

A numerical-symbolic algorithm for computing the multiplicity of a component of an algebraic set

Dan Bates* Chris Peterson† Andrew J. Sommese‡

Abstract

Let F_1, F_2, \dots, F_t be multivariate polynomials (with complex coefficients) in the variables z_1, z_2, \dots, z_n . The common zero locus of these polynomials, $V(F_1, F_2, \dots, F_t) = \{p \in \mathbb{C}^n \mid F_i(p) = 0 \text{ for } 1 \leq i \leq t\}$, determines an algebraic set. This algebraic set decomposes into a union of simpler, irreducible components. The set of polynomials imposes on each component a positive integer known as the multiplicity of the component. Multiplicity plays an important role in many practical applications. It determines roughly “how many times the component should be counted in a computation.” Unfortunately, many numerical methods have difficulty in problems where the multiplicity of a component is greater than one. The main goal of this paper is to present an algorithm for determining the multiplicity of a component of an algebraic set. The method sidesteps the numerical stability issues which have obstructed other approaches by incorporating a combined numerical-symbolic technique.

Keywords. Embedding, generic points, homotopy continuation, irreducible components, multiplicity, numerical algebraic geometry, polynomial system, primary decomposition

AMS Subject Classification. 65H10, 68W30

1 Introduction

Let F_1, F_2, \dots, F_t be multivariate polynomials (with complex coefficients) in the variables z_1, z_2, \dots, z_n . The common zero locus of these polynomials determines a geometric object, $V(F_1, F_2, \dots, F_t) = \{p \in \mathbb{C}^n \mid F_i(p) = 0 \text{ for } 1 \leq i \leq t\}$. An object defined in such a way as the zero locus of a set of polynomials is called an *affine algebraic set*. An affine algebraic set which cannot be decomposed as the union of two affine algebraic sets (neither of which is contained in the other) is

*Department of Mathematics, University of Notre Dame, Notre Dame, IN 46556 (dbates1@nd.edu, <http://www.nd.edu/~dbates1>) This author was supported by the Duncan Chair of the University of Notre Dame, the University of Notre Dame, NSF grant DMS-0410047 and the Arthur J. Schmitt Foundation

†Department of Mathematics, Colorado State University, Fort Collins, CO 80523 (peterson@math.colostate.edu, <http://www.math.colostate.edu/~peterson>). This author was supported by Colorado State University and NSF grant MSPA-MCS-0434351

‡Department of Mathematics, University of Notre Dame, Notre Dame, IN 46556 (sommese@nd.edu, <http://www.nd.edu/~sommese>). This author was supported by the Duncan Chair of the University of Notre Dame, the University of Notre Dame and NSF grant DMS-0410047

called an *affine variety*. Let $R = \mathbb{C}[z_1, z_2, \dots, z_n]$ denote the ring of polynomials in the variables z_1, z_2, \dots, z_n . Given the set of polynomials $\{F_1, F_2, \dots, F_t\} \subseteq R$, there is a set $\mathbf{I} \subseteq R$ defined by the rule: $H \in \mathbf{I}$ if and only if there exist multivariate polynomials G_1, G_2, \dots, G_t such that $H = F_1 G_1 + F_2 G_2 + \dots + F_t G_t$. A set generated in such a way is called a *finitely generated ideal*. We will use the notation $\mathbf{I} = (F_1, F_2, \dots, F_t)$ to denote the ideal generated by F_1, F_2, \dots, F_t .

Every polynomial in \mathbf{I} vanishes along the common zero locus of F_1, F_2, \dots, F_t . In other words, if $H \in \mathbf{I}$ then $H(p) = 0$ for every $p \in V(F_1, F_2, \dots, F_t)$. This establishes that $V(F_1, F_2, \dots, F_t) \subseteq V(\mathbf{I})$. Since $\{F_1, F_2, \dots, F_t\} \subseteq \mathbf{I}$, it is an easy exercise to show that $V(\mathbf{I}) \subseteq V(F_1, F_2, \dots, F_t)$. We have thus established that $V(\mathbf{I}) = V(F_1, F_2, \dots, F_t)$. In other words, the affine algebraic set determined by a set of polynomials is the same as the affine algebraic set determined by the ideal generated by the polynomials.

By definition, we have that if $H \in \mathbf{I}$ then $H(p) = 0$ for every $p \in V(\mathbf{I})$. However, if H is a general polynomial with $H(p) = 0$ for every $p \in V(\mathbf{I})$ then it may well occur that $H \notin \mathbf{I}$. A simple example that illustrates this phenomenon is provided by considering the single polynomial $F(z) = z^2$ (viewed as an element of $\mathbb{C}[z]$). It is clear that $V(F)$ consists solely of the origin in \mathbb{C}^1 . The ideal $\mathbf{I} = (z^2)$ consists of all polynomials which have z^2 as a factor. The function $G(z) = z$ vanishes at every point of $V(\mathbf{I})$ but is not an element of \mathbf{I} . In this particular case, membership in \mathbf{I} is determined by the conditions: $H \in \mathbf{I} \iff H(0) = 0$ and $H'(0) = 0$. In general, ideal membership requires that conditions are placed on both the zeroes of a function and on the zeroes of various partial derivatives of the function.

To account for the restrictions that ideal membership places on both the zeroes of a polynomial as well as the zeroes of various partial derivatives of a polynomial, it is useful to consider a larger class of geometric objects than determined by affine algebraic sets. This new class of geometric objects, from a practical point of view, is rich enough to capture the common features of a set of functions with respect to vanishing of the functions and with respect to vanishing of partial derivatives of the functions. Elements of this enlarged class of geometric objects are called *affine schemes*. Given any set of polynomials, we can construct an ideal \mathbf{I} , an affine algebraic set $V(\mathbf{I})$ and an affine scheme $\mathcal{S}(\mathbf{I})$. Varieties capture information about the zero set of a collection of polynomials. Schemes capture information about the zero set of a collection of polynomials as well as information about the zero sets of partial derivatives of the polynomials. An important property of a scheme is that $H \in \mathbf{I}$ if and only if it H satisfies all of the conditions imposed by $\mathcal{S}(\mathbf{I})$.

