computing times for the various subtasks of *CLCAD* 3 discussed so far are given in Table 6.2.3.

The reduced projection of A, as computed by *CLCSO* 3 is the set

$$P_2 = \{ldcf\ (F), discr\ (F), ldcf\ (G)\}.$$

After formation of the univariate projection of P_2, a univariate basis U_2 is formed. U_2 contains only 6 polynomials, the "worst" of which has degree 10 and maximum coefficient length 6 decimal digits:

$$X^{10} - 36X^9 + 540X^8 - 4212X^7 + 16875X^6$$

$$- 23679X^5 - 43659X^4 + 114669X^3$$

$$+ 96228X^2 - 58320X - 46656$$

The rest of the set U_2 is described in Table 6.2.2.

CLCSO 3 determines that the polynomials in U_2 have a total of 11 real roots. Thus the induced decomosition of the real line constructed by *CLCSO* 3 has $2 \times 11 + 1 = 23$ cells. The computing times for the various subtasks of *CLCSO* 3 are included in Table 6.2.3, for comparison with those of *CLCAD* 3.

Neither *CLCAD* 3 nor *CLCSO* 3 has yet run long enough to complete construction of the induced cad of the plane. *CLCSO* 3 used at least 13½ hours of CPU time on this computation before a system failure occurred.

The algorithm had almost finished determining the number of sections and sectors over each cell in 1-space, and was thus probably quite near finishing when it stopped.

The most expensive calculations appear to be those involving the two real algebraic numbers which are roots of the unique ten-ic $T(x)$ in U_2 ($T(x)$ is given above). In particular, where α_2 is the unique root of $T(x)$ in the interval $(-\frac{5}{4},-\frac{9}{8})$, the time t_2 to isolate the real roots of the algebraic polynomials $D(\alpha_2,y)$, with D an element of the basis for P_2, is about 6 hours (this includes the time to compute a squarefree basis for the set of algebraic polynomials $D(\alpha_2,y)$). This compares with a time t_1 of approximately 20 minutes for a similar computation for the real algebraic number α_1, the unique root of the polynomial $Q(x) = 16x^4 - 95x^3 + 24x^2 + 704x + 512$ (an element of U_2) in the interval $(-2,-\frac{3}{2})$.

Theory and experience with the algorithm suggest that the remaining algebraic number calculations (primitive element computations, for example) in *CLCSO*3 run quite quickly (see introduction to Chapter 6 of [ARN81]). The adjacency computations in the plane do not involve any algebraic number calculations and hence should proceed quite rapidly. Hence, we estimate that the total time for *CLCSO*3 to compute the induced cad of the plane is about 14 hours.

As a comparison, we shall attempt to estimate the total time for *CLCAD*3 to compute the induced cad of the plane. Now the univariate basis U_1 contains a polynomial $V(x)$ of degree 21, whose norm-length $L(|V|_1)$ is at least 39. Let α_3 be a real root of $V(x)$, and let t_3 be the time to isolate

the roots of the set of $D(\alpha,y)$, such that D is an element of the basis for P_1.

Let us assume that the root isolation for the polynomials $D(\alpha,y)$, with D a basis polynomial for P_2, takes time proportional to $(n*)^p\ (d*)^q$, where $n*$ and $d*$ are respectively the degree and norm-length of the minimal polynomial for α. For the ten-ic $T(x)$, the values of $n*$ and $d*$ are roughly double their values for the quartic $Q(x)$. For the 21-ic $V(x)$, the values of $n*$ and $d*$ are roughly double their values for the tenic $T(x)$. Hence, we might expect the ratios t_3/t_2 and t_2/t_1 to be roughly the same. Thus, as t_2/t_1 is about 18, t_3 would be roughly 100. As there are at least 7 real roots defined by the 21-ic $V(x)$ or by the even "worse" 22-ic, the total time for *CLCAD* 3 to compute the induced cad of the plane would be about 700 hours.

It is very likely that most of the time taken for the root isolation of algebraic polynomials was spent on algebraic polynomial greatest common divisor computations. A monic prs algorithm ([RUB73], Sec. 5.3) was used for the gcd computations. It seems likely, however, that use of some modification of Rubald's modular subresultant gcd algorithm ([RUB73], Sec. 5.2), or some modular gcd algorithm based on the theory in [WRO76], could substantially reduce the time for root isolation of algebraic polynomials.

