Numerical computation of the Hilbert function of a zero-scheme

Zachary A. Griffin∗ Jonathan D. Hauenstein† Chris Peterson‡ Andrew J. Sommese§

July 31, 2011

Abstract
Let \( R = \mathbb{C}[x_1, \ldots, x_N] \) and let \( F = \{f_1, \ldots, f_t\} \subset R \) be a set of generators for an ideal \( I \). Let \( Y = \{y_1, \ldots, y_\ell\} \subset \mathbb{C}^N \) be a subset of the set of isolated solutions of the zero-locus of \( F \). Let \( m_{y_i} \) denote the maximal ideal of \( y_i \) and let \( \mathcal{P}_{y_i} \) denote the \( m_{y_i} \)-primary component of \( I \). Let \( J = \bigcap_{i=1}^{\ell} \mathcal{P}_{y_i} \) and let \( Z \) denote the corresponding zero dimensional subscheme supported on \( Y \). This article presents a numeric-symbolic algorithm for computing the Hilbert function of \( Z \). The input for the algorithm is the polynomial system \( F \) and a numerical approximation of each element in \( Y \).

Keywords. regularity, Hilbert function, homotopy continuation, multiplicity, numerical algebraic geometry, polynomial system, dual basis

AMS Subject Classification. 65H10, 68W30

Introduction

Homotopy continuation can be used to determine a numerical approximation for each isolated solution of the zero locus of a multivariate polynomial system. By utilizing a deflation method for isolated solutions, such as described in [4, 7, 8], each isolated solution can be computed to arbitrary accuracy using a quadratically convergent Newton’s method. This article uses a numerical approximation of each isolated point in the

∗Harold Vance Department of Petroleum Engineering, Mailstop 3116, Texas A&M University, College Station, TX 77843 (zacgriffin21@neo.tamu.edu).
†Department of Mathematics, Mailstop 3368, Texas A&M University, College Station, TX 77843 (jhauenst@math.tamu.edu, [www.math.tamu.edu/~jhauenst]). This author was partially supported by Texas A&M University and NSF grant DMS-0915211.
‡Department of Mathematics, Colorado State University, Fort Collins, CO 80523 (peterson@math.colostate.edu, [www.math.colostate.edu/~peterson]). This author was partially supported by NSF grant DMS-0823633 and AFOSR grant FA9550-08-1-0166 P0004.
§Department of Applied and Computational Mathematics and Statistics, University of Notre Dame, Notre Dame, IN 46556 (sommese@nd.edu, [www.nd.edu/~sommese]). This author was partially supported by the Duncan Chair of the University of Notre Dame and NSF grant DMS-0712910.
support of a zero scheme to compute the Hilbert function, standard monomials, and index of regularity of the zero scheme. The underlying theory supporting the approach is based on Macaulay’s inverse systems [9].

The first section of the paper provides background information regarding dual bases, standard monomials, Hilbert functions, and the index of regularity along with an example to illustrate these ideas. Section 2 presents the underlying theory and the resulting algorithm to compute the standard monomials, Hilbert function, and the index of regularity. Section 3 discusses implementation details. Section 4 consists of two examples applying the algorithm. The final section consists of concluding comments, and a brief discussion of an extension of the algorithm to subschemes of zero-schemes together with practical limitations.

1 Background

This section consists of background information on dual bases, standard monomials, Hilbert functions, and the index of regularity. The section concludes with an example to illustrate these ideas.

1.1 Dual bases

Following the notation of [1, 4], for $\alpha = (\alpha_1, \ldots, \alpha_N) \in (\mathbb{Z}_{\geq 0})^N$, define $|\alpha| = \alpha_1 + \cdots + \alpha_N$, $\alpha! = \alpha_1! \alpha_2! \cdots \alpha_N!$, and $\partial_\alpha = \frac{1}{\alpha!} \partial^{\alpha_1} \partial x_1^{\alpha_1} \cdots \partial x_N^{\alpha_N}$.

Let $R = \mathbb{C}[x_1, \ldots, x_N]$, let $y \in \mathbb{C}^N$ and let $\alpha \in (\mathbb{Z}_{\geq 0})^N$. Viewing $R$ as a complex vector space, the linear functional, $\partial_\alpha[y] : R \to \mathbb{C}$, is defined by $\partial_\alpha[y](g) = (\partial_\alpha g)(y)$. When it is clear from context, $\partial_\alpha[y]$ may be written as $\partial_\alpha$.

Let $y \in \mathbb{C}^N$ and let $S_y = \{ \partial_\alpha[y] \mid \alpha \in (\mathbb{Z}_{\geq 0})^N \}$. For each $y \in \mathbb{C}^N$, one can associate the (infinite dimensional) complex vector space, $D_y$, consisting of all finite $\mathbb{C}$-linear combinations of elements from $S_y$. It is clear that $D_y$ is a subspace of the vector space, $\text{Hom}_\mathbb{C}(R, \mathbb{C})$, of linear functionals on $R$. If $I \subset \mathbb{C}[x_1, \ldots, x_N]$ is an ideal, the dual space of $I$ at $y$ is the set of all elements of $D_y$ that vanish on $I$, namely $D_y[I] = \{ \partial \in D_y \mid \partial(g) = 0 \text{ for all } g \in I \}$.

For a set of points $Y = \{ y_1, \ldots, y_\ell \}$, define $D_Y$ to be the vector space of all finite $\mathbb{C}$-linear combinations of elements from $S_{y_1} \cup \cdots \cup S_{y_\ell}$ and define the dual space of $I$ at $Y$ by $D_Y[I] = \{ \partial \in D_Y \mid \partial(g) = 0 \text{ for all } g \in I \}$.