Schemes play a role in a number of practical applications. Unfortunately, numerical methods have difficulty in this arena and more research must be done to better understand their intricacies from a numerical point of view. For many applications and numerical computations, the most useful information that is contained in a set of polynomials can be extracted from the associated affine algebraic set. However, certain key applications and numerical computations are better understood from the point of view of affine schemes than from the point of view of affine algebraic sets.

One particular piece of information that we will focus on in this paper is the *multiplicity* of a component of an algebraic set imposed by a set of defining equations. Essentially, to each irreducible component of an affine algebraic set, one uses the defining set of polynomials to attach a positive integer that determines roughly “how many times the component should be counted in a computation.” For instance, the ideal $\mathbf{I} = (z^2)$ imposes a multiplicity of 2 on the zero locus of \mathbf{I} . From the viewpoint of numerical computation, multiplicity is well understood in the case of ideals defined by a single polynomial. The situation changes dramatically when considering systems of polynomial equations. Numerical methods tend to throw away much of the additional structure inherent in a polynomial system. This approach makes certain “algebraic” information numerically unstable. By combining numerical methods with ideas from symbolic computation, algebraic structures become stable under small perturbations and can be computed. The main goal of this paper is to demonstrate this phenomenon in a combined numerical-symbolic technique for determining the multiplicity of a component of an algebraic set as imposed by a system of defining equations.

In [5], Dayton and Zeng study the multiplicity structures of polynomial systems. They provide an algorithm which yields as output the multiplicity of isolated solutions. This is done by counting how many partial derivatives of the polynomials are forced to be zero. Both their algorithm and the algorithm presented in the present paper yield multiplicity information (in addition to other invariants). However, the two techniques are different both in the specific calculations involved and in the nature of the calculations. The present paper is inspired, to a large degree, by certain Grobner basis calculations coupled with a fundamental result of Bayer and Stillman on regularity [2]. The paper of Dayton and Zeng is inspired, to a large degree, by Macaulay’s inverse systems approach. We would like to thank the authors of [5] for providing us with an early copy of their excellent paper.

2 Background

The following paragraphs give a brief outline of the vocabulary and tools we will be using throughout the paper. All definitions, propositions and theorems can be found in expanded detail in [4, 7, 8].

Let \mathbb{C} denote the field of complex numbers. Consider the ring of polynomials $R = \mathbb{C}[z_1, z_2, \dots, z_n]$. As a set, R consists of all polynomials in the variables z_1, z_2, \dots, z_n with complex coefficients.

Definition 1. *A subset $I \subset R = \mathbb{C}[z_1, z_2, \dots, z_n]$ is an ideal if*

$$(i) \ 0 \in I$$

$$(ii) \ F, G \in I \implies F + G \in I$$

$$(iii) \ F \in I \text{ and } G \in R \implies FG \in I$$

Definition 2. Let $R = \mathbb{C}[z_1, z_2, \dots, z_n]$. Let F, G be arbitrary elements in R . Let I be an ideal in R .

- I is **prime** if $FG \in I \implies F \in I$ or $G \in I$.
- I is **primary** if $FG \in I \implies F \in I$ or $G^m \in I$ for some m .
- I is **radical** if $F^m \in I \implies F \in I$.
- The **radical of I** is the set $\sqrt{I} = \{F \in R \mid F^m \in I \text{ for some } m\}$.
- I is a **radical ideal** if $I = \sqrt{I}$.

It should be noted that \sqrt{I} is an ideal, that every prime ideal is a radical ideal and that the radical of a primary ideal is a prime ideal. If I is a primary ideal and if $\mathfrak{p} = \sqrt{I}$ then I is said to be \mathfrak{p} -primary. An ideal, I , is *finitely generated* if there exists a finite list of elements $F_1, F_2, \dots, F_r \in I$ such that every element in I can be written as an R -linear combination of F_1, F_2, \dots, F_r . In other words, if

$$I = \{F_1G_1 + F_2G_2 + \dots + F_rG_r \mid G_1, G_2, \dots, G_r \in R\}.$$

We will denote this by $I = (F_1, F_2, \dots, F_r)$. A fundamental theorem concerning *Noetherian* rings has the following consequence in the setting of polynomial rings:

Theorem 3. (Hilbert Basis Theorem) Every ideal in $\mathbb{C}[z_1, z_2, \dots, z_n]$ is *finitely generated*.

Projective n -space over \mathbb{C} , written \mathbb{P}^n , is defined to be the set of lines through the origin in \mathbb{C}^{n+1} . Any non-zero point $\mathbf{z} = (z_1, z_2, \dots, z_{n+1}) \in \mathbb{C}^{n+1}$ determines a line through the origin: $L_{\mathbf{z}} = \{(\lambda z_1, \lambda z_2, \dots, \lambda z_{n+1}) \in \mathbb{C}^{n+1} \mid \lambda \in \mathbb{C}\}$. We will define two points $\mathbf{x}, \mathbf{y} \in \mathbb{C}^{n+1} \setminus (0, 0, \dots, 0)$ as equivalent if $L_{\mathbf{x}} = L_{\mathbf{y}}$. Thus \mathbf{x} and \mathbf{y} are equivalent if and only if there exists a $\lambda \in \mathbb{C}^*$ such that $\mathbf{x} = \lambda \mathbf{y}$. With this definition of equivalence of points, we obtain an equivalence relation on the points in $\mathbb{C}^{n+1} \setminus (0, 0, \dots, 0)$. Points in \mathbb{P}^n are in one to one correspondence with the equivalence classes of points in $\mathbb{C}^{n+1} \setminus (0, 0, \dots, 0)$. Let $R = \mathbb{C}[z_1, z_2, \dots, z_{n+1}]$. An element $F \in R$ is said to be *homogeneous* if every term of F has the same degree. An ideal is said to be homogeneous if it has a set of generators all of which are homogeneous. Let $\mathbf{z} \in \mathbb{C}^{n+1}$. If $F \in R$ is a homogeneous polynomial and $F(\mathbf{z}) = 0$ then $F(\lambda \mathbf{z}) = 0$ for every $\lambda \in \mathbb{C}$ thus F vanishes on the equivalence class of \mathbf{z} . In other words, F vanishes on a point in \mathbb{P}^n . Thus, to say that $F(\mathbf{z}) = 0$ when \mathbf{z} is a point in \mathbb{P}^n means that $F(p) = 0$ for every p in the equivalence class of \mathbf{z} . We will frequently use the notation $[z_1 : z_2 : \dots : z_{n+1}]$ to denote the point in \mathbb{P}^n corresponding to the equivalence class of $(z_1, z_2, \dots, z_{n+1})$ in $\mathbb{C}^{n+1} \setminus (0, 0, \dots, 0)$.