Composition of P_1				
poly	deg in x	deg in y	total deg	max coeff length
$ldcf\ (F)$	0	1	1	1
$discr\,(F)$	6	6	10	4
$subdiscr_1(F)$	4	4	7	3
$subdiscr_2(F)$	2	2	3	2
$ldcf\ (G)$	1	0	1	1
$discr\,(G)$	4	4	7	2

Table 6.2.1. Composition of P_1.
(coefficient length in decimal digits)

Composition of U_1 and U_2				
	U_1		U_2	
degree	# polys	max coeff length	# 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 6.2.2. Composition of U_1 and U_2.
(coefficient length in decimal digits)

Computing times in seconds for subtasks		
	CLCAD 3	*CLCSO* 3
computation of basis for input	10.9	10.9
construction of bivariate proj	303	4.83
computation of bivariate basis	11.4	2.75
construction of univariate proj	246	114
computation of univariate basis	131	24.5
real root isolation	28.2	3.10
total	730	160

Table 6.2.3. Computing times in seconds for subtasks.

Chapter Seven

Conclusion

Let us summarize the work reported in this thesis. The work centers on the projection operation in the cylindrical algebraic decomposition algorithm. It is shown that in constructing a cad of Euclidean space, one can use a substantially reduced projection operation in place of that proposed originally. The validity of the simpler projection method rests upon a theorem on real polynomials and discriminants which is called the lifting theorem. This theorem is an adaptation to real n-space of a theorem due to Zariski pertaining to complex n-space. An exposition of Zariski's theorem, which is tailored to our application, is presented in the thesis.

A number of cad construction algorithms using the reduced projection are developed. The reduced projection operation finds its most staightforward use in the algorithm *CADRW* to construct a cad invariant with respect to a set of well-oriented polynomials. It is also shown how to use the reduced projection to construct a cad for a general set of polynomials. Clustering cad algorithms for the plane and 3-space using reduced projection are formulated.

The algorithm *CADRW* is subjected to a detailed theoretical analysis, from which an improved computing time bound is derived. $SAC-2$ implementations

of the clustering cad algorithms are applied to several examples, and empirical computing times reported.

What can be concluded from the theoretical and empirical analysis of the cad algorithms that use reduced projection? The theoretical computing time bound derived for *CADRW* is not as great as that obtained in [COL75] for the original cad algorithm. (The improvement in the bound consists essentially in a reduction of the exponent of n, the maximum degree of the input polynomials, from 2^{2r+8} to $r2^{r+7}$, where r is the number of variables.) The bound remains, however, doubly-exponential in r. (It seems likely that a bound of this kind is the best achievable for the cad algorithm - see p. 135 of [COL75]). For small values of r, the bound obtained for *CADRW* (as well as the bound in [COL75]) is likely far too pessimistic.

A worst-case analysis of *CADR* (applicable in the non-well-oriented case) could not be expected to yield a lower bound than that in [COL75]. Although the reduced projection is used by *CADR*, the advantage is offset somewhat by the need to include additional polynomials in the input set.

The empirical computing times reported suggest that there is a (possibly considerable) advantage to be gained in using the reduced projection to compute a clustered cad of 3-space. Nevertheless, the cost of computing non-trivial examples remains high. Further reduction in computing time for the clustering cad algorithm would seem to hinge upon the development of a modular greatest common divisor algorithm for algebraic polynomials, and of a method by which the number of cells or pieces in the decomposition of 3-space could be reduced.

References

[ACM84a] **Arnon DS, Collins GE, McCallum S:** Cylindrical algebraic decomposition I: the basic algorithm, *SIAM J. Comp., 13,* 4 (1984), pp 865-n.

[ACM84b] **Arnon DS, Collins GE, McCallum S:** Cylindrical algebraic decomposition II: an adjacency algorithm for the plane, *SIAM J. Comp., 13,* 4, (1984), pp n+1-889.

[ARN81] **Arnon DS:** Algorithms for the geometry of semi-algebraic sets, Ph.D. thesis, Technical Report #436, Computer Science Dept., Univ. of Wisconsin, 1981.

[BUC56] **Buck RC:** *Advanced Calculus,* McGraw-Hill, 1956.

[BMA48] **Bochner S, Martin WT:** *Several Complex Variables,* Princeton Univ. Press, Princeton, 1948.

[BRT71] **Brown WS, Traub JF:** On Euclid's algorithm and the theory of subresultants, *J. ACM, 18* 4, (1971), pp-505-514.