A dual basis for a dual space is a subset of elements in the dual space that forms a $\mathbb{C}$-basis for the space.
Let \( \mathcal{V}(I) = \{ z \in \mathbb{C}^N | g(z) = 0 \text{ for all } g \in I \} \), let \( y \in \mathcal{V}(I) \), and let \( \mathfrak{m}_y \) denote the maximal ideal of \( y \). If \( y \) is an isolated element of \( \mathcal{V}(I) \), then \( \mathfrak{m}_y \) is a non-embedded associated prime of \( I \). In other words, in an irredundant primary decomposition of \( I \), \( \mathfrak{m}_y \) is a minimal associated prime. As a minimal associated prime, \( \mathfrak{m}_y \) has a well defined multiplicity, \( \text{mult}_I(y) \), in \( I \). In fact, if \( \mathcal{P}_y \) denotes the \( \mathfrak{m}_y \)-primary component in an irredundant primary decomposition of \( I \), then \( y \) being an isolated point implies that \( \text{mult}_I(y) \) is the same as the degree of the scheme associated to \( \mathcal{P}_y \) which, in turn, is the same as \( \dim_{\mathbb{C}} R/\mathcal{P}_y \). The following theorem of Macaulay makes an explicit connection between \( \text{mult}_I(y) \) and the dimension of \( D_y[I] \) as a complex vector space.

**Theorem 1.** Let \( I \subset \mathbb{C}[x_1, \ldots, x_N] \) be an ideal and let \( y \in \mathcal{V}(I) \). Then

i) \( \dim_{\mathbb{C}} D_y[I] < \infty \) if and only if \( y \) is an isolated point in \( \mathcal{V}(I) \).

ii) If \( y \) is an isolated point in \( \mathcal{V}(I) \) then \( \dim_{\mathbb{C}} D_y[I] = \text{mult}_I(y) \).

When \( y \) is an isolated point in \( \mathcal{V}(I) \), numerical algorithms can be used to compute \( \dim_{\mathbb{C}} D_y[I] \) and hence \( \text{mult}_I(y) \). Additionally, the local dimension test of \([1]\) is based on Theorem 1.

The following proposition about linear independence in \( \text{Hom}_{\mathbb{C}}(R, \mathbb{C}) \) leads to a stronger formulation of Macaulay’s theorem.

**Proposition 2.** Let \( Y_1 \) and \( Y_2 \) be finite sets of points in \( \mathbb{C}^N \). Then \( Y_1 \cap Y_2 = \emptyset \) if and only if \( D_{Y_1} \cap D_{Y_2} = 0 \).

**Proof.** It is clear that \( D_{Y_1} \cap Y_2 \subset D_{Y_1} \cap D_{Y_2} \). Therefore, \( Y_1 \cap Y_2 \neq \emptyset \) implies \( D_{Y_1} \cap D_{Y_2} \neq 0 \) yielding \( D_{Y_1} \cap D_{Y_2} \neq 0 \).

Now suppose that \( Y_1 \cap Y_2 = \emptyset \). The statement that \( D_{Y_1} \cap D_{Y_2} = 0 \) is equivalent to the statement that, for any non-zero elements \( \partial_1 \in D_{Y_1} \) and \( \partial_2 \in D_{Y_2} \), there exists an element \( g \in R \) such that \( \partial_1(g) \neq \partial_2(g) \). We will construct a \( g \in R \) such that \( \partial_1(g) = 0 \) but \( \partial_2(g) \neq 0 \). Let \( Y_1 = \{ p_1, \ldots, p_r \} \) and \( Y_2 = \{ q_1, \ldots, q_s \} \). There exists a number \( B \) such that

\[
\partial_1 = \sum_{\{\alpha| |\alpha| \leq B\}} \sum_{i=1}^{r} b_{\alpha,i} \partial_{\alpha}[p_i] \quad \text{and} \quad \partial_2 = \sum_{\{\alpha| |\alpha| \leq B\}} \sum_{i=1}^{s} c_{\alpha,i} \partial_{\alpha}[q_i].
\]

Let \( \mathfrak{m}_p \) denote the maximal ideal of \( p \). By reindexing the elements in \( Y_2 \), if necessary, we can assume there exists an \( \alpha \) such that \( c_{\alpha,s} \neq 0 \). Now choose an element \( g \in (\cap_{i=1}^{r} \mathfrak{m}_{p_i}^{B+1}) \cap (\cap_{i=1}^{s} \mathfrak{m}_{q_i}^{B+1}) \) such that \( \partial_2(g) \neq 0 \) (due to the contribution from \( q_s \)). By construction, \( \partial_1(g) = 0 \).

**Corollary 3.** Let \( I \subset \mathbb{C}[x_1, \ldots, x_N] \) be an ideal and \( Y = \{ y_1, \ldots, y_\ell \} \subset \mathcal{V}(I) \). Then

i) \( \dim_{\mathbb{C}} D_Y[I] < \infty \) if and only if every element of \( Y \) is an isolated point in \( \mathcal{V}(I) \).

ii) If every element of \( Y \) is an isolated point in \( \mathcal{V}(I) \) then \( \dim_{\mathbb{C}} D_Y[I] = \sum_{i=1}^{\ell} \text{mult}_I(y_i) \).
Proof. Part i) is an immediate corollary of Theorem 1. To prove part ii), note that \(\dim_{\mathbb{C}} D_{Y}[I] \leq \sum_{i=1}^{\ell} \text{mult}_{I}(y_{i})\) by Theorem 1. The equality of \(\dim_{\mathbb{C}} D_{Y}[I]\) and \(\sum_{i=1}^{\ell} \text{mult}_{I}(y_{i})\) follows from Proposition 2 by inducting on the number of points in \(Y\) and noting that \(D_{Y'[I]}\) is a subspace of \(D_{Y}\) for any \(Y' \subseteq Y\).

A graded monomial order is a monomial ordering that satisfies

1. \(|\alpha| > |\beta| \implies x^{\alpha} > x^{\beta}\)
2. \(x^{\alpha} > x^{\beta} \implies x^{\gamma}x^{\alpha} > x^{\gamma}x^{\beta}\)

A reverse graded monomial order is a monomial ordering that satisfies

1. \(|\alpha| < |\beta| \implies x^{\alpha} > x^{\beta}\)
2. \(x^{\alpha} > x^{\beta} \implies x^{\gamma}x^{\alpha} > x^{\gamma}x^{\beta}\)

Let \(>\) be a reverse graded monomial order. For any \(k \geq 0\), we can create an ordered list, with respect to the monomial ordering, of the \(q = \binom{N+k}{k}\) monomials of degree \(\leq k\), namely

\[1 = x^{\alpha_{1}} > \cdots > x^{\alpha_{q}}.\]