Definition 4. Let $U \subset R = \mathbb{C}[z_1, z_2, \dots, z_{n+1}]$, let $T \subset \mathbb{C}^{n+1}$ and let $T' \subset \mathbb{P}^n$.

- Define $V(U) = \{\mathbf{z} \in \mathbb{C}^{n+1} \mid F(\mathbf{z}) = 0 \text{ for every } F \in U\}$.

- Define $V_h(U) = \{\mathbf{z} \in \mathbb{P}^n \mid F(\mathbf{z}) = 0 \text{ for every } F \in U\}$.
- Define $I(T) = \{F \in R \mid F(\mathbf{z}) = 0 \text{ for every } \mathbf{z} \in T\}$.
- Define $I_h(T') = \{F \in R \mid F(\mathbf{z}) = 0 \text{ for every } \mathbf{z} \in T'\}$

With these definitions we have operations that associate geometric objects to algebraic objects and operations that associate algebraic objects to geometric objects. In particular, the operation $I(-)$ (resp. $I_h(-)$) takes as input a subset of \mathbb{C}^{n+1} (resp. \mathbb{P}^n) and produces a subset of R . The operation $V(-)$ (resp. $V_h(-)$) takes as input a subset of R and produces a subset of \mathbb{C}^{n+1} (resp. \mathbb{P}^n).

Definition 5. A subset $T \subset \mathbb{C}^n$ is called an **affine algebraic set** if $T = V(U)$ for some subset $U \subset \mathbb{C}[z_1, z_2, \dots, z_n]$. A subset $T \subset \mathbb{P}^n$ is called a **projective algebraic set** if $T = V_h(U)$ for some subset $U \subset \mathbb{C}[z_1, z_2, \dots, z_{n+1}]$.

We summarize some of the basic properties of the tools introduced thus far in the following proposition:

Proposition 6. For any subset $T \subset \mathbb{C}^{n+1}$ (resp. $T' \subset \mathbb{P}^n$) and for any subset $U \subset \mathbb{C}[z_1, z_2, \dots, z_{n+1}]$,

- (i) $I(T)$ is a radical ideal. $I_h(T')$ is a homogeneous radical ideal.
- (ii) $T \subseteq V(I(T))$ with equality if and only if T is an affine algebraic set. $T' \subseteq V_h(I_h(T'))$ with equality if and only if T' is a projective algebraic set.
- (iii) $U \subseteq I(V(U))$ with equality if and only if U is a radical ideal. $U \subseteq I_h(V_h(U))$ with equality if and only if U is a homogeneous radical ideal.
- (iv) If U is an ideal then $I(V(U)) = \sqrt{U}$. If U is a homogeneous ideal then $I_h(V_h(U)) = \sqrt{U}$.

We will use the word *algebraic set* to refer to both affine algebraic sets and projective algebraic sets. An algebraic set, V , is said to be *reducible* if it is possible to write $V = V_1 \cup V_2$ with V_1, V_2 algebraic sets and with $V \neq V_1$ and with $V \neq V_2$. Algebraic sets which are not reducible are called *irreducible*. Irreducible algebraic sets are called *varieties*. Algebraic sets, varieties, ideals and radical ideals have nice decomposition properties and relationships that are summarized as follows:

Proposition 7. *Decomposition properties:*

- Every algebraic set can be written uniquely as the union of a finite number of varieties, none of which are a subset of another.
- Every (homogeneous) radical ideal can be written uniquely as the intersection of a finite number of (homogeneous) prime ideals none of which are contained in another.

- Every (homogeneous) ideal can be written as the intersection of a finite number of (homogeneous) primary ideals.
- If V is an affine variety then $I(V)$ is a prime ideal. If V is a projective variety then $I_h(V)$ is a homogeneous prime ideal.
- If I is a primary ideal then $V(I)$ is an affine variety. If I is a homogeneous primary ideal then $V_h(I)$ is a projective variety.
- If $I = I_1 \cap I_2$ then $V(I) = V(I_1) \cup V(I_2)$. If $I = I_1 \cap I_2$ with I, I_1, I_2 homogeneous then $V_h(I) = V_h(I_1) \cup V_h(I_2)$.

In the proposition above, we see that every ideal can be written as the intersection of a finite number of primary ideals. Something much stronger can be said.

Definition 8. Let I be an ideal and let $I = I_1 \cap I_2 \cap \cdots \cap I_t$ be a primary decomposition of I . Suppose I_i is \mathfrak{p}_i -primary for each i . The primary decomposition is called **reduced** if

- (i) $\mathfrak{p}_i \neq \mathfrak{p}_j$ whenever $i \neq j$.
- (ii) For each i , $\bigcap_{j \neq i} I_j \not\subseteq I_i$.

The prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_t$ are called *associated primes*. As defined, they depend on the choice of primary decomposition. However, the following proposition simplifies the situation and demonstrates that the set of associated primes play a more central role than it first appears.

Proposition 9. (Primary decompositions)

- Every ideal has a reduced primary decomposition.
- Any reduced primary decomposition of a given ideal has the same set of associated primes.
- A radical ideal has a unique reduced primary decomposition.
- The associated primes of the radical of an ideal are a subset of the associated primes of the ideal.

As a consequence of the proposition above, it makes sense to talk about the associated primes of an ideal (rather than the associated primes of a primary decomposition of an ideal). The associated primes of an ideal that are not associated primes of the radical of the ideal are called *embedded primes*. It should be emphasized that the proposition does not claim there is a *unique* reduced primary decomposition for a general ideal, it only claims that the associated primes are uniquely determined. To each ideal, I , we can associate a degree and a dimension, denoted $\deg(I)$ and $\dim(I)$ respectively. The degree and dimension of an ideal can be defined in terms of the *Hilbert Polynomial* of R/I . Precise definitions of these terms can be found in [4, 7, 8]. The degree function allows one to define the multiplicity of a primary ideal.

