Conditions for Additional Roots from Maximal-Rank Minors of Macaulay Matrices

Deepak Kapur[1a], Manfred Minimair[b]

[a]University of New Mexico, Department of Computer Science, Albuquerque, NM, USA
[b]Seton Hall University, Department of Mathematics and Computer Science, South Orange, NJ, USA

Abstract

Necessary conditions, under which the maximal-rank minors of a (possibly singular) Macaulay matrix of a polynomial system vanish, are analyzed. It is shown that the vanishing of the maximal-rank minors of the Macaulay matrix of a system of parametric polynomials under specialization is a necessary condition for the specialized polynomials to have an additional common root even when the parametric system has common roots without any specialization of parameters. For such a parametric system, its resultant is identically zero. A theorem of independent interest also gives a degree bound from which the Hilbert function of a certain zero-dimensional polynomial system that is not necessarily a complete intersection, as defined by Macaulay in his 1913 paper, becomes constant. These results are not only of theoretical interest, but it extends the class of parametric polynomial systems whose zeros can be analyzed using matrix based resultant formulations. Particularly, the main result has applications in areas where conditions for additional common roots of polynomial systems with generic roots are needed, such as in implicitization of surfaces with base points and in reasoning about geometric objects.

Key words: Macaulay matrix, resultant, maximal-rank minor, Hilbert function

[1] Partially supported by an NSF award CCF-0729097.

1. Introduction

This paper generalizes the following observation for Sylvester matrices of bivariate homogeneous polynomials (or, equivalently, of univariate polynomials) to the multivariate case of Macaulay matrices [20]. Let f and g be bivariate homogeneous polynomials with parametric coefficients and with finitely-many common projective roots without any specialization (in the algebraic closure of the field generated by the coefficients of f and g). Then the vanishing of any maximal-rank minor of the Sylvester matrix of f and g under specialization of the parameters is a necessary condition for f and g to have at least one additional common projective root. This observation follows from the well-known fact [1] that the nullity of the Sylvester matrix equals the number of common roots of f and g (if f and g have finitely-many, including the possibility of no, common roots without any specialization of the parameters). (As it is usual, by *nullity* of a matrix, we mean the dimension of the nullspace of the matrix.) As an example, consider $f = (a_1x_1 + a_2x_2)(b_1x_1 + b_2x_2)$ and $g = (a_1x_1 + a_2x_2)(c_1x_1 + c_2x_2)$. Then any maximal-rank minor of the Sylvester matrix of f and g is a multiple of $b_1c_2 - b_2c_1$ which is the resultant of $b_1x_1 + b_2x_2$ and $c_1x_1 + c_2x_2$, a polynomial system obtained after factoring out the common root $a_1x_1 + a_2x_2$.

Multivariate polynomials differ in two aspects from two bivariate homogeneous polynomials.

- Firstly, bivariate homogeneous polynomials that have a common projective root always have a common factor which clearly influences the structure of the Sylvester matrix. (See [4, 5] for techniques that can be used to study coefficient matrices of reducible polynomials.) In contrast, multivariate polynomials with a common root do not necessarily have a common factor. Therefore the common root influences the structure of the associated resultant matrices, particularly Macaulay matrices, in a less obvious way.

- Secondly, the nullity of the Macaulay matrix is not necessarily equal to the number of common roots of the given system of polynomials. As an example, consider three nonhomogeneous quadratic polynomials in the variables x_1 and x_2 with independent symbolic coefficients and assume that the coefficient of x_1^2 in the first polynomial vanishes. Vanishing of this coefficient however does not lead to the three polynomials having a non-trivial common root [25] after homogenization. However, as it can be checked easily using the Maple packages [24] for constructing the Macaulay matrix and [26] for determining its rank, the nullity of the Macaulay matrix of this polynomial system is 1.

Using the concept of the Hilbert function [15], we generalize the above observation for Sylvester matrices for bivariate homogeneous polynomials to Macaulay matrices for multivariate homogeneous polynomials. Since the nullity of the Macaulay matrix of a polynomial system does not equal to the number of common roots of the system, we will analyze the nullity of a related matrix, the *dialytic matrix* of the ideal generated by the polynomial system as discussed in [21]. For a system of homogeneous polynomials, the rows of the dialytic matrix of a certain degree consist of the coefficients of all the monomial multiples, of that degree, of the polynomials in the system. The well-known Macaulay matrix is a proper submatrix of this dialytic matrix. It was shown in [21] that the nullity of the dialytic matrix equals the Hilbert function of the ideal generated by the system. Using results about Hilbert functions [14], it is proved in this paper that from a suitable degree on, the Hilbert function equals the number of common roots of the polynomial system. The upper bound on Hilbert functions is also shown to be related to Castelnuovo-Mumford regularity [11] of ideals, as well as the Chardin-Philippon Theorem [3].

The above results are not only of theoretical interest, but are also useful in applications (see Section 2.2. For an example, the maximal-rank minors of the Macaulay matrix can be used to extract implicit equations for parametric surfaces with base points [33, 7] (see Section 2.2.6). The results can also be used for reasoning about geometric objects, as discussed in a later section of this paper (Section 2.2.7).

1.1. Related Work

This paper is a continuation of the research direction initiated in [16] about extracting resultants from singular resultant matrices, and more recently in [7], in which it is shown that the vanishing of the maximal-rank minor of any resultant matrix is a necessary condition for common roots outside a certain variety. In contrast, the main result of this paper does not require that the common roots be outside some variety. More importantly, our techniques are able to consider multiplicities of common roots of a polynomial system, in contrast to [16, 7], where multiplicities are ignored. Our main result implies that the maximal-rank minors of the Macaulay matrix also vanish if the multiplicity of a common root of the system increases under a specialization. In this sense, our results are a generalization of the results in [7].

Moreover, this paper addresses the question posed in [19] about whether maximal-rank minors of Macaulay matrices can be used for solving systems of polynomial equations.

Another related work is [2] which studies the resultant for roots outside of the variety of a given complete intersection. But the systems of [2] have a more specific structure, different from the polynomials systems considered in our paper. Furthermore, the techniques used in [2] do not seem to be applicable to the problems studied in our paper.

Furthermore, in [21], Macaulay discussed how to compute the Hilbert polynomial of an ideal that is a *complete intersection*, which is an ideal generated by $k \leq n$ homogeneous polynomials in n variables and whose set of common roots has the dimension $n - k$ in the projective space. In this paper, we give a method for computing the Hilbert function of ideals generated by a system of n homogeneous polynomials in n variables that have finitely-many common roots (i.e. zero-dimensional systems). Such ideals are not necessarily complete intersections. Their Hilbert function is expressed as the difference of two Hilbert functions one of which is the Hilbert function of a complete intersection. In this sense, this work is a generalization/extension of the results by Macaulay [21] about Hilbert functions of zero-dimensional ideals. Theorem 5 of the paper gives a degree bound from which on the Hilbert function of such an ideal is constant.

1.2. Background and Structure

The reader is assumed to be familiar with resultants, primary decomposition and the Hilbert function. There are some excellent classical and modern texts covering these topics [15, 20, 18, 17, 21, 22, 29, 14, 30, 31, 32, 10, 8, 11, 27]. For algorithms based on the Hilbert function for computing the multiplicity structure of roots, see for example [9]. In a recent paper [28], several open and interesting problems in the area of Hilbert functions are stated.

The resultants and Macaulay matrices have been computed with the Maple package MR [24]. The maximal-rank minors have been extracted with the Maple package DR [26]. Furthermore, primary decompositions have been computed with Singular [13] and Maple.

The rest of the paper is organized as follows. Section 2 states the main result about vanishing of maximal minors of a Macaulay resultant matrix and the zero set of a system of parametric polynomials under specialization with some key applications. Section 3 states the result about the Hilbert function of a zero-dimensional ideal that is not a complete intersection. Section 4 reviews some key observations about primary decomposition of ideals, how they get affected by the quotient operation on ideals, as well as reviews properties of Hilbert functions of ideals. Using these properties Section 5 gives a proof on the upper bound of the Hilbert function of an ideal generated by n homogeneous polynomials in n variables. Section 6 gives a proof of the main result, Theorem 1, about the vanishing of maximal minors of Macaulay resultant matrices under specialization.

2. Macaulay Matrices of a Parametric Polynomial System with Additional Common Roots under Specialization

This section informally discusses the main result reported in this paper at a high level, illustrating its significance, but without getting into technical details which follow in later sections. It is proved that a maximal rank minor of a Macaulay matrix of a system of parametric polynomials vanishes under a parameter specialization if the specialized polynomial system has an additional common root due to the specialization.

This main result is proved using the second result in the paper about an upper bound on the Hilbert function of a zero-dimensional ideal and its constancy after a certain degree bound. The second result is informally discussed in Section 3.