By Corollary 3 the dual space of the ideal of a zero-scheme, \(S\), is a finite dimensional vector space over \(\mathbb{C}\) whose dimension is equal to the degree of \(S\). It will be convenient to represent the dual space as the row space of a matrix. To that end, let \(I \subset \mathbb{C}[x_{1}, \ldots, x_{N}]\) be an ideal, let \(Y = \{y_{1}, \ldots, y_{\ell}\} \subset \mathcal{V}(I)\) be a set of isolated solutions, and let \(m = \dim_{\mathbb{C}} D_{Y}[I]\). Suppose that \(B = \{\partial_{1}, \ldots, \partial_{m}\}\) is a basis for \(D_{Y}[I]\). Given \(z = (z_{1}, \ldots, z_{N}) \in \mathbb{C}^{N}\) and \(\alpha_{j} = (\alpha_{j,1}, \ldots, \alpha_{j,N})\), let \((x - z)^{\alpha_{j}} = \prod_{i=1}^{N}(x_{i} - z_{i})^{\alpha_{j,i}}\) and let \(A_{k}(z)\) be the \(m \times q\) matrix where

\[A_{k}(z)_{i,j} = \partial_{i}((x - z)^{\alpha_{j}}). \quad (1)\]

The linear independence of \(B\) immediately yields that \(\text{rank}(A_{k}(z)) = m\) for \(k \gg 0\).

This matrix will be used in Section 2 to compute the Hilbert function, index of regularity, and standard monomials. As a function of \(k\), the number of monomials of degree \(\leq k\) displays rapid growth. Due to this rapid growth in the number of monomials and the notorious ill-conditioning of a monomial basis, numerical computations with the matrix \(A_{k}(z)\) may be difficult. These issues are addressed in Section 3.

1.2 Standard monomials

If \(g\) is a nonzero polynomial, let \(\text{in}_{>}(g)\) denote the initial monomial of \(g\) with respect to a graded monomial order \(>\). That is, if \(g = \sum_{j=1}^{k} a_{j}x^{\alpha_{j}}\), where each \(a_{j} \neq 0\) and \(x^{\alpha_{1}} > x^{\alpha_{2}} > \cdots > x^{\alpha_{k}}\), then \(\text{in}_{>}(g) = x^{\alpha_{1}}\).

If \(I\) is an ideal, then \(\text{in}_{>}(I) = \{\text{in}_{>}(f) | f \in I\}\) is the set of initial monomials of \(I\). A monomial \(x^{\alpha}\) is a standard monomial of \(I\) with respect to \(>\) if \(x^{\alpha} \notin \text{in}_{>}(I)\).
If \( y \in V(I) \), then monomial orders can naturally be extended to \( D_y[I] \). In particular, set \( \partial_\alpha > \partial_\beta \) if \( x^\alpha > x^\beta \) and
\[
\text{in}_{\succ}(D_y[I]) = \{ \text{in}_{\succ}(\partial) \mid \partial \in D_y[I] \}. 
\]
If \( y \) is isolated with \( \text{mult}_I(y) = m \) and if \( \succ \) is a reverse graded monomial order then, by the first part of Theorem 3.1 of [8], we have \( |\text{in}_{\succ}(D_y[I])| = \dim_C(D_y[I]) = m \).

If \( B = \{ \partial_1, \ldots, \partial_m \} \) is a basis for \( D_y[I] \), we say that \( B \) is a reduced dual basis with respect to \( \succ \) if no two basis elements have the same initial terms, that is, \( \text{in}_{\succ}(\partial_i) \neq \text{in}_{\succ}(\partial_j) \) for \( i \neq j \). It is easy to see that given a monomial ordering \( \succ \), any dual basis can be made into a reduced dual basis with respect to \( \succ \). In particular, if \( B \) is a reduced dual basis, then \( \text{in}_{\succ}(B) = \{ \partial_{i} \mid i = 1, \ldots, m \} \) consists of \( m \) differential functionals and \( \text{in}_{\succ}(D_y[I]) = \text{in}_{\succ}(B) \).

The standard monomials relate to the initial terms of a dual space. The opposite monomial ordering of \( \succ \), denoted \( \succ \), is defined by \( x^\alpha \succ x^\beta \) if and only if \( x^\beta > x^\alpha \). The second part of Theorem 3.1 of [8] provides the following relationship.

**Proposition 4** (Theorem 3.1 of [8]). Let \( I \) be an ideal such that \( V(I) = \{ y \} \). If \( \succ \) and \( \succ \) are opposite monomial orderings, then the initial terms of \( D_y[I] \) with respect to \( \succ \) is the set of standard monomials for \( I \) with respect to \( \succ \). That is,
\[
\text{in}_{\prec}(D_y[I]) = \{ \partial_\alpha[y] \mid x^\alpha \notin \text{in}_{\succ}(I) \}.
\]

### 1.3 Hilbert functions

The following information contains only the necessary information regarding Hilbert functions and the index of regularity for this article. This information, along with expanded details, can be found in [8].

Recall that a graded monomial order is a monomial order, \( \succ \), that respects monomial multiplication and satisfies \( |\alpha| > |\beta| \implies x^\alpha > x^\beta \). Its opposite ordering, \( \prec \), is a reverse graded monomial ordering (i.e. a monomial order, \( \prec \), that respects monomial multiplication and satisfies \( |\beta| > |\alpha| \implies x^\alpha > x^\beta \)). Unless otherwise stated, for the rest of this article, when dealing with polynomials, we will only consider graded monomial orderings and when dealing with differentials, we will only consider reverse graded monomial orderings.

The degree of a polynomial with respect to a monomial ordering is the total degree of its initial monomial. Over the set of graded monomial orderings, the degree of a polynomial is invariant. That is, if \( \succ_1 \) and \( \succ_2 \) are any two graded monomial orderings, then for any polynomial \( f \), \( \deg(\text{in}_{\succ_1}(f)) = \deg(\text{in}_{\succ_2}(f)) \).