Definition 10. Let I be a \mathfrak{p} -primary ideal. The **multiplicity** of I at \mathfrak{p} is defined to be $\mu(I) = \deg(I)/\deg(\mathfrak{p})$.

Since multiplicity is defined as a fraction, it may at first seem a bit surprising that the following proposition is true.

Proposition 11. The multiplicity of any \mathfrak{p}_i -primary ideal is a positive integer.

The next proposition makes the definition that follows seem very natural.

Proposition 12. If \mathfrak{p}_i is not an embedded prime of I then the \mathfrak{p}_i -primary component that appears in any reduced primary decomposition of I is the same.

Definition 13. Let I be an ideal. If \mathfrak{p}_i is an associated prime of I but is not an embedded prime of I then the multiplicity of I at \mathfrak{p}_i is defined to be the multiplicity of the \mathfrak{p}_i -primary component of I at \mathfrak{p}_i .

Multiplicity arises very naturally in polynomial factorization. By the fundamental theorem of algebra, every univariate polynomial factors into a product of linear polynomials over \mathbb{C} . That is to say, if $F(z)$ is a polynomial in the single variable, z , then we can write $F(z) = A(z - c_1)^{d_1}(z - c_2)^{d_2} \dots (z - c_t)^{d_t}$ where A is a non zero complex number, c_1, c_2, \dots, c_t are distinct complex numbers and d_1, d_2, \dots, d_t are positive integers. Let $I = (F)$. Then $V(I)$ will be the set of points in \mathbb{C} corresponding to the roots of F (i.e. $V(I) = \{c_1, c_2, \dots, c_t\}$). The radical of I will be the ideal $\sqrt{I} = (G)$ where $G = (z - c_1)(z - c_2) \dots (z - c_t)$. The reduced primary decomposition of I is $I = ((z - c_1)^{d_1}) \cap ((z - c_2)^{d_2}) \cap \dots \cap ((z - c_t)^{d_t})$. The associated primes of I are $(z - c_1), (z - c_2), \dots, (z - c_t)$. The associated primes of \sqrt{I} yield the same list, thus (F) has no embedded primes. By the previous definitions, (F) has multiplicity d_i at the prime ideal $(z - c_i)$ for each i .

In general, if F is a multivariate polynomial then F can be written as $F = AF_1^{d_1}F_2^{d_2} \dots F_t^{d_t}$ with A a nonzero constant, with each F_i an irreducible polynomial and with each d_i a positive integer. Furthermore, the factorization can be made so that F_i is not a multiple of F_j whenever $i \neq j$. The (unique) reduced primary decomposition of (F) is $(F) = (F_1^{d_1}) \cap (F_2^{d_2}) \cap \dots \cap (F_t^{d_t})$. To each irreducible factor, F_i , there is associated a variety, $V(F_i)$. $V(F)$ is the union of these varieties. $(F_i^{d_i})$ is a primary ideal with multiplicity d_i at (F_i) . (F) has multiplicity d_i at (F_i) for each i . If F itself is irreducible then the ideal $I = (F)$ is a prime ideal. In general, for ideals with more than one generator, the multiplicity of the ideal at a given prime ideal is rather subtle and requires a more thorough understanding of the degree function. Nevertheless, it arises naturally in a number of engineering problems, poses significant challenges to numerical computation and is often associated with slow convergence rates. The next section presents a few standard theorems from commutative algebra that will aid in the development of a numerical-symbolic algorithm to compute multiplicity. An overview of the main algorithm is also presented.

3 Theory for Algorithm

In the previous section, we saw that it makes sense to talk about the multiplicity of an ideal I at a prime ideal \mathfrak{p} provided \mathfrak{p} is not an embedded prime of I . Let I_i be a \mathfrak{p}_i -primary ideal appearing in a reduced primary decomposition of I where \mathfrak{p}_i is not an embedded prime of I . Let V_i be the variety associated to I_i . Let q be a general point on V_i . In this section we give an overview of an algorithm that takes as input the point q and the dimension, d_i of the variety V_i and produces as output the multiplicity of I at \mathfrak{p}_i . Let I_q be the prime ideal corresponding to the point, q . We reduce the problem to the computation of the multiplicity of an I_q -primary ideal. In order to do this, we first form the ideal, $J = (I, L_1, L_2, \dots, L_{d_i})$ where L_1, L_2, \dots, L_{d_i} are general linear forms in I_q . We show that J has an I_q -primary component, that I_q is not an embedded prime, and that the multiplicity of the I_q -primary component of J is the same as the multiplicity of the \mathfrak{p}_i -primary component of I . We then compute this multiplicity by a numerical-symbolic method. Throughout this section we will assume that all ideals are homogeneous. In order to make use of this simplifying assumption, we need a homogenization procedure for non-homogeneous polynomials and we need to understand the effect that this procedure has on multiplicity. All of the theorems and propositions found in this section are well known to experts. The proofs of these theorems go well beyond the scope of this paper. The presentation given in the following pages hopefully will aid the reader in understanding how these well known theorems can be used to produce the algorithm given in the next section.

Definition 14. *Let $F \in \mathbb{C}[z_1, z_2, \dots, z_n]$. The homogenization of F with respect to z_{n+1} is defined to be the element*

$$F^h = z_{n+1}^{\deg(F)} F\left(\frac{z_1}{z_{n+1}}, \frac{z_2}{z_{n+1}}, \dots, \frac{z_n}{z_{n+1}}\right) \in \mathbb{C}[z_1, z_2, \dots, z_{n+1}].$$

Example 15. *Let $F = x^2 + y^3 + 1 \in \mathbb{C}[x, y]$. The homogenization of F with respect to z is*

$$F^h = z^3 F\left(\frac{x}{z}, \frac{y}{z}\right) = (z^3) \left(\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^3 + 1 \right) = x^2 z + y^3 + z^3.$$

Proposition 16. *(Multiplicity unaffected by homogenization)*

Let $F_1, F_2, \dots, F_t \in \mathbb{C}[z_1, z_2, \dots, z_n]$. Let F^h denote the homogenization of F with respect to z_{n+1} . Let $q = (q_1, q_2, \dots, q_n) \in \mathbb{C}^n$ and let $q' = [q_1 : q_2 : \dots : q_n : 1] \in \mathbb{P}^n$. The multiplicity of (F_1, F_2, \dots, F_t) at I_q is equal to the multiplicity of $(F_1^h, F_2^h, \dots, F_t^h)$ at $I_{q'}$.