[COH74] **Collins GE, Horowitz E:** The minimum root separation of a polynomial, *Math. Comp., 28,* 126, (1974), pp 589-597.

[COL71] **Collins GE:** The calculation of multivariate polynomial resultants, *J. ACM, 18,* 4, (1971), pp 515-532.

[COL75] **Collins GE:** Quantifier elimination for real closed fields by cylindrical algebraic decomposition, in *Second GI Conference on Automata Theory and Formal Languages,* vol. 33 of Lecture Notes in Computer Science, Springer-Verlag, Berlin, 1975, pp 134-183.

[GEL60] **Gelfond AO:** *Transcendental and algebraic numbers,* Dover, New York, 1960.

[GRO65] **Gunning RC, Rossi H:** *Analytic functions of several complex variables,* Prentice-Hall, Englewood Cliffs, 1965.

[HIL35] **Hilbert D:** *Mathematische Probleme, Gesammelte Abhandlungen,* Band 3, Springer, 1935.

[HIR76] **Hirsch MW:** *Differential topology,* Springer-Verlag, New York, 1976.

[JOH75] **John F:** *Partial differential equations,* Springer-Verlag, New York, 1975.

[KAH78] **Kahn PJ:** private communication to GE Collins, May 1978.

[KAL82] **Kaltofen E:** Polynomial factorization, in *Computing,* Supplementum 4: *Computer Algebra - Symbolic and Algebraic Computation,* Springer-Verlag, Vienna and New York, 1982.

[KAP52] **Kaplan W:** *Advanced calculus,* Addison-Wesley, Reading, 1952.

[KAP66] **Kaplan W:** *Introduction to analytic functions,* Addison-Wesley, Reading, 1966.

[LOO82a] **Loos RGK:** Computing in algebraic extensions, in *Computing,* Supplementum 4: *Computer Algebra - Symbolic and Algebraic Computation,* Springer-Verlag, Vienna and New York, 1982.

[LOO82b] **Loos RGK:** Generalized polynomial remainder sequences, in *Computing,* Supplementum 4: *Computer Algebra - Symbolic and Algebraic Computation,* Springer-Verlag, Vienna and New York, 1982.

[MCC79] **McCallum S:** Constructive triangulation of real curves and surfaces, M.Sc. thesis, Univ. of Sydney, 1979.

[MUE77] **Mueller F:** *Ein exacter Algorithmus zur nichtlinearen Optimierung fuer beliebige Polynome mit mehreren Veranderlichen,* Verlag Anton Hain, Meisenheim am Glan, 1978.

[MUN75] **Munkres J:** *Topology - a first course,* Prentice-Hall, Englewood Cliffs, 1975.

[MUS71] **Musser DR:** Algorithms for polynomial factorization, Ph.D. thesis, Univ. of Wisconsin Comp. Sci. Dept. Tech. Report No. 134, Sept. 1971.

[NEW] **Newton I:** *The mathematical works of Isaac Newton, Vol. 2,* (DT Whiteside, ed.), Johnson Reprint Corp., New York, 1967.

[RUB74] **Rubald CM:** Algorithms for polynomials over a real algebraic number field, Ph.D. thesis, Univ. of Wisconsin Comp. Sci. Dept. Tech. Report No. 206, Jan. 1974.

[TAR51] **Tarski A:** *A decision method for elementary algebra and geometry,* University of California Press, 1951 (second edn., rev.).

[WAL50] **Walker RJ:** *Algebraic curves,* Princeton Univ. Press, Princeton, 1950.

[WHI72] **Whitney H:** *Complex analytic varieties,* Addison-Wesley, Philippines, 1972.

[WRO76] **Weinberger PJ, Rothschild LP:** Factoring polynomials over algebraic number fields, *ACM Trans. Math. Software, 2,* 4, (1976), pp 335-350.

[ZAR35] **Zariski O:** *Algebraic surfaces,* Springer-Verlag, New York-Heidelberg-Berlin, 1935.

[ZAR65] **Zariski O:** Studies in equisingularity II, *Amer. J. Math.*, *87*, 4, (1965), pp 972-1006.

[ZAR75] **Zariski O:** On equimultiple subvarieties of algebroid hypersurfaces, *Proc. Nat. Acad. Sci. USA*, *72*, 4, (1975), pp 1425-1426.