Let \( R = \mathbb{C}[x_1, \ldots, x_N] \). For \( t \in \mathbb{Z}_{\geq 0} \), let \( R_{\leq t} \) denote the finite-dimensional \( \mathbb{C} \)-vector space of polynomials of degree \( \leq t \). For an ideal \( I \subset R \), define
\[
I_{\leq t} = I \cap R_{\leq t}. 
\]
The affine Hilbert function of $I$ is $H_I(t) = \dim_C \mathbb{C}[x_1, \ldots, x_N]_{\leq t}$ and the affine Hilbert function of $R/I$ is

$$H_{R/I}(t) = \dim_C \mathbb{C}[x_1, \ldots, x_N]_{\leq t} - \dim_C \mathbb{C}[x_1, \ldots, x_N]_{\leq t-1}.$$

The following proposition of Macaulay [9] provides a relationship between standard monomials and the Hilbert function for a graded monomial ordering.

**Proposition 5.** Let $I \subset R$ be an ideal and let $>$ be a graded monomial ordering. Then for all $t$, $H_{R/I}(t) = H_{R/(\langle I \rangle)}(t)$. In particular, $H_{R/I}(t)$ is the number of standard monomials of $I$ that are of degree $\leq t$.

For any ideal $I$, $H_{R/I}(t)$ agrees with a polynomial function in $t$ for $t \gg 0$. The (affine) Hilbert polynomial of $R/I$ is the polynomial $HP_{R/I}$ where, for $t \gg 0$, $HP_{R/I}(t) = H_{R/I}(t)$. The index of regularity of $R/I$ is the minimum $t_0 \geq 0$ such that $H_{R/I}(t) = HP_{R/I}(t)$ for all $t \geq t_0$.

Suppose that $\mathcal{V}(I)$ is zero dimensional and $t_0$ is the index of regularity of $R/I$. Let $h_t = H_{R/I}(t)$. Then

$$1 = h_0 < h_1 < \cdots < h_{t_0} = h_{t_0+1} = h_{t_0+2} = \cdots.$$

In particular, the index of regularity of $R/I$ is the minimum $t_0 \geq 0$ such that $h_{t_0} = h_{t_0+1}$. Since $h_t$ is the number of standard monomials of $I$ that are of degree at most $t$, the index of regularity of $R/I$ is the maximum degree of the standard monomials. When $R/I$ is a finite dimensional vector space, we can characterize its Hilbert function by its values $H_{R/I} = \{h_0, h_1, h_2, \ldots\}$ remembering that $h_{t_0} = h_{t_0+1}$ and $h_{t_0+1} = h_{t_0+2}$.

### 1.4 Basic example

Consider the ideal $I = \langle x_1 - x_2^2, x_1^2 \rangle$ where $\mathcal{V}(I) = \{(0,0)\}$. The set

$$B = \{\partial_{(0,0)}[0], \partial_{(0,1)}[0], \partial_{(1,0)}[0] + \partial_{(0,2)}[0], \partial_{(1,1)}[0] + \partial_{(0,3)}[0]\}$$

is a basis for $D_0[I]$. Written more explicitly,

$$B = \{\partial_1[0], \partial_{x_2}[0], \partial_{x_1}[0] + \partial_{x_2^2}[0], \partial_{x_1x_2}[0] + \partial_{x_2^3}[0]\}.$$

Let $>$ be the graded lexicographic monomial ordering defined by $x_2 > x_1$ and $\succ$ be the opposite monomial ordering. That is, for the monomials of degree $\leq 3$, we have

$$x_2^3 > x_2^2x_1 > x_2x_1^2 > x_1^3 > x_2^2 > x_2x_1 > x_1^2 > x_2 > x_1 > 1 \quad \text{and}$$

$$1 \succ x_1 > x_2 > x_1^2 > x_1x_2 > x_2^2 > x_1^3 > x_2^2x_2 > x_1x_2^2 > x_2^3.$$

It is easy to verify that $S = \{1, x_1, x_2, x_1x_2\}$ is the set of standard monomials of $I$ with respect to $>$. In particular, $H_{R/I} = \{1, 3, 4, 4, \ldots\}$ and the index of regularity is 2. Since $B$ is a reduced dual basis with respect to $\succ$, we have

$$\text{in}_\succ(D_0[I]) = \text{in}_\succ(B) = \{\partial_1[0], \partial_{x_1}[0], \partial_{x_2}[0], \partial_{x_1x_2}[0]\}.$$
which corresponds to $S$, as required by Proposition \ref{prop:example}.

Consider the array

\[
\begin{array}{|l|cccccccc|}
\hline
 & 1 & x_1 & x_2 & x_1^2 & x_1x_2 & x_2^2 & x_1^2x_2 & x_1x_2^2 & x_1^3x_2^3 \\
\hline
\partial_1[0] & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\partial_{x_2}[0] & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
\partial_{x_1}[0] + \partial_{x_2}[0] & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\partial_{x_1x_2}[0] + \partial_{x_2}[0] & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
\hline
\end{array}
\]

The matrices $A_0(0), A_1(0), A_2(0),$ and $A_3(0)$ correspond to the first, the first 3 columns, the first 6 columns, and all 10 columns of this array, respectively, which have rank 1, 3, 4, and 4, respectively. Moreover, the pivot columns of $A_k(0)$ correspond to the monomials in $S$ of degree at most $k$. Section \ref{sec:algorithm} shows that this is not a coincidence.

## 2 The algorithm

Let $I \subset \mathbb{C}[x_1, \ldots, x_N]$ be an ideal and $Y = \{y_1, \ldots, y_k\} \subset \mathcal{V}(I)$ be a collection of isolated points. Let $m_{y_i}$ be the maximal ideal of $y_i$. Let $P_{y_i}$ be the $m_{y_i}$-primary component of $I$ and define

\[
J = \bigcap_{i=1}^{\ell} P_{y_i}.
\]

Clearly, $D_Y[I] = D_Y[J]$. The remainder of this section describes an algorithm and the underlying theory for computing the Hilbert function, standard monomials, and index of regularity for $J$. The input for the algorithm is a numerical approximation for each $y_i$ and generators for the ideal $I$.

Theorem \ref{thm:isolatedHilbertFunction} is a key result which supports the computations performed in the algorithm \textbf{isolatedHilbertFunction}. Before stating and proving Theorem \ref{thm:isolatedHilbertFunction} we will need the following lemma.