2.1. Maximal-Rank Minors of the Macaulay Matrix

Let $f_1, \ldots, f_n$ be homogeneous polynomials in $\mathbb{F}[\mathcal{A}][x_1, \ldots, x_n]$ where $\mathcal{A}$ is a list of independent parameters disjoint from the variables x_i's and $\mathbb{F}$ is an algebraically closed field. Furthermore, assume that the f_i's have finitely-many (possibly no) common projective roots in the algebraic closure of the field generated by $\mathbb{F}$ and the symbols in $\mathcal{A}$ without any specialization.

The Macaulay matrix of the f_i's is a submatrix of the dialytic matrix of the ideal generated by the f_i's of degree $e = 1 + (d_1 - 1) + \cdots + (d_n - 1)$ [20, 21, 22, 14]. The entries of the Macaulay matrix are the coefficients of certain monomial multiples of the f_i's. For each f_i, we construct a set S_i of corresponding monomial multipliers of total degree $e - d_i$: The set S_1 consists of all monomials in $x_1, \ldots, x_n$ of total degree $e - d_1$. The set S_i consists of all monomials m of total degree $e - d_i$ such that m is not divisible by $x_1^{d_1}, \ldots, x_{i-1}^{d_{i-1}}$. The Macaulay matrix is a square matrix whose determinant is a multiple of the projective resultant of the f_i's.

Consider a maximal-rank submatrix S of the (possibly singular) Macaulay matrix of the above system of parametric polynomials. We state below that the determinant of S vanishes under a parameter specialization if the specialized polynomial system has an additional common root due to specialization. This result holds irrespective of whether the original polynomial system has a common zero or not without any specialization of parameters. This is illustrated using a simple example as well.

Theorem 1 (Main Theorem). *Let $\phi : \mathbb{F}[\mathcal{A}][x_1, \ldots, x_n] \rightarrow \mathbb{F}[x_1, \ldots, x_n]$ be a specialization homomorphism that assigns values from $\mathbb{F}$ to the parameters in $\mathcal{A}$. Then any maximal-rank minor of the Macaulay matrix of the f_i's vanishes under the specialization ϕ if the specialized $\phi(f_1), \ldots, \phi(f_n)$ have finitely-many* **more** *common roots (including the possibility of the same roots with higher multiplicities) than the common roots of the f_i's without specialization of the parameters.*

The reader would notice a close relation between this result and rank submatrix construction proposed in [16] for extracting a projection operator, which is a nontrivial multiple of the resultant, from a Dixon matrix of a system of parametric polynomials. It is proved in [16] that the vanishing of a maximal minor of the Dixon matrix is a necessary condition for the parametric polynomial system to have a common zero, thus implying that the determinant of such a minor is a nontrivial multiple of the resultant.

We also state the following immediate corollary which will be used in Section 2.2 on applications.

Corollary 2. *The rank of the Macaulay matrix M of $f_1, \ldots, f_n$ is greater than the rank of the Macaulay matrix $\phi(M)$ of $\phi(f_1) \ldots, \phi(f_n)$ from Theorem 1. Furthermore, the nullities of M and of $\phi(M)$ are respectively greater than or equal to the number of common roots of the f_i's and $\phi(f_i)$'s.*

The following remark is also important for applications.

Remark 3. We note that Theorem 1 has been stated for homogeneous polynomials f_i for the sake of a simple presentation. However, it can easily be adopted to nonhomogeneous systems $f_1, \ldots, f_n$ in the variables $x_1, \ldots, x_{n-1}$. For such systems the phrase "common roots" is understood to refer to affine roots as well as to roots at infinity.

Theorem 1 is illustrated using a simple example.

Example 4. Let

$$\begin{aligned} f_1 &= (d_{01}x_2 + d_{00}x_3)(x_1 - x_3) \\ f_2 &= (e_{10}x_1 + e_{01}x_2 + e_{00}x_3)(x_2 - x_3) \\ f_3 &= c_{20}x_1^2 + c_{11}x_1x_2 + c_{02}x_2^2 + c_{10}x_1x_3 + c_{01}x_2x_3 \\ &\quad - (c_{20} + c_{11} + c_{02} + c_{10} + c_{01})x_3^2 \end{aligned}$$

The f_i's have the simple common projective root $(1 : 1 : 1)$ without any specialization of the parameters. Furthermore, the rank of the 15×15 Macaulay matrix of f_1, f_2, f_3 is 13. The rank 13 occurs because the f_i's have been chosen such that the vanishing of the extraneous minor [20] of the Macaulay matrix causes the rank of the Macaulay matrix to drop by one.

The gcd of all maximal-rank minors of the Macaulay matrices of all possible permutations of f_1, f_2, f_3 giving rise to different Macaulay matrices is given by the product of polynomials $r_1r_2r_3r_4$. (Taking the gcd allows us to remove the extraneous factors occurring in the minors, which here are certain coefficients, similar to r_1.) Now the factors r_i are

$$\begin{aligned} r_1 &= c_{20} \\ r_2 &= d_{00} + d_{01} \\ r_3 &= e_{01}c_{11} + c_{01}e_{01} - c_{02}e_{10} - e_{00}c_{02} + e_{01}c_{02} \\ r_4 &= c_{11}e_{01}d_{00}^2e_{10} - c_{11}d_{00}d_{01}e_{00}e_{10} + c_{11}d_{01}^2e_{10}^2 - c_{20}d_{00}^2e_{01}^2 \\ &\quad - e_{01}d_{00}d_{01}c_{10}e_{10} + 2e_{01}d_{00}d_{01}c_{20}e_{00} - c_{02}e_{10}^2d_{00}^2 + d_{00}e_{10}^2d_{01}c_{01} \\ &\quad + c_{20}d_{01}^2e_{10}^2 + d_{01}^2e_{00}c_{10}e_{10} + d_{01}^2c_{02}e_{10}^2 + c_{01}e_{10}^2d_{01}^2 - c_{20}d_{01}^2e_{00}^2 + d_{01}^2c_{10}e_{10}^2. \end{aligned}$$

Let us analyze the factors:

- $r_1 = 0$ implies that the system has the root $(1 : 0 : 0)$.
- r_2 is the resultant of the factors $(d_{01}x_2 + d_{00}x_3), (x_2 - x_3)$ and of f_3. Its vanishing also implies an additional root of the system.
- r_3 is the resultant of the factors $(x_1 - x_3), (e_{10}x_1 + e_{01}x_2 + e_{00}x_3)$ and of f_3 divided by $(e_{10} + e_{01} + e_{00})$. The factor $(e_{10} + e_{01} + e_{00})$ is removed because its vanishing does not influence the common roots of the f_i's or their multiplicities. Thus the vanishing of r_3 implies an additional root of the system.

- r_4 is the resultant of the factors $(d_{01}x_2 + d_{00}x_3), (e_{10}x_1 + e_{01}x_2 + e_{00}x_3)$ and of f_3. Its vanishing also implies an additional root of the system.

Because of the particular structure of the f_i's, that is, f_1 and f_2 being certain products, it is easy to see that these are the only cases how new roots can arise under any specialization.

2.2. Applications

We discuss several applications of Theorem 1, Corollary 2, and Remark 3. For computations we use the Maple packages [24] for constructing Macaulay matrices and resultants, and [26] for determining their ranks.

2.2.1. Bound on the Number of Discrete Roots

Corollary 2 implies a bound on the number of discrete roots of an overdetermined polynomial system. For example, consider

$$\begin{aligned}
f_1 &= -420\,{x_1}^2 + 206\,x_1x_2 - 1910\,x_1x_3 + 350\,{x_2}^2 + 1839\,x_2x_3 - 920\,{x_3}^2,\\
f_2 &= 5550\,{x_1}^2 - 1408\,x_1x_2 + 3219\,x_1x_3 - 6624\,{x_2}^2 - 2972\,x_2x_3 + 222\,{x_3}^2,\\
f_3 &= 10\,x_1 + 7\,x_2 + 40\,x_3.
\end{aligned}$$

The polynomials f_1, f_2 and f_3 have been chosen to have finitely-many common projective roots. By Bezout's Theorem, we know that the number of these common roots is four. Thus the system $F = (f_1, f_2, f_3)$ can have at most four common roots. Now, the Macaulay matrix of F is of size 10×10 and has rank 8. This implies that the system F has at most two common roots because if it had 3 common roots then the rank of the Macaulay matrix were at least 7. Indeed, f_3 has been chosen such that F precisely has the two common roots $(x_1, x_2, x_3) = (-3722, -2940, -1445)$ and $(x_1, x_2, x_3) = (-2621, 2590, 202)$. Note that precisely counting the number of common roots requires a Gröbner basis computation. If for some particular situation one is satisfied with an upper bound then determining the rank of the Macaulay matrix is a much more efficient alternative to computing a Gröbner basis.