The next theorem allows us to reduce a general multiplicity computation to the multiplicity of a zero-dimensional object.

Theorem 17. *(Multiplicity preserved by general hyperplane sections)*

Let I be a homogeneous ideal. Let \mathfrak{p} be a non-embedded, associated prime of I . Let $V_h(\mathfrak{p})$ be the projective variety associated to \mathfrak{p} . Let q be a general

point on $V_h(\mathfrak{p})$ and let $D = \text{Dim}(V_h(\mathfrak{p}))$. Let I_q be the homogeneous prime ideal associated to the point q . Let L_1, L_2, \dots, L_D be general linear forms in I_q . Let $J = (I, L_1, L_2, \dots, L_D)$. Then

- (i) I_q is an associated prime of J .
- (ii) I_q is not an embedded prime of J .
- (iii) The multiplicity of J at I_q is equal to the multiplicity of I at \mathfrak{p} .

Definition 18. Let $R = \mathbb{C}[z_1, z_2, \dots, z_n]$. The **maximal ideal of R** is the ideal $\mathfrak{m} = (z_1, z_2, \dots, z_n)$.

It should be noted that if I is an \mathfrak{m} -primary ideal then $V(I)$ is the origin while $V_h(I)$ is the empty set! If I is a homogeneous ideal whose associated projective variety is a single point, q , then I_q is a non-embedded, associated prime of I . It does not necessarily follow that I is I_q primary. A reduced primary decomposition of I may still contain an \mathfrak{m} -primary component. In other words, \mathfrak{m} may be an embedded prime. In any case, the computation of the multiplicity of I at I_q is aided by the following theorem but first we need to define some notation.

Definition 19. Let I be a homogeneous ideal in $R = \mathbb{C}[z_1, z_2, \dots, z_n]$. The k^{th} **homogeneous part of I** is defined to be the set of all elements of I which are homogeneous of degree k . It is denoted $(I)_k$ and is a finite dimensional vector space over \mathbb{C} . Note that $(R)_k = (\mathfrak{m}^k)_k$.

Theorem 20. (Multiplicity of a homogeneous ideal supported at a point)

Let q be a point in \mathbb{P}^n . Let I be a homogeneous ideal with $V_h(I) = q$. Let $R = \mathbb{C}[z_1, z_2, \dots, z_{n+1}]$. The multiplicity of I at I_q is the dimension of $(R/I)_d$ as a \mathbb{C} -vector space for $d \gg 0$. Furthermore, if I is I_q -primary then the multiplicity of I at I_q is the dimension of $R/(I, L)$ as a \mathbb{C} -vector space where L is a general, homogeneous linear form in R .

The next proposition relates the multiplicity of a homogeneous ideal supported at a point to the regularity of the ideal. For the definition and some of the basic theorems concerning regularity, see [2, 6, 11]. For the purposes of this paper, it suffices to make the following connection between regularity and multiplicity.

Proposition 21. (Regularity and multiplicity)

Let q be a point in \mathbb{P}^n . Let I be a homogeneous ideal with $V(I) = q$. Let $R = \mathbb{C}[z_1, z_2, \dots, z_{n+1}]$. The dimension of $(R/I)_d$ as a \mathbb{C} -vector space is equal to the dimension of $(R/I)_{d+1}$ as a \mathbb{C} -vector space for all d greater than or equal to the regularity of I .

The algorithm that we develop utilizes the previous theorem and proposition. In order to use these tools, we need a method for computing the regularity of an ideal. This will provide us with a stopping criterion in the computation of the dimension of $(R/I)_d$.

Definition 22. Let $R = k[x_1, x_2, \dots, x_n]$. An element $h \in R$ is **generic** for I if h is not a zero-divisor on R/I^{sat} . If $\dim(R/I) = 0$ then every $h \in S$ is generic for I . For $j > 0$, define $U_j(I)$ to be the subset $\{(h_1, h_2, \dots, h_j) \in R_1^j \mid h_i \text{ is generic for } (I, h_1, h_2, \dots, h_{i-1}), 1 \leq i \leq j\}$.

Definition 23. Let I be an ideal and let F be an element of $R = k[x_1, x_2, \dots, x_n]$. The **ideal quotient** of I by F is defined to be $(I : F) = (\{G \in R \mid GF \in I\})$.

With these definitions in place, we can now state the following crucial theorem of Bayer and Stillman [2].

Theorem 24. (*Criterion for m -regularity*)

Let k be an infinite field and let $R = k[x_1, x_2, \dots, x_n]$. Let $I \subset R$ be a homogeneous ideal generated in degree at most m . The following conditions are equivalent:

1. I is m -regular.

2. There exists $h_1, h_2, \dots, h_j \in R_1$ for some $j \geq 0$ such that

$$((I, h_1, h_2, \dots, h_{i-1}) : h_i)_m = (I, h_1, h_2, \dots, h_{i-1})_m \quad \text{for } i = 1, 2, \dots, j$$

$$\text{and } (I, h_1, h_2, \dots, h_j)_m = R_m.$$

3. Let $r = \dim(R/I)$. For all $(h_1, h_2, \dots, h_r) \in U_r(I)$, and all $p \geq m$,

$$((I, h_1, h_2, \dots, h_{i-1}) : h_i)_p = (I, h_1, h_2, \dots, h_{i-1})_p \quad \text{for } i = 1, 2, \dots, r$$

$$\text{and } (I, h_1, h_2, \dots, h_r)_p = R_p.$$

Furthermore, if h_1, h_2, \dots, h_j satisfy condition 2 then $(h_1, h_2, \dots, h_j) \in U_j(I)$.