\textbf{Lemma 6}. Let $R = \mathbb{C}[x_1, \ldots, x_N]$. Let $I \subset R$ be an ideal and let $Y = \{y_1, \ldots, y_k\} \subset \mathcal{V}(I)$ be a collection of isolated points in the variety defined by $I$. Let $J$ be the ideal consisting of the intersection of the $m_{y_i}$-primary components of $I$ (as in Equation \ref{eq:intersection}). Let $g \in R$. If $\partial(g) = 0$ for all $\partial \in D_Y[I] = D_Y[J]$, then $g \in J$.

\textbf{Proof}. Let $P_{y_i}$ denote the $m_{y_i}$-primary component of $I$ and let $J = \bigcap_{i=1}^{\ell} P_{y_i}$. If $g \notin J$, then there exists an $i \in \{1, \ldots, \ell\}$ such that $g \notin P_{y_i}$. Let $\succ$ be any graded monomial ordering and $\preceq$ be its opposite monomial ordering. The standard monomials of $P_{y_i}$ are a basis for the $\mathbb{C}$-vector space $R/P_{y_i}$. Since $g \notin I_i$, the image $h$ of $g$ in $R/P_{y_i}$ is non-zero and can be expressed in terms of the standard monomials of $P_{y_i}$. In this way, we can write $g = h + F$ where $F \in P_{y_i}$ and every monomial of $h$ is a standard monomial of $P_{y_i}$. In particular, we can assume $\text{in}_{\succ}(h) \notin \text{in}_{\succ}(P_{y_i})$.

Let $x^\alpha = \text{in}_{\succ}(h)$. By Proposition \ref{prop:example} there exists a $\partial \in D_{y_i}[P_{y_i}]$ such that $\text{in}_{\succ}(\partial) = \partial_{y_i}[y_i]$. Since $g = h + F$, $F \in P_{y_i}$, and $\partial \in D_{y_i}[P_{y_i}]$, we can conclude that $\partial(g) = \partial(h)$. 

7
Let \( c_\alpha \) be the coefficient of \( x^\alpha \) in \( h \) and let \( d_\alpha \) be the coefficient of \( \partial_\alpha[y_i] \) in \( \partial \). Since \( > \) and \( \succ \) are opposite orderings, \( \partial(h) = c_\alpha d_\alpha \neq 0 \). We conclude that \( \partial(g) \neq 0 \).

Since \( y_i \subseteq Y \) and \( J \subset \mathcal{P}_{y_i} \), we have that \( D_{y_i}[\mathcal{P}_{y_i}] \subseteq D_Y[J] \). Therefore, \( \partial \in D_Y[J] \) with \( \partial(g) \neq 0 \).

We are now ready to prove the main theorem regarding the standard monomials, Hilbert function, and index of regularity of \( J \).

**Theorem 7.** Let \( R = \mathbb{C}[x_1, \ldots, x_N] \), let \( I \subset R \) be an ideal, let \( Y = \{y_1, \ldots, y_r\} \subset \mathcal{V}(I) \) where each \( y_i \) is isolated, and let \( J \) be the ideal defined by Equation\([3]\). Let \( > \) be a graded monomial ordering and \( \succ \) be its opposite monomial ordering. Let \( B \) be a basis of \( D_Y[I] \). For each \( k \geq 0 \), let \( A_k(0) \) be the matrix defined by Equation\([4]\) with respect to \( B \) and \( \succ \). Then, the pivot columns of \( A_k(0) \) correspond to the standard monomials of \( J \), with respect to \( \succ \), of degree at most \( k \). In particular, \( H_{R/J}(k) = \text{rank}(A_k(0)) \) and the index of regularity of \( R/J \) is the minimum \( k_0 \geq 0 \) such that \( \text{rank}(A_{k_0}(0)) = \text{rank}(A_{k_0+1}(0)) \).

**Proof.** Fix \( k \geq 0 \) and order the \( q = \binom{N+k}{k} \) monomials of degree \( \leq k \) with respect to \( \succ \), that is,

\[
1 = x^{\alpha_1} > x^{\alpha_2} > \cdots > x^{\alpha_q}.
\]

Suppose that the \( j \)th column of \( A_k(0) \) is a pivot column. This means that there exists a \( \partial \in D_Y[I] = D_Y[J] \) such that \( \partial(x^{\beta}) = 0 \) when \( x^\beta \succ x^{\alpha_j} \) and \( \partial(x^{\alpha_j}) \neq 0 \). For any \( g \in J \) with \( \text{in}_>(g) = x^{\alpha_j} \), since \( > \) and \( \succ \) are opposite orderings, \( \partial(g) \) can be computed using the leading terms of \( \partial \) and \( g \). In particular, \( \partial(g) \neq 0 \) which is not possible. Thus, \( x^{\alpha_j} \) is a standard monomial of \( J \) with respect to \( > \).

Suppose that \( x^{\alpha_j} \) is a standard monomial of \( J \) with respect to \( > \). If the \( j \)th column of \( A_k(0) \) is not a pivot column, then this column is the linear span of the first \( j - 1 \) columns. That is, there exists \( c_1, \ldots, c_{j-1} \in \mathbb{C} \) such that

\[
A_k(0)_{j} = \sum_{p=1}^{j-1} c_p A_k(0)_p
\]

where \( A_k(0)_r \) is the \( r \)th column of \( A_k(0) \). Define \( g = x^{\alpha_j} - \sum_{p=1}^{j-1} b_p x^{\alpha_p} \). By construction, \( \partial(g) = 0 \) for all \( \partial \in D_Y[J] \). Lemma\([6]\) yields \( g \in J \) which is not possible since \( \text{in}_>(g) = x^{\alpha_j} \).

The last statement of the theorem follows directly from the first statement and Proposition\([3]\). \(\square\)

The following algorithm to compute the standard monomials, Hilbert function, and index of regularity is justified by Theorem\([7]\). A numerical dual basis may be computed using either \( [4] \) or \( [13] \).

**Procedure** \((S, \text{reg}, H) = \text{isolatedHilbertFunction}(f, Y, >)\)
Input A finite set of polynomials $f \subset \mathbb{C}[x_1, \ldots, x_N]$, a set $Y = \{y_1, \ldots, y_\ell\}$ of numerical approximations of distinct isolated solutions of $f$, and a graded monomial ordering $>$. 

Output The set of standard monomials $S$ with respect to $>$ for the ideal $J$ as defined in Equation 2 where $I = (f)$, the index of regularity $\text{reg}$, and the vector $H$ corresponding to the Hilbert function of $R/J$ up to order $\text{reg}$.