2.2.2. Verifying General Position of Common Roots

For applications it is often useful to verify that the common roots of a polynomial system are "in a general position", that is, no coordinate occurs twice in any of the roots. For example in numerically solving the system, multiple roots with the same coordinates may lead to numerical complications. Furthermore, one may also be interested in finding all the possible coordinates that may correspond to common roots. For instance, consider the polynomial system

$$\begin{aligned}
f_1 &= -7\,{x_1}^2 + 22\,x_1x_2 - 55\,x_1x_3 + 87\,{x_2}^2 - 56\,x_2x_3 - 62\,{x_3}^2 \\
&\quad - 94\,x_1 + 97\,x_3 - 73, \\
f_2 &= -4\,{x_1}^2 - 83\,x_1x_2 - 10\,x_1x_3 - 82\,{x_2}^2 + 80\,x_2x_3 + 71\,{x_3}^2 \\
&\quad + 62\,x_1 - 44\,x_2 - 17\,x_3 - 75, \\
f_3 &= -10\,{x_1}^2 - 7\,x_1x_2 - 40\,x_1x_3 - 50\,{x_2}^2 + 23\,x_2x_3 - 92\,{x_3}^2 \\
&\quad + 42\,x_1 + 75\,x_2 + 6\,x_3 + 74.
\end{aligned}$$

Note that for the sake of a simple presentation we consider an inhomogeneous system because the problem of determining if the common roots are in general position is more easily treated for an inhomogeneous system than for a homogeneous system. That is, for inhomogeneous systems the common roots have unique coordinates, whereas for homogeneous systems the *projective* roots are given by multiples of tuples of coordinates. However, one can extend these techniques to homogeneous systems by dehomogenizing, thus fixing a unique system of coordinates.

We would like to know if the system $F = (f_1, f_2, f_3)$ has common roots whose x_3-coordinates agree. The Macaulay matrix M, with respect to the variables x_1 and x_2, of F is of size 15×15 and of rank 15 for almost all choices of x_3 because the system F only has finitely-many common roots. Let us also note that the resultant R, eliminating x_1 and x_2, of F is

$$\begin{aligned}
&1286356108135946557 2469\,x_3^8 + 62661323468043946947772\,x_3^7 \\
&\quad - 44624269755395455103 58\,x_3^6 - 21276440367559502680841 4\,x_3^5 \\
&\quad + 11172196397655702411253 7\,x_3^4 - 11204036231027121506740 4\,x_3^3 \\
&\quad + 14168432592592391929824 4\,x_3^2 - 35510378302601517078 10\,x_3 \\
&\qquad + 2438727666149798537850 1.
\end{aligned}$$

Now, any specific value ξ_3 substituted for x_3 in R for which the system F has a common root with the value ξ_3 in its x_3-coordinate causes the resultant R to vanish. Thus the rank of the Macaulay matrix M is less than 15 for such $x_3 = \xi_3$. Furthermore, by Theorem 1, any specific $\xi_3 = x_3$ for which the system F has multiple common roots with the same value ξ_3 as the

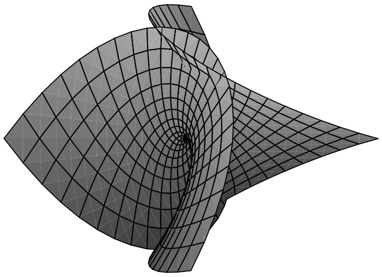

Figure 1: Enneper surface

x_3-coordinate cause any minor of size 14 × 14 of the Macaulay matrix M to vanish. Now, let us choose one minor, say, the determinant D of the submatrix of M consisting of the first 14 rows and columns. It is

$$\begin{aligned} &-621584492305782131358043\,x_3^6 - 2470606740472809699820808\,x_3^5 \\ &\quad - 23717642505164076912986\,2\,x_3^4 + 2476401742066288612694076\,x_3^3 \\ &\quad + 1228510517747574633430600\,x_3^2 + 1723924601513536672480706\,x_3 \\ &\qquad + 571685511992856706856775. \end{aligned}$$

Then one finds that the resultant, eliminating x_3, from of the two polynomials R and D does not vanish. Therefore, there is no pair of common roots of F that have the same x_3-coordinates.

2.2.3. Certifying Simple Points

We want to certify that a given point on a surface is a simple point, that is, a point of multiplicity one. For example, consider the Enneper surface [6] in Figure 1. The Enneper surface is named after the German mathematician Alfred Enneper who constructed the surface in 1863. This is a well known minimal surface, that is, a surface with vanishing mean curvature. As one can see in the upper part of the figure, this surface has some self-intersection and, thus, has multiple points. A parametric representation of the Enneper surface is given by

$$\begin{aligned} f_1 &= s - 1/3\, s^3 + st^2, \\ f_2 &= -t - s^2 t + 1/3\, t^3, \\ f_3 &= s^2 - t^2. \end{aligned}$$

For the parameters $t = \frac{1}{5}$ and $s = \frac{1}{2}$ the surface contains the point $(x_1, x_2, x_3) = (\frac{371}{1500}, -\frac{287}{600}, -\frac{21}{100})$. Now, the Macaulay matrix of $f_i - x_i$, for $i = 1, 2, 3$, is of size 28 × 28 and of rank 27. This implies, by Corollary 2, that the point (x_1, x_2, x_3) is a simple point of the Enneper surface.

2.2.4. Closeness to a System with More Roots

We want to know if a given polynomial system with a certain number of roots is close to another system that has more roots. For this example, let us continue with the system $f_i - x_i$, for $i = 1, 2, 3$, from Section 2.2.3, for which we have already shown that it only has one root with multiplicity one. Using Maple, we compute the singular values $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_{27} > \sigma_{28} = 0$ of the Macaulay matrix M of the system, a matrix of size 28×28 and of rank 27. We find that σ_{27}, the second smallest singular value, is approximately 0.03803. It is a well-known result [12] that the closest distance (in the 2-norm) of a matrix B of rank k to another matrix A equals the singular value σ_{k+1} of A. Since the σ_i's are decreasing, this implies that the closest distance (in the 2-norm) of a matrix B of rank less than or equal to 26 to the Macaulay matrix M is approximately 0.03803. Note that by Corollary 2, any Macaulay matrix N of any system G of the same total degrees as F, with more than one common root is of rank 26 or less. Therefore any such matrix N is not closer to M than approximately 0.03803. Thus, we can view the distance of the Macaulay matrices N and M as a measure of the distance of the polynomial systems G and F that is sensitive to the number of common roots.

2.2.5. Resultant for Bivariate System with Infinite Roots

The main result can be used to extract resultants for polynomial systems that have generic roots at infinity. Here we consider the special case of a system that has the root $(x_1, x_2) = (1, 0)$ at infinity due to some degenerate supports. Consider

$$\begin{aligned}
f_1 &= \mathbf{0} \cdot x_1^2 + a_{11}x_1x_2 + a_{02}x_2^2 + a_{10}x_1 + a_{01}x_2 + a_{00},\\
f_2 &= \mathbf{0} \cdot x_1^2 + b_{11}x_1x_2 + b_{02}x_2^2 + b_{10}x_1 + b_{01}x_2 + b_{00},\\
f_3 &= \mathbf{0} \cdot x_1^2 + c_{11}x_1x_2 + c_{02}x_2^2 + c_{10}x_1 + c_{01}x_2 + c_{00}.
\end{aligned}$$

The support of the polynomials $F = (f_1, f_2, f_3)$, that is, the set of exponent vectors of monomials occurring in F, is

$$\mathcal{S} = \{(1,1), (0,2), (1,0), (0,1), (0,0)\}.$$

Since the coefficients of x_1^2 are zero, the polynomials have the common root $(1,0)$ at infinity and therefore their Macaulay (dense/projective) resultant vanishes. Furthermore, the Macaulay matrix of F is of size 15×15 and of rank 13. Let us now choose a maximal-rank minor, say, with the row indices $1, \ldots, 13$ and the column indices $2, 3, 5, \ldots, 15$. It is the product $a_{00}a_{11}(-a_{02}b_{10} + a_{10}b_{02})$ times an irreducible polynomial R of degree 9 in the a's, b's, and c's. It vanishes if the system F has an additional common root. This implies, by Theorem 1, that R is the toric (sparse) resultant of F with respect to the support $\mathcal{S}$ [8]. In this way, this example can be viewed as an extension of results from [23, 25] that give formulas for resultants under vanishing coefficients when the resultants do not vanish.

2.2.6. Implicitization in the presence of base points

It is well known that implicitization of rationally parametrized surfaces with base points is usually harder to compute than those without base points [33, 7]. Therefore methods for implicitization of such surfaces are under active investigation. A technique based on moving surfaces is proposed by [33]. A different approach for certain surfaces based on Dixon matrices is described in [7]. Here, we illustrate how Macaulay matrices can be used to find implicit equations of rational surfaces with base points. We start with introducing some notation. The points (x, y, z) of the rational surface are the common roots of a polynomial system of the form

$$\begin{aligned}
f_1 &= x\,W(s,t) - X(s,t),\\
f_2 &= y\,W(s,t) - Y(s,t),\\
f_3 &= z\,W(s,t) - Z(s,t),
\end{aligned}$$

where X, Y, Z, W are polynomials in the parameters s and t. The surface has a base point if the polynomials X, Y, Z, W have a common affine or infinite root. In this example we consider a system with base points at infinity. However, it is important to point out that Macaulay matrices can also be applied in the same way in order to compute implicitizations of surfaces with finite base points. Now, let us consider the polynomials

$$\begin{aligned}X(s,t) &= -s^2t^2 - s^2t - 2 + 2s,\\ Y(s,t) &= s^2t^2 - 2s^2t - 1,\\ Z(s,t) &= -2s^2t^2 - 2s^2t - 2 + s,\\ W(s,t) &= s^2t^2 + 1 - 2s\end{aligned}$$

from [33]. This system has the infinite base points $(s,t) = (\infty, 0)$ and $(s,t) = (0, \infty)$.