Corollary 25. (*Stopping Criterion for regularity computation*)

Let I be a homogeneous ideal which is generated in degree at most k . Suppose $V_h(I)$ is a single point $q \in \mathbb{P}^n$. Let L be a linear form which is not contained in I_q . The regularity of I is less than or equal to k if and only if $(I : L)_k = (I)_k$ and if $(I, L)_k = (R)_k$.

Proof. The corollary follows immediately from the theorem of Bayer and Stillman under the assumption that I defines a zero dimensional scheme. \square

Theorem 26. (*Convergence of multiplicity at an isolated point*)

Let \mathbf{p} be a point in \mathbb{P}^n . Suppose $I_{\mathbf{p}}$ is an associated, non embedded prime of an ideal I . Let $J_k = (I, I_{\mathbf{p}}^k)$. Then the multiplicity of I at $I_{\mathbf{p}}$ is equal to the multiplicity of J_k at $I_{\mathbf{p}}$ for $k \gg 0$.

Proposition 27. (*Persistence of multiplicity in neighborhood of a point*)

If the multiplicity of J_k at $I_{\mathbf{p}}$ is equal to the multiplicity of J_{k+1} at $I_{\mathbf{p}}$ then the multiplicity of I at $I_{\mathbf{p}}$ is equal to the multiplicity of J_k at $I_{\mathbf{p}}$,

With the theorems in this section in place, it is now easy to describe the algorithm. This is done in the following section.

4 Algorithm and implementation details

In this section, the complete multiplicity algorithm is presented and several details of an implementation are discussed.

4.1 The algorithm

Recall that if \mathbf{I} is a homogeneous ideal, if \mathbf{p} is a point in \mathbb{P}^n and if $V_h(\mathbf{I}) = \mathbf{p}$ then the multiplicity of \mathbf{I} at $\mathbf{I}_{\mathbf{p}}$ is the same as the dimension of $(R/\mathbf{I})_k$ as a \mathbb{C} -vector space for sufficiently large k . Note that the dimension of $(R/\mathbf{I})_k$ is equal to $\dim(R)_k - \dim(\mathbf{I})_k$. When this is combined with the stopping criterion given in Corollary 25 we obtain:

Algorithm 1. *find_mult*($\{F_1, F_2, \dots, F_r\}, \mathbf{p}; \mu$)

Input: A set of homogeneous polynomials $\{F_1, F_2, \dots, F_r\} \subset \mathbb{C}[z_0, z_1, \dots, z_n]$ and an isolated point $\mathbf{p} = [p_0 : p_1 : \dots : p_n] \in \mathbb{P}^n$ of $V_h(F_1, F_2, \dots, F_r)$ with $\mathbf{p} \notin V_h(z_n)$.

Output: μ = the multiplicity of the ideal, (F_1, F_2, \dots, F_r) , at $\mathbf{I}_{\mathbf{p}}$.

Algorithm:

```

Form  $\mathbf{I}_{\mathbf{p}} := (\{p_i z_j - p_j z_i \mid 0 \leq i, j \leq n\})$ .
Form  $\mathbf{m} := (z_0, z_1, \dots, z_n)$ .
Let  $k := 1$ ,  $\mu(0) := 0$ , and  $\mu(1) := 1$ .
while  $\mu(k) \neq \mu(k-1)$  do
  Form  $\mathbf{I}_{\mathbf{p}}^k$ .
  Form  $\mathbf{J}_k := (\mathbf{I}, \mathbf{I}_{\mathbf{p}}^k)$ .
  Form  $\mathbf{m}^k$  and  $z_n \cdot \mathbf{m}^k$ .
  Let  $A := 0$  and  $B := 1$ .
  while  $A \neq B$  do
    Form  $(\mathbf{J}_k)_{k+1}$ .
    Compute  $\mathbf{P} := (\mathbf{J}_k)_{k+1} \cap z_n \cdot \mathbf{m}^k$ . (*)
    Compute the preimage  $\overline{\mathbf{P}} \subseteq (\mathbf{m})_k$  of  $\mathbf{P}$ . (**)
    Compute  $A := \text{rank}((\mathbf{J}_k)_k)$ .
    Compute  $B := \text{rank}(\overline{\mathbf{P}})$ .
    if  $A = B$  then let  $\mu(k) := \text{rank}((\mathbf{m})_k) - A$ , else let  $\mathbf{J}_k := \overline{\mathbf{P}}$ .
  if  $\mu(k) = \mu(k-1)$ , then  $\mu := \mu(k)$ , else let  $k = k + 1$ .

```

Two steps of this algorithm are of particular interest, so they have been marked with the symbols (*) and (**). Those two steps will be discussed in detail in the following section.

4.2 Details of the implementation

The algorithm, *find_mult*, has been implemented as a module of the Bertini software package, which is under development by the first and third authors

and Charles Wampler of GM Research and Development (with earlier work by Chris Monico of Texas Tech University). The Bertini package is written in C and allows for the use of arbitrarily high precision by making use of the MPFR multiprecision floating point library, although regular (16 digit) precision suffices for the examples described in the subsequent section.

The basic data structure used in the implementation is the one-dimensional array. Fixing a term order, every polynomial may be represented uniquely as a vector. Operations such as polynomial multiplication or the expansion of a homogeneous polynomial into a fixed degree via multiplication by an appropriate monomial basis is then a combinatorial manipulation.

The Bertini implementation of *find_mult* accepts as input a file containing the ideal with one polynomial per line, written in a format similar to that used by the Maple computer algebra system. A parser making use of the C libraries flex and bison is used to parse the ideal from the input file into a set of vectors. Most steps of *find_mult* are then straightforward, although the computation of the singular value decomposition of a matrix and steps (*) and (**) deserve some extra attention.