Begin

1. Construct the opposite monomial ordering $\succ$ from $>$. 
2. Construct a basis $B_i$ for each $D_{y_i}[I]$. 
4. Set $H_0 := 1$ and $k := 0$. 
5. do 
   (a) Set $k := k + 1$. 
   (b) Construct $A_k(0)$ from $B$ and $\succ$. 
   (c) Set $H_k := \text{rank}(A_k(0))$. 
   while $H_k < P$. 
6. Set $\text{reg} := k$ and $S := \text{set of monomials corresponding to the pivot columns of } A_k(0)$. 

Remark 8. The Hilbert function, index of regularity, and standard monomials for $\sqrt{J}$ can be computed using isolatedHilbertFunction by only utilizing the identity differential functionals at each $y_i$ rather than a basis for $D_{y_i}[I]$. This simplification reduces the matrix $A_k(0)$ to the degree $k$ Veronese embedding of the points.

3 Implementation details

Since the numerical computation of a dual basis at an isolated point was discussed in detail in [1, 4, 13], we will focus on the computations regarding the matrix $A_k(0)$ defined in Equation 1. The two main concerns regarding $A_k(0)$ is the ill-conditioning arising from the use of a monomial basis and the growth in the number of columns, which are addressed in Sections 3.1 and 3.2 respectively.

The ideas presented in the following sections are demonstrated using the polynomial system arising from the nine-point path synthesis problem [10]. We setup the polynomial system $\mathcal{F}_9$ using the nine points of Problem 3 listed in Table 2 of [10] (see also [6, § 5.2]) which has 8652 isolated nonsingular solutions. We took $\mathcal{Y}_9$ to be 8652 points in $\mathbb{C}^{12}$, each being an approximation within $10^{-75}$ of a distinct isolated nonsingular solution.
3.1 Numerical concerns

There are two main numerical concerns with isolatedHilbertFunction, namely the accuracy of the input data and the ill-conditioning of using a monomial basis in $A_k(0)$. We note that if the set of points $Y$ used in isolatedHilbertFunction are exact solutions, then all of the computations can be performed exactly. When the points are numerical approximations, care must be taken to maintain numerical integrity. Since each $y_i$ is an approximation of an isolated solution, using an approximate dual basis with a simple modification of the deflation algorithm of [8], one can create a polynomial system which has a nonsingular isolated solution corresponding to $y_i$ and a basis for $D_{y_i}[I]$. By using Newton’s method on this deflated system, the point $y_i$ and a basis for $D_{y_i}[I]$ can be computed to arbitrary accuracy. One can then rerun isolatedHilbertFunction using the more accurate solutions and higher precision to increase the security of the numerical methods.

Due to the ill-conditioning arising from using a monomial basis, the precision one must use to properly determine the rank of $A_k(0)$ may be prohibitively large. For example, the third column of Table 1 presents the largest singular value (i.e., 2-norm) of the matrix $A_k(0)$ for the polynomial system $F_9$ and points $Y_9$. In particular, reliable rank determination, especially for $k \geq 3$, would require the use of higher precision.

We can overcome much of the ill-conditioning by using a preconditioner, namely scaling each row to have unit norm. By interpreting each row of $A_k(0)$ as a vector in a projective space, this preconditioner is equivalent to choosing a different representative of the same point in projective space. The last four columns of Table 1 show that after preconditioning, we can now reliably use double precision to determine the ranks.

3.2 Efficiency improvements

The number of columns of the matrix $A_k(0)$ is the dimension of $\mathbb{C}[x_1, \ldots, x_N]_{\leq k}$, namely $\binom{N+k}{k}$, which grows rapidly as $k$ increases. For $k \geq 2$, we can use information already computed from $A_{k-1}(0)$ to control the growth on the number of columns of $A_k(0)$.

Let $B_k(0)$ be the columns of $A_k(0)$ which correspond to the monomials of degree $k$,
that is, we can write
\[ A_k(0) = \begin{bmatrix} A_{k-1}(0) & B_k(0) \end{bmatrix}. \]

Since the pivot columns of \( A_{k-1}(0) \) have already been computed, the first reduction
is the removal of the nonpivot columns of \( A_{k-1}(0) \). Instead of simply removing the
nonpivot columns from \( A_{k-1}(0) \), for improved numerics, one can replace \( A_{k-1}(0) \) with
a matrix, say \( \tilde{A}_{k-1}(0) \), whose columns form an orthonormal basis of the linear span
of the columns of \( A_{k-1}(0) \), which is the linear span of the pivot columns of \( A_{k-1}(0) \).

The second reduction is based on algebra. In particular, if \( x^\alpha \) is not a standard
monomial, then, for any \( \beta \in (\mathbb{Z}_{\geq 0})^N \), \( x^{\alpha + \beta} \) is also not a standard monomial. Let \( S_j \)
denote the set of standard monomials of degree at most \( j \) and suppose \( x^\alpha \in S_k \). For
every \( \beta \in (\mathbb{Z}_{\geq 0})^N \) such that \( \beta_i \leq \alpha_i \), we must have \( x^{\beta} \in S_{|\beta|} \subset S_k \). That is, given \( S_k \),
one can easily determine a set \( \tilde{S}_{k+1} \) such that \( S_{k+1} \subset \tilde{S}_{k+1} \). Let \( \tilde{B}_k(0) \) consist of the
columns of \( B_k(0) \) which correspond to the monomials in \( \tilde{S}_k \) ordered with respect to \( \succ \).

We know that the pivot columns of \( A_k(0) \) are the pivot columns of \( A_{k-1}(0) \) and the
columns of \( \tilde{B}_k(0) \) which are pivot columns of the matrix
\[ \begin{bmatrix} \tilde{A}_{k-1}(0) & \tilde{B}_k(0) \end{bmatrix}. \]

For example, consider the four nonpivot columns of \( A_2(0) \) for the polynomial system
\( \mathcal{F}_9 \) and points \( \mathcal{Y}_9 \). These columns correspond to the monomials \( a\tilde{x}, \tilde{a}x, b\tilde{y}, \) and \( \tilde{b}y \) which arise from the four quadratic polynomials in \( \mathcal{F}_9 \), namely
\[ n - a\tilde{x}, \quad \tilde{n} - \tilde{a}x, \quad m - b\tilde{y}, \quad \text{and} \quad \tilde{m} - \tilde{b}y. \]

Using only these four monomials, we can immediately remove 13% (48 out of 364) of
the columns of \( B_3(0) \), 22% (306 out of 1365) of the columns of \( B_4(0) \), 32% (1384 out of
4368) of the columns of \( B_5(0) \), 40% (4996 out of 12376) of the columns of \( B_6(0) \), and
48% (15336 out of 31824) of the columns of \( B_7(0) \).