The Macaulay matrix of the system f_1, f_2, f_3 is of size 66×66 and of rank 48. Let us study a maximal-rank minor of the Macaulay matrix, say, the one consisting of the first 45 rows and rows $51, 52, 53$, and the columns with indices $3, \ldots, 7$, $10, \ldots, 13$, $16, 17, 18$, $21, 22, 24, 25, 27, \ldots, 30$, $33, 34, 37, 38, 41, 42, 43$, $45, 46$, $48, \ldots, 66$. It has the factors $(-x - 1 + y)^2$, $(1 + x)^7$, $(-2x - 2 + y)^2$, $(x + 2)^5$, $(-3 - 2x + y)^9$ and

$$\begin{aligned}R \;=\; & 23\,y^3 + 62\,zy^2 - 151\,y^2 - 190\,y^2x + 484\,yx^2 + 36\,z^2y + 820\,yx + 333\,y\\ & - 276\,zy - 296\,zxy - 910\,x + 302\,z - 261 - 88\,z^2x - 1036\,x^2 - 392\,x^3\\ & + 344\,zx^2 + 632\,zx - 76\,z^2 + 8\,z^3.\end{aligned}$$

Theorem 1 implies that one of these factors is the implicit representation of the rational surface. It can be easily verified in Maple by substituting $\frac{X}{W}, \frac{Y}{W}, \frac{Z}{W}$ for x, y, z that the polynomial R is the implicit representation. Note that the polynomial R is different from the one reported in [33] which, in fact, is not the implicitization of the surface.

2.2.7. Geometric theorem with multiple intersection

We study a condition on the parameters of a line for it to pass through both intersection points of two circles. Such a line, drawn in solid, is shown in Figure 2.

From geometric considerations, we know that the line must be perpendicular to the line connecting the centers of the two circles (see the dotted line

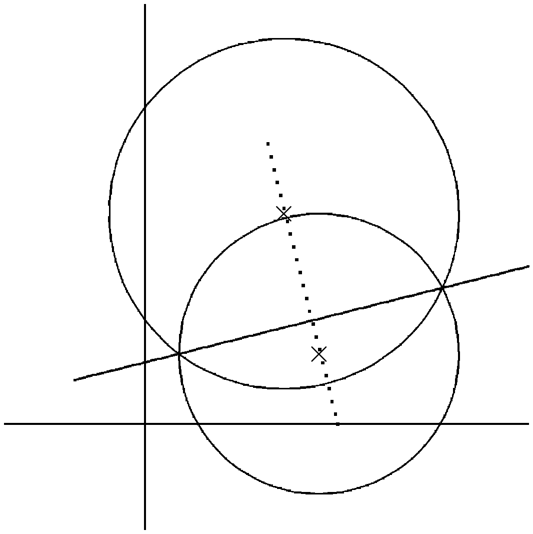

Figure 2: Line meeting two circles in both intersection points

in the figure). Now let us carry out this analysis with a Macaulay matrix. We define polynomials corresponding to the two circles and a line.

$$\begin{aligned} f_1 &= (x_1 - a_1)^2 + (x_2 - a_2)^2 - a_3^2, \\ f_2 &= (x_1 - b_1)^2 + (x_2 - b_2)^2 - b_3^2, \\ f_3 &= c_1 x_2 + c_2 x_2 + c_3. \end{aligned} \tag{1}$$

The Macaulay matrix of f_1, f_2, f_3 is of dimension 10×10 and has rank 9. Let us fix f_1 and f_2. Then any choice of coefficients c_1, c_2, c_3 such that the line $f_3 = 0$ passes through both intersection points of the circles causes the resultant R and, by Theorem 1, any nontrivial 8×8 minor M of the Macaulay matrix of f_1, f_2, f_3 to vanish.

Let us consider the resultant S_M of R and M with respect to c_3. One easily finds that the only common factor of the S_M's that depends on c_1, c_2 and the coefficients of f_1 and f_2 is $((a_1 - b_1)c_2 - (a_2 - b_2)c_1)^2$. The vanishing of this factor indeed means that the line given by $f_3 = 0$ is perpendicular to the line connecting the centers of the circles defined by f_1 and f_2. Note that the authors did not find any existing method for solving polynomial systems that was able to derive this result directly from the system (1).

3. Upper Bound on Hilbert function

The proof of the main Theorem 1 uses a result about the Hilbert function of a polynomial ideal. In this section, we provide a high-level overview of the properties of the Hilbert function leading to this result. The use of properties of Hilbert functions in the proof of Theorem 1 is discussed in Section 6.

Following [15, 29, 14], the Hilbert function of a homogeneous ideal $I \subseteq \mathbb{F}[x_0, x_1, \ldots, x_n]$ is defined below. The homogeneous polynomials in the ring $\mathbb{F}[x_0, x_1, \ldots, x_n]$ of total degree t form a vector space whose basis is the monomials in the variables $x_0, \ldots, x_n$ of total degree t. Therefore the dimension of this vector space is $\binom{t+n}{n}$. The homogeneous polynomials of total degree t in the ideal I form a subspace of this vector space. The dimension of this subspace is called the *volume* of the ideal I, depending on the degree t, and is denoted by $\mathcal{V}(t,\, I)$.

The Hilbert function of the ideal I is defined by $\mathcal{H}(t,\, I) \;=\; \binom{t+n}{n} - \mathcal{V}(t,\, I)$. The Hilbert function $\mathcal{H}(t,\, I)$ equals a polynomial in t, called the *Hilbert polynomial* [15], for all t greater than or equal to some number depending on I. The minimal number with this property is denoted by $\gamma(I)$ and is called the *regularity index* of the ideal I.

Theorem 5 (Upper Bound on Hilbert function). *Let $f_1, \ldots f_n$ be homogeneous polynomials in $\mathbb{F}[x_1, \ldots, x_n]$ of total degrees $d_1, \ldots, d_n$ with finitely-many common projective roots and let I be the ideal generated by the f_i's. Then $\gamma(I) \leq 1 + (d_1 - 1) + \cdots + (d_n - 1)$.*

The study of the Hilbert function is motivated by the fundamental fact that the value of the Hilbert function of degree t for an ideal equals the number of independent linear equations the coefficients of a homogeneous polynomial of degree t in the ideal satisfy. For an ideal I considered in Theorem 5, the Hilbert function of degree t is equal to the number of common projective roots of I for almost all degrees t. Therefore, Theorem 5 shows that for $t \geq (d_1 - 1) + \cdots + (d_n - 1)$, the Hilbert function equals the number of common roots of I.

The upper bound of Theorem 5 seems fundamental. Still, the authors were not able to find it in this generality in the literature. Macaulay showed it for ideals without common projective roots (Corollary 19). (Indeed the proof of Theorem 5 builds on Macaulay's work.) Another subcase can be derived from some important results on Castelnuovo-Mumford regularity [11], denoted by $\operatorname{reg}(I)$ below. The following theorem establishes a relationship between the regularity index of the Hilbert function and the Castelnuovo-Mumford regularity.

Theorem 6 (Theorem 4.2 of [11]). *The Hilbert function $\mathcal{H}(t, I)$ agrees with the Hilbert polynomial for $t \geq 1 + \mathrm{reg}(I)$.*

Therefore, we have $\gamma(I) \leq 1 + \mathrm{reg}(I)$.

There is also a relationship between Theorem 5 and the Chardin-Philippon Theorem 7. (In [3] it is stated for projective schemes. For the sake of a presentation uniform with the rest of the current paper, we state it using homogeneous ideals.)

Theorem 7 ([3]). *Let J be the homogeneous ideal corresponding to a zero-dimensional component of the homogeneous ideal I generated by $f_1, \ldots, f_r$ of total degrees $d_1, \ldots, d_r$. Then* $\mathrm{reg}(J) \leq (d_1 - 1) + \cdots + (d_r - 1)$.

Thus, if the ideal I in Theorem 5 does not have a trivial component in its primary decomposition (cf. Section 4.1), then Theorems 6 and 7 imply the upper bound of Theorem 5. Such an ideal can be found in Example 8.

Example 8. The ideal $I = \langle f_1, f_2, f_3 \rangle$, where $f_1 = x_1 x_2$, $f_2 = x_2(x_1 + x_2 - x_3)$, and $f_3 = x_1(x_1 + x_2 - x_3)$ does not have any trivial component. Its primary decomposition is

$$\langle x_1, x_2 \rangle \cap \langle -x_1 + x_3, x_2 \rangle \cap \langle x_1, -x_2 + x_3 \rangle.$$

Thus the Chardin-Philippon Theorem 7 is applicable in the way discussed above. □

In contrast, Example 25 shows an ideal I with trivial component where Theorem 7 is not applicable in the same way.