The singular value decomposition (SVD) algorithm is implemented as described in [17], and singular values of absolute value less than 10^{-8} are considered to be 0. In particular, a general complex matrix may be reduced to a bidiagonal complex matrix by left and right multiplication by unitary matrices formed from Householder reflectors. It is trivial to convert a complex bidiagonal matrix into a real bidiagonal matrix by multiplying by unitary matrices. Finally, an iterative method may be applied to any real bidiagonal matrix to produce a real diagonal matrix with the singular values on the diagonal, again using unitary matrices. Combining the left and right unitary matrices then yields the singular value decomposition. The rank of a matrix is then the number of its singular values that are nonzero. To check that such small singular values are actually 0, the SVD may again be computed, but at a higher level of precision. Then, those singular values which approach 0 at the higher precision may more safely be considered to be 0. Naturally, this checking procedure may continue *ad infinitum* for singular values that are exactly 0, so a threshold must ultimately be chosen. We have found that the threshold 10^{-8} was sufficient for the following examples.

Step (*) of *find_mult* involves the intersection of the degree $k + 1$ component of two graded ideals, a procedure that deserves some explanation. Since the degree $k + 1$ component of the each of the two ideals is represented as a vector space (with the generators representing bases), the intersection of the degree $k + 1$ component of the two graded ideals is equivalent to the intersection of two vector spaces, say V and W . Briefly, the left singular vectors of V and W corresponding to zero singular values form bases for V^\perp and W^\perp , respectively. Then, by concatenating these bases into a single matrix and computing the SVD of that matrix, the left singular vectors corresponding to the zero singular values form a basis for $(V^\perp \cup W^\perp)^\perp = V \cap W$. Step (**) is simply a matter of mechanically removing a factor of z_n from each polynomial of \mathbf{P} .

5 Computational experiments

For each example in this section, the ideal was run through the Bertini implementation of *find_mult* discussed in the previous section, on a single processor 3 GHz Pentium 4 machine running Linux. To simplify parsing, all exact numbers were first converted to 16 digit floating point approximations. In each example, the invariants predicted by theory or computed symbolically were confirmed numerically.

5.1 Monomial ideals

Let I be a monomial ideal of the form $I = (M_1, M_2, \dots, M_N)$, with $M_i = z_1^{k_{i,1}} z_2^{k_{i,2}} \dots z_n^{k_{i,n}}$ (where the $k_{i,j}$ are nonnegative integers). Suppose $V(I) = (0, 0, \dots, 0)$ (or equivalently, that $V_h(I) = \emptyset$). Then the multiplicity of I at the prime ideal (z_1, z_2, \dots, z_n) is exactly the number of monomials that are not in I . This leads to the easily understood staircase counting method, as described in [4]. For example, the ideal $I = (x^5, y^5, x^2y^4, x^3y)$ in $\mathbb{C}[x, y]$ has multiplicity 16 at (x, y) since $\{1, x, y, x^2, xy, y^2, x^3, x^2y, xy^2, y^3, x^4, x^2y^2, xy^3, y^4, x^2y^3, xy^4\}$ is a full list of the monomials not in I . Using *find_mult*, this multiplicity was confirmed (by considering I as an ideal in $\mathbb{C}[x, y, z]$). The multiplicities of a large number of similar problems was also confirmed by this method.

An upper bound on the multiplicity of a zero-scheme defined by a square ideal, i.e., an ideal with a generating set which possesses the same number of polynomials and variables, may be obtained via homotopy continuation by counting the number of solution paths converging to the point in question (see [15]). However, when considering a polynomial system with more equations than unknowns, this bound is generally much too high. It is therefore interesting to note that *find_mult* works for any zero-scheme, whether the ideal is square or not.

5.2 A nontrivial exact problem

Consider the ideal

$$I = (x^4 + 2x^2y^2 + y^4 + 3x^2yz - y^3z, x^6 + 3x^4y^2 + 3x^2y^4 + y^6 - 4x^2y^2z^2) \quad (1)$$

in $\mathbb{C}[x, y, z]$. This ideal is a homogenized form of an example discussed in [7]. As described in the book, the multiplicity of I at $I_{[0:0:1]}$ can be computed as the intersection number of the two generators of the ideal at $[0 : 0 : 1]$. Using the techniques described in that text, a hand calculation determines that the multiplicity of I at $I_{[0:0:1]}$ is 14. The multiplicity was confirmed numerically to be 14 via the Bertini implementation of *find_mult*.

5.3 A related inexact problem

Although symbolic algorithms for computing the previously mentioned multiplicities could easily handle either of the preceding examples, such techniques

cannot be applied if the input data is inexact. This is due to the fact that small perturbations in the generators of an ideal can have drastic effects on the (exact) zero locus of the generators.

For example, consider the following ideal in $\mathbb{C}[x, y, z]$,

$$I = (x^4 + 2x^2y^2 + y^4 + 3x^2yz - y^3z + .001z^4, x^6 + 3x^4y^2 + 3x^2y^4 + y^6 - 4x^2y^2z^2), \quad (2)$$

created by perturbing a single coefficient of (1) by 10^{-3} . A symbolic algorithm will compute the multiplicity of I at $I_{[0:0:1]}$ to be 0 (since $[0 : 0 : 1]$ is not a point on $V_h(I)$). However, *find_mult* reports that the multiplicity of the associated zero-scheme and Hilbert function are the same as those for (1). This is a consequence of the combined symbolic-numeric technique stabilizing the problem under small perturbations.

5.4 Another inexact problem

One difficulty that frequently arises when using symbolic techniques over \mathbb{Q} is *coefficient blowup*. If the defining equations of an ideal involves many different prime numbers, then the rational operations involved in the computation of a Gröbner basis leads to fractions whose numerator and denominator are arbitrarily large. For instance, an ideal involving five general homogeneous quartics in four variables with random integer coefficients between 0 and 100 had lexicographic Gröbner basis elements whose coefficients were fractions involving ratios of integers with over 200 digits! Frequently, a symbolic version of roundoff is done to prevent coefficient blowup. The computations are carried out with exact arithmetic but over a field with finite characteristic. There are settings in which this technique can lead to some uncertainty as to the meaning of the results. In the following example, symbolic techniques over \mathbb{Q} were used to determine the multiplicity at a certain prime. In carrying out this computation, some of the coefficients involved in the Gröbner basis computation reached 42 digits!