Since the columns of \( \tilde{A}_{k-1}(0) \) are orthonormal, the third reduction constructs a
matrix \( Q_{k-1} \) such that \( \begin{bmatrix} \tilde{A}_{k-1}(0) & Q_{k-1} \end{bmatrix} \) is unitary. We then have
\[ \text{rank } A_k(0) = \text{rank } \tilde{A}_{k-1}(0) + \text{rank } Q_{k-1} \cdot \tilde{B}_k(0) = \text{rank } A_{k-1}(0) + \text{rank } Q_{k-1} \cdot \tilde{B}_k(0) \]
where \( Q_{k-1}^* \) is the Hermitian adjoint, i.e., conjugate transpose, of \( Q_{k-1} \). Due to the
added cost of computing \( Q_{k-1} \), this reduction is only beneficial when the number of
columns of \( Q_{k-1} \), which is the difference between the number of rows and the rank of
\( \tilde{A}_{k-1}(0) \), is small.

4 Examples

The following examples discussed in this section were run on an Opteron 250 processor
running 64-bit Linux. We used the graded lexicographic monomial ordering \( \succ \) defined
<table>
<thead>
<tr>
<th>$I$</th>
<th>Hilbert function</th>
<th>index of reg.</th>
<th>standard monomials</th>
</tr>
</thead>
<tbody>
<tr>
<td>$Y_1$</td>
<td>1, 2, 2, ...</td>
<td>1</td>
<td>1, $x_1$</td>
</tr>
<tr>
<td>$Y_2$</td>
<td>1, 3, 4, 4, ...</td>
<td>2</td>
<td>1, $x_1$, $x_3$, $x_1 x_3$</td>
</tr>
<tr>
<td>$Y_3$</td>
<td>1, 4, 6, 6, ...</td>
<td>2</td>
<td>1, $x_1$, $x_2$, $x_3$, $x_1 x_2$, $x_1 x_3$</td>
</tr>
<tr>
<td>$Y_4$</td>
<td>1, 4, 7, 7, ...</td>
<td>2</td>
<td>1, $x_1$, $x_2$, $x_3$, $x_1 x_2$, $x_1 x_3$, $x_2 x_3$</td>
</tr>
<tr>
<td>$Y_5$</td>
<td>1, 4, 7, 8, 8, ...</td>
<td>3</td>
<td>1, $x_1$, $x_2$, $x_3$, $x_1 x_2$, $x_1 x_3$, $x_2 x_3$, $x_1 x_2 x_3$</td>
</tr>
</tbody>
</table>

Table 2: Computing the Hilbert function, index of regularity, and standard monomials for $I$ at $\hat{Y_i}$

by $x_N > x_{N-1} > \cdots > x_1$ so that its opposite monomial ordering $\succ$ has

$$1 \succ x_1 \succ x_2 \succ \cdots \succ x_N \succ x_1^2 \succ x_1 x_2 \succ \cdots .$$

Though exact solutions are known for the following examples (either by hand or using symbolic software), these examples utilized numerical approximations of the solutions generated by Bertini $^2$ with the matrix computations performed using Matlab.

### 4.1 A collection of isolated solutions

Consider $I = (x_1^2 + x_2 + x_3 - 1, x_1 + x_2^2 + x_3 - 1, x_1 + x_2 + x_3^2 - 1) \subset \mathbb{C}[x_1, x_2, x_3]$ from [11]. This ideal has the following 5 isolated solutions:

$$y_1 = (1, 0, 0), \quad y_2 = (0, 1, 0), \quad y_3 = (0, 0, 1),$$

$$y_4 = (-1 - \sqrt{2}, -1 - \sqrt{2}, -1 - \sqrt{2}), \quad \text{and} \quad y_5 = (\sqrt{2} - 1, \sqrt{2} - 1, \sqrt{2} - 1).$$

Solutions $y_1$, $y_2$, and $y_3$ have multiplicity 2 while $y_4$ and $y_5$ have multiplicity 1. The points $\hat{y}_i$ that were used approximated $y_i$ to 10 digits. Table 2 displays the Hilbert function, index of regularity, and standard monomials using isolated Hilbert Function with $\hat{Y_i} = \{\hat{y}_1, \ldots, \hat{y}_i\}, \ i = 1, \ldots, 5$. All of these computations, including the computation of $\hat{Y}_i$, took less than a second.

### 4.2 A system with isolated and positive-dimensional solution components

Consider

$$I = \langle (x_2 - x_1^2)(x_1 - 2)^2, (x_1 x_2 - x_3)(x_2 - 2)^2, (x_2^2 - x_1 x_3)(x_3 - 2) \rangle \subset \mathbb{C}[x_1, x_2, x_3].$$

This ideal has a one-dimensional solution component, namely the twisted cubic $C = \{(t, t^2, t^3) \mid t \in \mathbb{C}\}$, and the following 5 isolated solutions:

$$a_1 = (2, 1, 2), \quad a_2 = (\sqrt{2}, 2, 2), \quad a_3 = (-\sqrt{2}, 2, 2),$$

$$a_4 = (2, 0, 0), \quad \text{and} \quad a_5 = (2, 2, 2).$$
Solutions $a_1, \ldots, a_4$ have multiplicity 2 and $a_5$ has multiplicity 8. Let $\hat{A} = \{\hat{a}_1, \ldots, \hat{a}_5\}$ where $\hat{a}_i$ is a 10 digit approximation to $a_i$. Table 3 displays the Hilbert function and index of regularity using \texttt{isolatedHilbertFunction} using the generators for the ideal $I$ with $\hat{A}$ as well as its radical. All of these computations, including the computation of $\hat{A}$, took less than a second.