Is the upper bound of Theorem 5 sharp? It is shown later by Corollary 19 that this is indeed the case if the ideal I only has the trivial root. But, it is not sharp for the ideals of Examples 8 and 25. The regularity indices of the corresponding ideals are 1 and 2, whereas the upper bounds are 4 and 3.

4. Properties of Ideal Quotients, Hilbert Functions, and Primary Ideals

For the convenience of the reader, this section first reviews some key foundational results from various sources used in the proof of the main results. We first discuss basic properties ideal quotients, primary ideals, and Hilbert functions. This is followed by a discussion of properties of primary ideals and the associated Hilbert functions needed in the proof of the main results.

4.1. Ideal Quotients

We review basic properties of ideal quotients [18, 17, 14, 30].

Proposition 9 ([30]). *Let I and J be ideals. Then*

$$(I \cap J) : f \;=\; (I : f) \cap (J : f).$$

In certain cases, the ideal quotient can be determined by simple formulas as expressed below.

Theorem 10 ([30]). *Let I be an ideal $\subseteq \mathbb{F}[x_0, \ldots, x_n]$.*

1. *If f is contained in I, then $I : f = \mathbb{F}[x_0, \ldots, x_n]$.*
2. *If f is not contained in any of the prime ideals of the primary decomposition of I, then $I : f = I$, and conversely.*

4.2. Primary Ideals

Note that an ideal that only has the trivial root $(0, \ldots, 0)$ is called a trivial ideal. If a trivial ideal is part of a reduced primary decomposition of a homogeneous ideal then it is called a trivial component. Certain homogeneous ideals do not have any trivial components. Particularly, homogeneous ideals with finitely many roots that are **complete intersections**, do not have a trivial component as stated in the following theorem.

Theorem 11 ([14]). *Let $g_1, \ldots, g_n$ be homogeneous polynomials in the polynomial ring $\mathbb{F}[x_0, x_1, \ldots, x_n]$ and assume that the g_i's have finitely-many (at least one) common projective roots. Then the ideal generated by the g_i's does not have a trivial component.*

PROOF. The well-known unmixedness theorem of complete intersections (see e.g. §6, p. 125, [14]) states that all the irreducible components of the variety of the ideal I generated by the g_i's have the same dimension. By the assumption of the theorem, the ideal I has at least one component whose set of roots has projective dimension 0 (in other words, affine dimension 1). However, a trivial component has (by definition) projective dimension -1 (in other words, affine dimension 0). Therefore the ideal I does not have a trivial component. □

We now discuss how primary decomposition interacts with certain ideal quotients to prove results needed in the proof of the main result.

Consider an ideal J with finitely many roots and without a trivial component. The corresponding primary decomposition of the divided ideal $J : x_0$ also lacks a trivial component and its primes are among the primes of the undivided ideal, as shown below.

Lemma 12. *Let the homogeneous ideal $J \subseteq \mathbb{F}[x_0, x_1, \ldots, x_n]$ have the reduced primary decomposition $Q_1 \cap \cdots \cap Q_l$ without trivial component. Then a reduced primary decomposition of $J : x_0$ is $(Q_{i_1} : x_0) \cap \cdots \cap (Q_{i_l} : x_0)$, for some subsequence $i_1, \ldots, i_l$ of $1, \ldots, k$, where $Q_{i_j} : x_0$ belongs to the same prime ideal as Q_{i_j} and, thus, no $Q_{i_j} : x_0$ is trivial.*

PROOF. By Theorem 9, $J : x_0 = (Q_1 : x_0) \cap \cdots \cap (Q_l : x_0)$. Furthermore, by Lemma 13, the divided ideal $Q_i : x_0$ either equals a primary ideal belonging to the prime of Q_i or equals $\mathbb{F}[x_0, x_1, \ldots, x_n]$. The latter ideal quotients can be dropped from the primary decomposition. □

Let $Q \subseteq \mathbb{F}[x_0, \ldots, x_n]$ be a homogeneous primary ideal whose variety precisely consists of one projective root (point). The divided ideal $Q : x_0$ again is a homogeneous primary ideal, whose variety consists of the same point, but with reduced multiplicity. Three cases occur which can be intuitively described by:

1. If the x_0 coordinate of the root of Q does not vanish, then dividing by x_0 does not have any effect.
2. If $x_0 = 0$ for the root of Q and the multiplicity of the coordinate $x_0 = 0$ is one then the root is removed by dividing by x_0.
3. Otherwise, $Q : x_0$ is a primary ideal with the same root of reduced multiplicity.

Lemma 13. *Let $P^k \subseteq Q \subseteq P \subseteq \mathbb{F}[x_0, \ldots, x_n]$, for some $k > 0$, where Q and P, respectively are homogeneous primary and homogeneous prime ideals. Furthermore, let the variety of P be exactly one projective point. Then*

1. *If $x_0 \notin P$ then $Q : x_0 = Q$.*
2. *If $x_0 \in Q$ then $Q : x_0 = \mathbb{F}[x_0, \ldots, x_n]$.*
3. *If $x_0 \in P$ and $x_0 \notin Q$ then $Q : x_0$ is a primary ideal with $P^k \subseteq Q : x_0 \subseteq P$.*

Proof.
1. Since x_0 is not contained in the prime ideal P, x_0 does not vanish on the root of P. Therefore, by Theorem 10, we have $Q : x_0 = Q$.
2. It follows from Theorem 10 because $x_0 \in Q$.
3. By the definition of ideal quotient, we have $Q \subseteq Q : x_0$. Therefore $P^k \subseteq Q \subseteq Q : x_0$.
   Next assume that $f \in Q : x_0$. Then $f x_0 \in Q$. Since $x_0 \notin Q$, we have $f \in P$. Therefore $Q : x_0 \subseteq P$.
   Next assume that $fg \in Q : x_0$ and $g \notin Q : x_0$. Then $f\,g\,x_0 \in Q$ and $g\,x_0 \notin Q$. Therefore $f \in P$. Thus $Q : x_0$ is primary.

□

4.3. Hilbert Function

The following material is taken from [14, 22].

If the ideal I is generated by the polynomials $f_1, \ldots, f_r$, then the Hilbert function $\mathcal{H}(t,\, I)$ is the dimension of the kernel of the dialytic matrix of the ideal generated by the f_i's of degree t [21]. The rows of the dialytic matrix for degree t consists of the coefficients of the monomial multiples of the f_i's of total degree t. (The row and column ordering of the dialytic matrix can be chosen arbitrarily.)

Subsequently we review some important properties of the Hilbert function:

As stated below, The Hilbert function is compatible with ideal inclusion as shown by the next theorem.

Theorem 14 ((9a), p. 158, [14]). *If $J \subseteq I$ then $\mathcal{H}(t,\, I) \leq \mathcal{H}(t,\, J)$.*

Further, the Hilbert function $\mathcal{H}(t,\, I)$ is not necessarily increasing monotonically with respect to the degree t. But for an important class of homogeneous ideals it is.

Theorem 15 (p. 157, [14]). *The Hilbert function $\mathcal{H}(t,\, I)$ of a homogeneous ideal I without trivial component is monotonically increasing with respect to the degree t.*

The following theorem rewrites the Hilbert function of the sum of two ideals in terms of a difference of Hilbert functions depending on the summands.

Theorem 16 ((9e), p. 158, [14]). *Let I be a homogeneous ideal and f be a homogeneous polynomial of total degree d in $\mathbb{F}[x_0, x_1, \dots, x_n]$. Then*

$$\mathcal{H}(t,\, I + \langle f\rangle) \,=\, \mathcal{H}(t,\, I) - \mathcal{H}(t-d,\, I : f).$$

The following theorem implies that the Hilbert polynomial is constant if the homogeneous ideal I has finitely many common roots.

Theorem 17 (§13, p. 160, [14]). *Let I be a homogeneous ideal with finitely many roots. Then for all $t \geq \gamma(I)$, the value of the Hilbert function $\mathcal{H}(t,\, I)$ equals the number of roots of I (counting multiplicities).*

The next theorem by Macaulay computes the Hilbert function of homogeneous ideals that are complete intersections. The statement of the theorem uses the notion of **rank** of an ideal generated by homogeneous polynomials in the variables $x_1, \dots, x_n$, which is defined by Macaulay, as the difference between n and the dimension of the set of common roots of the homogeneous polynomials regarded as an affine variety.

A homogeneous ideal of rank r is a complete intersection iff it is generated by r homogeneous n-variate polynomials. For example, a single projective point has dimension 1 in affine space and an ideal generated by n-variate homogeneous polynomials whose common roots consist of this single projective point has rank $n-1$. If this ideal has $n-1$ generators, then it is a complete intersection.