Consider the ideal in $\mathbb{Q}[w, x, y, z]$ generated by the following polynomials,

$$\begin{aligned} &3x^2 - y^2 - z^2 + 2yz - 12xw - \frac{1212}{161}yw + \frac{729}{161}zw + \frac{383678}{77763}w^2, \\ &x^3 - 8x^2w - 6xyw - 4y^2w + z^2w + \frac{1047}{63}xw^2 + \frac{117}{7}yw^2 - \frac{183}{23}zw^2 + \frac{2600452}{699867}w^3, \\ &z^3 + 4x^2w + 2xyw - \frac{102}{23}z^2w - \frac{415}{21}xw^2 - \frac{19}{3}yw^2 + \frac{5055}{529}zw^2 + \frac{12496664}{766521}w^3, \\ &x^2 - \frac{16}{3}xw + \frac{64}{9}w^2. \end{aligned}$$

This ideal was confirmed symbolically to have multiplicity 2 at the prime ideal corresponding to the point in projective space $[1 : \frac{8}{3} : -\frac{2}{7} : \frac{34}{23}]$. The example is a modified version of an example found in [16]. The modification involves slicing by x^2 and then applying a change of variables. Using *find_mult*, we have confirmed that the multiplicity of the zero-scheme is 2. This multiplicity information was obtained using a fairly meager amount of computational resources, and coefficient blowup was completely avoided.

6 Conclusions

A combined numerical-symbolic algorithm has been presented which allows multiplicity computations to be made in a numerical setting. Numerical stability issues have made the computation of multiplicity difficult in the past. The algorithm *find_mult* has been implemented as a module of the Bertini software package and several examples were presented to demonstrate the algorithm's stability under small perturbations.

In computing the multiplicity of an ideal at a point, we ended up also computing the regularity. One can use a bound on the regularity of an ideal to provide a stopping criterion for the computation of more subtle invariants of the ideal. For example, the regularity places an upper bound on the types of syzygies that may occur in a free resolution of the ideal and one may use this to produce the free resolution of the ideal. This leads to the ability to compute numerical cohomology as well as carry out other computations that depend on the matrices appearing in a free resolution.

One could improve *find_mult* by developing a more secure technique for determining how many singular values are zero. When determining which singular values of a matrix are zero via numerical methods, one is forced to choose a threshold below which a singular value is deemed to be zero. If one is dealing with inexact equations then there is a limit on the accuracy of the information obtained. If one can quantify the inaccuracy then reasonable thresholds can be determined. However, if one is dealing with exact equations, it is certainly possible that some singular values are very small but non-zero. One way to improve confidence is to compute the singular values at two levels of precision and then observe which move towards zero under higher precision. This is an approach which is satisfactory in many situations. However, there will always be problems that can be made which will fool the system. By starting with exact equations and then using numerical methods one is necessarily losing information. It will be important to quantify this in such a way as to improve confidence levels.

References

- [1] D. Bayer and D. Mumford. What can be Computed in Algebraic Geometry? *in: Computational algebraic geometry and commutative algebra (Cortona, 1991)*, 1–48, Symposium Math., XXXIV, Cambridge University Press, Cambridge, 1993.
- [2] D. Bayer and M. Stillman. A criterion for detecting m -regularity. *Invent. Math.* 87 (1987), 1–11.
- [3] D. Bini and G. Fiorentino. Design, analysis, and implementation of a multiprecision rootfinder. *Numer. Algorithms* 23 (2000), 127–173.
- [4] D. Cox, J. Little and D. O'Shea. *Ideals, Varieties, and Algorithms*, Second Edition. Undergraduate Texts in Mathematics, Springer, New York, 1996.

- [5] B. Dayton and Z. Zeng. Computing the multiplicity structure in solving polynomial systems. *Preprint*.
- [6] D. Eisenbud and S. Goto. Linear free resolutions and minimal multiplicity. *J. of Algebra* 88 (1984), 89–133.
- [7] W. Fulton. Algebraic Curves. W.A. Benjamin, New York, 1969.
- [8] R. Hartshorne. Algebraic Geometry. Graduate Texts in Mathematics 52, Springer, New York, 1977.
- [9] H. Kobayashi, H. Suzuki and Y. Sakai. Numerical calculation of the multiplicity of a solution to algebraic equations. *Math. Comp.* 67 (1998), 257–270.
- [10] H. Möller and H. Stetter. Multivariate polynomial equations with multiple zeros solved by matrix eigenproblems. *Numer. Math.* 70 (1995), 311–329.
- [11] D. Mumford. Lectures on curves on an algebraic surface. Princeton University Press, Princeton, New Jersey, 1966.
- [12] A. Sommese, J. Verschelde and C. Wampler. Numerical decomposition of the solution sets of polynomials into irreducible components. *SIAM J. Numer. Anal.* 38 (2001), 2022–2046.
- [13] A. Sommese, J. Verschelde and C. Wampler. A method for tracking singular paths with application to the numerical irreducible decomposition. Algebraic Geometry, 329–345, de Gruyter, Berlin, 2002.
- [14] A. Sommese, J. Verschelde and C. Wampler. Numerical factorization of multivariate complex polynomials. *Theor. Comp. Sci.* 315 (2004), 651–669.
- [15] A. Sommese and C. Wampler. The Numerical Solution to Systems of Polynomials Arising in Engineering and Science. World Scientific, Singapore, 2005.
- [16] H. Stetter. Numerical Polynomial Algebra. SIAM, 2004.
- [17] G.W. Stewart. Matrix Algorithms 1: Basic Decompositions. SIAM, 1998.
- [18] B. Sturmfels. Solving systems of polynomial equations. CBMS Regional Conference Board of the Mathematical Sciences, Washington, DC. By the American Mathematical Society, Providence, RI, 2002.
- [19] A. Wright. Finding all solutions to a system of polynomial equations. *Math. Comp.* 44 (1985), 125–133.
- [20] Z. Zeng. Algorithm 835: MultRoot—a Matlab package for computing polynomial roots and multiplicities. *ACM Trans. Math. Software* 30 (2004), 218–236.
- [21] Z. Zeng. Computing multiple roots of inexact polynomials. *Math. Comp.* 74 (2005), 869–903.