### 4.3 A sequence of systems

For each $n \geq 3$, consider a generalization of the $mth191$ system of Bernd Sturmfels presented in [4, 7], namely $I_n = \langle f_1, \ldots, f_n \rangle \subset \mathbb{C}[x_1, \ldots, x_n]$ where

$$f_i = x_i^3 - x_i^2 + \sum_{j=1}^{n} x_j^2 - 1.$$

Let $Y_n = \{e_1, \ldots, e_n\} \subset \mathbb{C}^n$ be the set of standard basis vectors of $\mathbb{C}^n$ and $\hat{Y}_n = \{\hat{e}_1, \ldots, \hat{e}_n\}$ where each $\hat{e}_i$ is a 12 digit approximation to $e_i$. For $n = 3, 4, 5, 6$, the multiplicity of each $e_i$ is 4, 12, 16, and 32, respectively. Table 4 displays the Hilbert function and index of regularity using \texttt{isolatedHilbertFunction} for the ideal $I_n$ at $\hat{Y}_n$ for $3 \leq n \leq 6$. We note that less than one percent of the time was spent actually performing rank computations. In particular, for $n = 6$, approximately 22% of the time was spent computing dual bases using an implementation of [4] and approximately 77% of the time was spent by Matlab constructing the matrices $A_k(0)$ from the points and dual bases.

Table 5 displays the Hilbert function and index of regularity using \texttt{isolatedHilbertFunction} for $\sqrt{I_n}$ for $3 \leq n \leq 6$ using the points in $V(I_n)$ computed by Bertini to 12 digits. For $n = 6$, Bertini took 27 seconds to compute the points with \texttt{isolatedHilbertFunction} taking 85 seconds. Of this 85 seconds, roughly 60 seconds was used to construct the matrices $A_k(0)$ and roughly 25 seconds was used to perform the rank


Table 5: Computing the Hilbert function and index of regularity for $\sqrt{I_n}$

<table>
<thead>
<tr>
<th>$n$</th>
<th>Hilbert function</th>
<th>index of reg.</th>
<th>time</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1, 4, 10, 16, 18, 18, ...</td>
<td>4</td>
<td>1s</td>
</tr>
<tr>
<td>4</td>
<td>1, 5, 15, 28, 36, 37, ...</td>
<td>5</td>
<td>4s</td>
</tr>
<tr>
<td>5</td>
<td>1, 6, 21, 51, 96, 167, 168, ...</td>
<td>8</td>
<td>11s</td>
</tr>
<tr>
<td>6</td>
<td>1, 7, 28, 78, 168, 294, 425, 506, 536, 542, 543, ...</td>
<td>10</td>
<td>1m52s</td>
</tr>
</tbody>
</table>

computations. We note that using Macaulay2 v1.3.1 [5], both the primaryDecomposition and radical algorithms working over $\mathbb{Q}$ failed to terminate within 24 hours for both $I_5$ and $I_6$.

5 Concluding remarks

As before, let $Y = \{y_1, \ldots, y_\ell\} \subset \mathbb{C}^N$, let $m_{y_i}$ denote the maximal ideal of $y_i$ and let $P_{y_i}$ denote an $m_{y_i}$-primary ideal. Let $J = \cap_{i=1}^{\ell} P_{y_i}$, let $L$ be an ideal such that $V(L) \cap V(J) = \emptyset$, and let $I = J \cap L$. This paper presents an algorithm, isolatedHilbertFunction, to compute the Hilbert function of $R/J$ from a set of generators for $I$ and a set of numerical approximations $\hat{Y} = \{\hat{y}_1, \ldots, \hat{y}_\ell\} \subset \mathbb{C}^N$ to the elements in $Y$. There are several algorithms that follow, in a natural manner, from isolatedHilbertFunction (and modifications).

One of the more immediate applications is a direct algorithm to determine if a set of points satisfies the Uniform Position Property. A set of points $Y = \{y_1, \ldots, y_\ell\} \subset \mathbb{C}^N$ has the Uniform Position Property if the Hilbert function of any subset $Y'$ of $Y$ only depends on the cardinality of $Y'$. This property can be checked by iterating isolatedHilbertFunction over the power set of $Y$. While the power set of $Y$ has cardinality $2^\ell$, the ability to parallelize the computation suggests it is feasible on sets consisting of fewer than 30 points.

Examples were presented involving the Hilbert function of $R/J$ and of $R/\sqrt{J}$. The approach for computing the Hilbert function of $R/\sqrt{J}$ can be generalized as follows. Let $v = (v_1, \ldots, v_\ell) \in (\mathbb{Z}_{\geq 0})^\ell$ and let $J(v) = \cap_{i=1}^{\ell} (P_{y_i}, m_{y_i}^v)$. The Hilbert function of $R/\sqrt{J}$ was computed by utilizing only the identity differential functionals at each $y_i$ rather than a basis for $D_{y_i}[I]$. This corresponds to computing $R/J(v)$ when $v = (1, 1, \ldots, 1)$. In general, by utilizing a subset, dependent on $v_i$, of the differential functionals at each $y_i$, the Hilbert function of $R/J(v)$ can be computed for any $v$. When all the entries of $v$ are sufficiently large, then $J(v) = J$. When some of the entries of $v$ are equal to zero, then the corresponding points are excluded. The scheme defined by $J(v)$ is a subscheme of the scheme defined by $J$. The ability to make such a broad range of direct computations on subschemes of zero-schemes is due to the ability to numerically decompose varieties over $\mathbb{C}$, a feature which is often difficult in an exact setting.

Finally, it is important to note the limits of such computations. As part of isolatedHilbertFunction, reliable rank computations must be made on the matrices $A_k(0)$.
These matrices can become very large and have numerical entries. The limit of reliable rank computations on such matrices is not completely clear. Such a limit must depend on the minimum of the number of rows and columns as well as the relationship between the nonzero singular values and singular values which should be zero. Since the number of rows of $A_k(0)$ is constant, we have a constant bound on the minimum of the number of rows and columns. For example, Table 1 shows that successful computations can be made on a matrix with approximately 8,600 rows and 50,000 columns. Computations involving a matrix where the minimum of the number of rows and columns is 30,000 would require a tremendous amount of patience and memory. Matrices where the minimum is more than 100,000 are currently out of reach.

References