Theorem 18 ([21]). *Let $f_1, \dots, f_r$ be homogeneous polynomials of degrees $d_1, \dots, d_r$ in the variables $x_1, \dots, x_n$ and let I be the ideal generated by the f_i's. If the ideal I has rank r, then the value of the Hilbert function $\mathcal{H}(t,\, I)$ is the coefficient of x^t in*

$$(1-x^{d_1})(1-x^{d_2})\dots(1-x^{d_r})(1-x)^{-n}.$$

In other words, $\mathcal{H}(t,\, I)$ is the number of factors of degree t of the product

$$x_1^{d_1-1}x_2^{d_2-1}\dots x_r^{d_r-1}x_{r+1}^{t}\dots x_n^{t}.$$

We will apply certain aspects of Theorem 18 to two different types of ideals, that is, ideals that have only the trivial common root and ideals that have finitely-many common projective roots. The relevant conclusions from the theorem are summarized in the following corollary.

Corollary 19 ([21, 14]). *Using the notation of Theorem 18:*

1. *If $r = n$, then for all $t \geq 1 + (d_1 - 1) + \cdots + (d_n - 1)$, the Hilbert function $\mathcal{H}(t,\, I)$ vanishes and $\gamma(I) = 1 + (d_1 - 1) + \cdots + (d_n - 1)$.*
2. *If $r = n - 1$, then for all $t \geq (d_1 - 1) + \cdots + (d_n - 1)$, the Hilbert function $\mathcal{H}(t,\, I)$ equals $d_1 \ldots d_{n-1}$ and $\gamma(I) = (d_1 - 1) + \cdots + (d_n - 1)$.*

Proof.
1. If $r = n$, then $(1 - x^{d_1})(1 - x^{d_2}) \ldots (1 - x^{d_r})(1 - x)^{-n}$ is the polynomial $\frac{1-x^{d_1}}{1-x} \ldots \frac{1-x^{d_n}}{1-x}$. The coefficients of x^t with $t \geq 1 + (d_1 - 1) + \cdots + (d_n - 1)$ vanish. Furthermore, for $t = (d_1 - 1) + \cdots + (d_n - 1)$ the coefficient of x^t is 1.
2. Like Item 1 this can be derived from Theorem 18 by combinatorial arguments. However, we skip this proof because this result is also given by p. 164 of [14]. □

4.4. Putting Results about Primary Ideals and Hilbert Functions Together

Consider a set of homogeneous polynomials $f_1, \ldots, f_n$ in the variables $x_1, \ldots, x_n$, but viewed as elements of the polynomial ring $\mathbb{F}[x_0, x_1, \ldots, x_n]$, which also contains the variable x_0. Viewing the f_i's as members of the ring $\mathbb{F}[x_0, x_1, \ldots, x_n]$ corresponds to extending the variety of common roots of the f_i's from $(n-1)$-dimensional projective space to n-dimensional projective space by allowing x_0 to range freely. Intersecting the extended variety with the hyperplane of points with $x_0 = 0$ reduces its dimension by one.

Lemma 20. *Let $f_1, \ldots f_n$ be homogeneous polynomials in $\mathbb{F}[x_1, \ldots, x_n]$. Furthermore, adding the variable x_0 to the ring of polynomials, let J be the ideal generated by $f_1, \ldots, f_n$ in $\mathbb{F}[x_0, x_1, \ldots, x_n]$. Then $J : x_0 = J$.*

Proof. By the definition of ideal quotient, we have $J : x_0 \supseteq J$. It remains to show $J : x_0 \subseteq J$.

Let $p \in J : x_0$. Then $p\, x_0 \in J$. Therefore, there are polynomials $a_i \in \mathbb{F}[x_0, x_1, \ldots, x_n]$ such that

$$p\, x_0 = \sum_{i=1}^{n} a_i f_i.$$

Fix the a_i's. They can be written as $a_i = b_i x_0 + c_i$, where $b_i \in \mathbb{F}[x_0, x_1, \ldots, x_n]$ and $c_i \in \mathbb{F}[x_1, \ldots, x_n]$. Therefore

$$p\, x_0 = x_0 \sum_{i=1}^{n} b_i f_i + \sum_{i=1}^{n} c_i f_i.$$

Thus x_0 divides $\sum_{i=1}^{n} c_i f_i$ with does not contain x_0. This implies that $\sum_{i=1}^{n} c_i f_i$ vanishes. Therefore $p\, x_0 = x_0 \sum_{i=1}^{n} b_i f_i$ and $p = \sum_{i=1}^{n} b_i f_i$. Thus $p \in J$. □

The following lemma shows that the Hilbert function of an ideal is invariant under a certain extension of the underlying ring and a suitable extension of the ideal. This extension is useful because it allows us to embed a certain ideal that is a complete intersection into this extended ideal (see the proof of Theorem 5). This lemma is stated in §66 of [21]. But no proof is provided. Therefore we give a proof.

Lemma 21. *Let $f_1, \ldots f_n$ be homogeneous polynomials in $\mathbb{F}[x_1, \ldots, x_n]$ and let I be the ideal generated by the f_i's in $\mathbb{F}[x_1, \ldots, x_n]$. Furthermore, let K be the ideal generated by $f_1, \ldots f_n$ and x_0 in $\mathbb{F}[x_0, x_1, \ldots, x_n]$. Then $\mathcal{H}(t,\, I) = \mathcal{H}(t,\, K)$.*

Proof. Let J be the ideal generated by the f_i's in $\mathbb{F}[x_0, x_1, \ldots, x_n]$ (as opposed to $\mathbb{F}[x_1, \ldots, x_n]$). Observe that $K = J + \langle x_0 \rangle$. Then, by Theorems 16 and 20,

$$\begin{aligned} &\mathcal{H}(t,\, K) = \mathcal{H}(t,\, j + \langle x_0 \rangle) = \mathcal{H}(t,\, J) - \mathcal{H}(t-1,\, J : x_0) \\ &= \mathcal{H}(t,\, J) - \mathcal{H}(t-1,\, J) = \binom{t+n}{n} - \mathcal{V}(t,\, J) - \binom{t-1+n}{n} + \mathcal{V}(t-1,\, J) \\ &\qquad\qquad = \binom{t+n-1}{n-1} - (\mathcal{V}(t,\, J) - \mathcal{V}(t-1,\, J)). \end{aligned}$$

It remains to show that $\mathcal{V}(t,\, I) = \mathcal{V}(t,\, J) - \mathcal{V}(t-1,\, J)$.

Let $\mathcal{M}(t,\, I)$ and $\mathcal{M}(t,\, J)$ stand for the vector space of monomial multiples of the f_i's respectively in $\mathbb{F}[x_1, \ldots, x_n]$ and $\mathbb{F}[x_0, x_1, \ldots, x_n]$. Then

$$\mathcal{M}(t,\, J) = \mathcal{M}(t,\, I) + x_0\, \mathcal{M}(t-1,\, I) + \cdots + x_0^t\, \mathcal{M}(0,\, I).$$

Note that for $r \neq s$ we have that $x_0^r\mathcal{M}(t-r,\, I) \cap x_0^s\mathcal{M}(t-s,\, I) = \{0\}$. Therefore the above sum of vector spaces is a direct sum which commutes with the dimension function. Thus

$$\mathcal{V}(t,\, J) = \mathcal{V}(t,\, I) + \mathcal{V}(t-1,\, I) + \cdots + \mathcal{V}(0,\, I).$$

Therefore $\mathcal{V}(t,\, J) - \mathcal{V}(t-1,\, J) = \mathcal{V}(t,\, I)$. □

It is easy to verify that one can perturb a non-homogeneous polynomial by a constant such that it does not vanish on a list of given irreducible varieties, or, equivalently by Hilbert's Nullstellensatz, that the polynomial is not contained in the prime ideals of these varieties.

Lemma 22. *Let $P_1, \ldots, P_k \subseteq \mathbb{F}[x_1, \ldots, x_n]$ be non-homogeneous prime ideals and f be a non-homogeneous polynomial in $\mathbb{F}[x_1, \ldots, x_n]$. Then there is y in $\mathbb{F}$ such that $f + y \notin P_1, \ldots, P_k$.*

Proof. Recall that by Hilbert's Nullstellensatz and by the primality of P_i, the polynomial f is contained in P_i if and only if f vanishes on the variety V_i of P_i, that is, $f(V_i) = \{0\}$. Now, order the P_i's such that $f(V_1), \ldots, f(V_l)$ are infinite sets and $f(V_{l+1}), \ldots, f(V_k)$ are finite sets, for some l. Then for all y, we have that $(f+y)(V_1), \ldots, (f+y)(V_l)$ are infinite sets, obviously, different from $\{0\}$. Observe that we can choose $y \in \mathbb{F}$ such that $(f+y)(V_{l+1}), \ldots, (f+y)(V_k)$ are finite sets that are not equal to $\{0\}$. Therefore there exists a $y \in \mathbb{F}$ such that $(f+y)(V_1) \neq \{0\}, \ldots, (f+y)(V_k) \neq \{0\}$. □

It is possible now to complete a certain non-complete intersection. That is, from n homogeneous polynomials in n variables with finitely-many roots, a non-complete intersection, we will construct a complete intersection, that is, n homogeneous polynomials in $n+1$ variables with finitely-many roots.

Lemma 23. *Let $f_1, \ldots f_n$ be homogeneous polynomials in $\mathbb{F}[x_1, \ldots, x_n]$ of total degrees $d_1, \ldots, d_n$ with finitely-many common roots (including the possibility of no common roots). Furthermore, let $g_i = f_i + y_i\, x_0^{d_i}$, for $i = 1, \ldots, n$. Then there are $y_1, \ldots, y_n$ in $\mathbb{F}$ such that the g_i's have finitely-many common roots.*

Proof. The g_i's have finitely many common roots if and only if the g_i's have finitely-many projective roots with $x_0 = 0$ and the g_i's have finitely-many affine roots with $x_0 = 1$. The former holds because $g_i|_{x_0=0} = f_i$. In order to find y_i's such that the latter is valid, consider L_k, the ideal generated by $f_0 + y_0, \dots, f_k + y_k$, where y_0 is chosen arbitrarily from $\mathbb{F}$, say, $y_0 = 0$. For k from 0 to $n-1$, we choose y_{k+1} such that f_{k+1} is not contained in the (non-homogeneous) prime ideals of the primary decomposition of L_k. If f_{k+1} is not contained in the prime ideals then choose $y_{k+1} = 0$. If f_{k+1} is contained in one of the prime ideals then there is a suitable y_{k+1} according to Lemma 22. □

The construction suggested by Lemma 23 is used in Section 5 to establish the constancy of the Hilbert function of certain ideals, thus proving the main result about Hilbert functions (Theorem 5).

The next lemma studies a case of ideals where inclusion of ideals and computation of the regularity index are compatible, that is, when $I \supseteq J$ implies that $\gamma(I) \leq \gamma(J)$.

Lemma 24. *Let $g_1, \dots g_n$ be homogeneous polynomials in $\mathbb{F}[x_0, x_1, \dots, x_n]$ of total degrees $d_1, \dots, d_n$ with finitely-many common roots and let J be the ideal generated by the g_i's. If the ideal $I \supseteq J$ has no trivial component, then $\gamma(I) \leq (d_1 - 1) + \cdots + (d_n - 1) = \gamma(J)$.*

Proof. We will intersect the ideals I and J with a linear form that does not vanish on the varieties of I and J. This technique is also used in [14] in order to show that the Hilbert polynomial of an ideal that has finitely-many roots is constant.

Since $J \subseteq I$, the variety of I is contained in the variety of J. Therefore, since J has finitely-many roots, also I has finitely-many roots. Therefore we can choose a linear form l that does not vanish on the roots of J and I. Since I does not have a trivial component, by Theorem 10, we have $I : l = I$. Furthermore, since $J + \langle l \rangle \subseteq I + \langle l \rangle$, by Theorem 14, we have $\mathcal{H}(t,\, I + \langle l \rangle) \leq \mathcal{H}(t,\, J + \langle l \rangle)$. Next note that by the choice of the linear form l, the ideal $J + \langle l \rangle$ only has the trivial root. Now, by Corollary 19 and Theorem 16, for $t \geq 1 + (d_1 - 1) + \cdots + (d_n - 1)$,

$$\begin{aligned} 0 = \mathcal{H}(t,\, J + \langle l \rangle) \geq& \\ &\mathcal{H}(t,\, I + \langle l \rangle) = \mathcal{H}(t,\, I) - \mathcal{H}(t-1,\, I : l) = \mathcal{H}(t,\, I) - \mathcal{H}(t-1,\, I). \end{aligned}$$

Thus, for $t \geq 1 + (d_1 - 1) + \cdots + (d_n - 1)$, we have $\mathcal{H}(t-1,\, I) \geq \mathcal{H}(t,\, I)$. In other words, for $t \geq (d_1 - 1) + \cdots + (d_n - 1)$, the Hilbert function $\mathcal{H}(t,\, I)$ is monotonically decreasing.

Next recall that by assumption the ideal I does not have a trivial component. Therefore, by Theorem 15, the Hilbert function $\mathcal{H}(t, I)$ is monotonically increasing. Thus, for $t \geq (d_1 - 1) + \cdots + (d_n - 1) \geq \gamma(I)$, the Hilbert function $\mathcal{H}(t, I)$ is constant. To conclude the proof, observe that by Corollary 19, the regularity index $\gamma(J) = (d_1 - 1) + \cdots + (d_n - 1)$. □

5. Proof of Constancy of the Hilbert Function

Using the results from Section 4, we are ready to prove the upper bound for the regularity index of the ideal generated by n homogeneous polynomials in n variables that have finitely many common roots. Before stating the proof formally, let us discuss its intuition by an example.

Example 25. Let $f_1 = x_1^2$, $f_2 = x_2$, and $f_3 = x_1 x_3$. Then the primary decomposition of the ideal I generated by the f_i's is

$$\langle x_1, x_2 \rangle \cap \langle x_1^2, x_3, x_3 \rangle$$

which shows that the f_i's have finitely many roots. That is, the only and simple projective root is $(0 : 0 : 1)$. Furthermore, note that the trivial component of I is $\langle x_1^2, x_2, x_3 \rangle$.

We want to show that from a certain suitable degree the Hilbert function of the ideal I is constant. In order to achieve this, we intend to relate the ideal I to some other ideal J that is a certain complete intersection. Thus let, $g_1 = x_1^2 + x_0^2$, $g_2 = x_2 + x_0$, and $g_3 = x_1 x_3 + x_0^2$. Then the primary decomposition of the ideal J generated by the g_i's is

$$\langle x_0 + x_2, x_1, x_2^2 \rangle \cap \langle x_0 + x_2, x_1 - x_3, x_2 + jx_3 \rangle \cap \langle x_0 + x_2, x_1 - x_3, x_2 - jx_3 \rangle ,$$

where $j^2 = -1$. Now $(0 : 0 : 0 : 1)$ is a double projective root whereas the projective points $(j : 1 : -j : 1)$ and $(-j : 1 : j : 1)$ are additional simple roots for J. Notice that the ideal J is a complete intersection, that is, has finitely-many roots, and consists of 3 homogeneous polynomials in 4 variables. Moreover, being a complete intersection, J does not have any trivial component.

Furthermore, accordingly the ideal quotient $J : x_0$ has the primary decomposition

$$\langle x_0 + x_2, x_1, x_2 \rangle \cap \langle x_0 + x_2, x_1 - x_3, x_2 + jx_3 \rangle \cap \langle x_0 + x_2, x_1 - x_3, x_2 - jx_3 \rangle ,$$

with simple roots $(0:0:0:1)$, $(j:1:-j:1)$, and $(-j:1:j:1)$. We observe that the ideal $J:x_0$ has the same roots as the ideal J. However, the multiplicities of the projections of the roots with $x_0 = 0$ onto the x_0-coordinate axis are reduced by one. Therefore the roots (taking into account multiplicities) of the system $f_1, f_2, f_3,\, x_0$ are the roots of the ideal J minus the roots of the ideal $J:x_0$. Thus, one can write the Hilbert function of the ideal I in terms of the Hilbert functions of the ideals J and $J:x_0$. Furthermore, notice that, like the ideal J, the ideal $J:x_0$ does not have a trivial component either. Using these observations we will derive the suitable degree from which on the Hilbert function of the ideal I is constant. This suitable degree will turn out to be the same degree as the monomial multiples used to construct the Macaulay matrix of the f_i's □

Proof (Theorem 5). Let I be the ideal generated by the f_i's in $\mathbb{F}[x_1, \ldots, x_n]$. Furthermore, let K be the ideal generated by $f_1, \ldots f_n$ and x_0 in $\mathbb{F}[x_0, x_1, \ldots, x_n]$. Then, by Lemma 21,

$$\mathcal{H}(t,\, I) \;=\; \mathcal{H}(t,\, K).$$

Next, let J be the ideal generated by $g_1 = f_1 + y_1 x_0^{d_1}, \ldots, g_n = f_n + y_n x_0^{d_n}$ where the y_i's are chosen such that the g_i's have finitely many common roots as in Lemma 23. Since $K \;=\; J + \langle x_0 \rangle$, we have by Theorem 16 that

$$\mathcal{H}(t,\, K) \;=\; \mathcal{H}(t,\, J + \langle x_0 \rangle) \;=\; \mathcal{H}(t,\, J) \;-\; \mathcal{H}(t-1,\, J:x_0).$$

By Corollary 19, for all t greater than or equal to $(d_1 - 1) + \cdots + (d_n - 1)$ we have that $\mathcal{H}(t,\, J)$ is constant. By Theorem 11, the ideal J does not have a trivial component. Therefore, by Lemma 12, the ideal $J:x_0$ has finitely many common roots and does not have a trivial component. Since by the definition of ideal quotient $J \subseteq J:x_0$, applying Lemma 24, for all $t-1$ greater than or equal to $(d_1 - 1) + \cdots + (d_n - 1)$ we have that $\mathcal{H}(t-1,\, J)$ is constant. Therefore, for all $t \geq 1 + (d_1 - 1) + \cdots + (d_n - 1)$ we have that $\mathcal{H}(t,\, K)$ is constant. □

6. Proof of the main Theorem 1

Given a set of multivariate parametric homogeneous polynomials $f_1, \ldots, f_n$ in the variables $x_1, \ldots, x_n$ with finitely-many common (generic) roots, the goal is to show that under a specialization ϕ that increases the number of common roots, the maximal-rank minors of the specialized Macaulay matrix of these polynomials vanish. This is established using the property that the Hilbert function of the ideals respectively generated by the f_i's and by the specialized polynomials $\phi(f_i)$'s is constant from a certain suitable degree that is independent from the specialization ϕ.

Proof (Theorem 1). Let $e = 1 + (d_1 - 1) + \cdots + (d_n - 1)$ and let I and J be the ideal generated by the f_i's and respectively by the $\phi(f_i)$'s. By Theorems 17 and 5, we have to show that $\mathcal{H}(e, I) < \mathcal{H}(e, J)$ implies that all maximal-rank minors of the Macaulay matrix of the f_i's vanish under the specialization ϕ. Note that the dialytic matrix of J of degree e is obtained from the dialytic matrix of I of degree e by the specialization ϕ. Therefore $\mathcal{H}(e, I) < \mathcal{H}(e, J)$ implies that any maximal-rank minor of the dialytic matrix of I vanishes under specialization. Since the Macaulay matrix of the f_i's is a submatrix of the dialytic matrix of I of degree e with the same number of columns, $\mathcal{H}(e, I) < \mathcal{H}(e, J)$ implies that any maximal-rank minor of the Macaulay matrix of the f_i's vanishes under specialization by ϕ. This completes the proof. □

7. Conclusion

It is proved in this paper that the vanishing of the maximal-rank minors of the Macaulay matrix of a parametric polynomial system under a specialization is a necessary condition for the specialized polynomials to have additional common roots (Theorem 1), even if the multiplicity of a common root increases. This result generalizes results in [16] as well as in [7]. This result is proved using Theorem 5, which gives a bound on the degree from which on the Hilbert function of a certain zero-dimensional ideal which is not necessarily a complete intersection, becomes constant; this result about Hilbert functions is of independent interest.

Many interesting questions arise for future investigations. For example, is the gcd of the maximal-rank minors of the dialytic matrix of suitable degree discussed above also the generator of some elimination ideal, analogous to the projective resultant, and if so, what is it? What precisely happens to the Macaulay matrix when the parametric polynomials are specialized to have infinitely-many common roots? Answers to these questions can have significant practical implications as a large class of parametrized polynomial systems can be analyzed using matrix based resultant formulations. Such methods have typically lower computational complexity (both in time and space) in contrast to Gröbner basis algorithms.

Acknowledgments

The authors thank Professor Robert Lewis for discussions about maximal-rank minors of Macaulay matrices and Professor Stephen Watt for proposing the use of singular value decomposition for the application of Section 2.2.4.

References

[1] S. Barnett. A new look at classical algorithms for polynomials resultant and g.c.d. calculation. *SIAM Rev.*, 16:193–206, 1974.

[2] L. Busé, M. Elkadi, and B. Mourrain. Resultant over the residual of a complete intersection. *J. Pure Appl. Algebra*, 164(1-2):35–57, 2001. Effective methods in algebraic geometry (Bath, 2000).

[3] M. Chardin. Bounds for Castelnuovo-Mumford regularity in terms of degrees of defining equations. *NATO Sci. Ser. II Math. Phys. Chem.*, 115:67–73, 2003.

[4] A. Chtcherba, D. Kapur, and M. Minimair. Cayley-Dixon resultant matrices of multi-univariate composed polynomials. In V. Ganzha and E. Mayr, editors, *Computer Algebra in Scientific Computing*, volume 3718 of *Lecture Notes in Computer Science*, pages 125–137, Berlin Heidelberg, 2005. Springer Verlag. 8th International Workshop, CASC 2005, Kalamata, Greece, September 2005, Proceedings.

[5] A. Chtcherba, D. Kapur, and M. Minimair. Cayley-Dixon projection operator for multi-univariate composed polynomials. Accepted by J. Symbolic Computation, 2008.

[6] A. D. Chtcherba. *A new Sylvester-type Resultant Method based on the Dixon-Bézout Formulation.* PhD dissertation, University of New Mexico, Department of Computer Science, Aug 2003.

[7] A. D. Chtcherba and D. Kapur. Conditions for determinantal formula for resultant of a polynomial system. In *ISSAC '06: Proceedings of the 2006 international symposium on Symbolic and algebraic computation*, pages 55–62, New York, NY, USA, 2006. ACM.

[8] D. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry.* Springer Verlag, New York, Berlin, Heidelberg, 2nd edition, 2004.

[9] B. H. Dayton and Z. Zeng. Computing the multiplicity structure in solving polynomial systems. In *ISSAC'05*, pages 116–123 (electronic). ACM, New York, 2005.

[10] D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry.* Number 150 in Graduate Texts in Mathematics. Springer-Verlag, New York, 1995.

[11] D. Eisenbud. *The geometry of syzygies*, volume 229 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005. A second course in commutative algebra and algebraic geometry.

[12] G. H. Golub and C. F. van Loan. *Matrix Computations.* Johns Hopkins University Press, Baltimore, MD, USA, 3rd edition, 1996.

[13] G.-M. Greuel, G. Pfister, and H. Schönemann. Singular 3.1.0. A computer algebra system for polynomial computations, Department of Mathematics, University of Kaiserslautern, 2009. http://www.singular.uni-kl.de.

[14] W. Gröbner. *Moderne Algebraische Geometrie.* Springer Verlag, Wien, Innsbruck, 1949.

[15] D. Hilbert. Ueber die Theorie der algebraischen Formen. *Mathematische Annalen*, 36:473–534, 1890.

[16] D. Kapur, T. Saxena, and L. Yang. Algebraic and geometric reasoning using the Dixon resultants. In *ACM ISSAC 94*, pages 99–107, Oxford, England, July 1994.

[17] E. Lasker. Bemerkungen und Fehlerverzeichnis zu meiner Arbeit "Zur Theorie der Moduln und Ideale". *Mathematische Annalan*, 60(4):607–609, 1905.

[18] E. Lasker. Zur Theorie der Moduln und Ideale. *Mathematische Annalan*, 60(1):20–116, 1905.

[19] R. Lewis. Comparing acceleration techniques for the dixon and macaulay resultants. *Mathematics and Computers in Simulation*, 2008. Accepted.

[20] F. S. Macaulay. Some formulae in elimination. *Proceedings of the London Mathematical Society*, 35:3–27, May 1903.

[21] F. S. Macaulay. On the resolution of a given modular system into primary systems including some properties of Hilbert numbers. *Mathematische Annalen*, 74:66–121, 1913.

[22] F. S. Macaulay. *The algebraic theory of modular systems*. Cambridge Mathematical Library, 1916.

[23] M. Minimair. Dense resultant of composed polynomials. *J. Symbolic Computation*, 36(6):825–834, December 2003.

[24] M. Minimair. MR. http://minimair.org/MR.mpl, April 2003. Macaulay resultant package for Maple.

[25] M. Minimair. Sparse resultant under vanishing coefficients. *J. Algebraic Combinatorics*, 18(1):53–73, July 2003.

[26] M. Minimair. DR. http://minimair.org/dr, 2007. Maple package for computing Dixon projection operators (resultants).

[27] T. Mora. *Solving polynomial equation systems. II*, volume 99 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, 2005. Macaulay's paradigm and Gröbner technology.

[28] I. Peeva and M. Stillman. Open problems on syzygies and Hilbert functions. *J. Commut. Algebra*, 1(1):159–195, 2009.

[29] B. van der Waerden. Eine Verallgemeinerung des Bezoutschen Theorems. *Mathematische Annalen*, 99, 1928.

[30] B. L. van der Waerden. *Algebra II*. Springer-Verlag, Berlin, Heidelberg, New York, 5th edition, 1967.

[31] O. Zariski and P. Samuel. *Commutative algebra. Vol. 1*. Springer-Verlag, New York, 1975. With the cooperation of I. S. Cohen, Corrected reprinting of the 1958 edition, Graduate Texts in Mathematics, No. 28.

[32] O. Zariski and P. Samuel. *Commutative algebra. Vol. II*. Springer-Verlag, New York, 1975. Reprint of the 1960 edition, Graduate Texts in Mathematics, Vol. 29.

[33] Jianmin Zheng, Thomas W. Sederberg, Eng-Wee Chionh, and David A. Cox. Implicitizing rational surfaces with base points using the method of moving surfaces. In *Topics in algebraic geometry and geometric modeling*, volume 334 of *Contemp. Math.*, pages 151–168. Amer. Math. Soc., Providence, RI, 2003.