An Introduction to the Theory of Resultants

Peter F. Stiller*

Introduction

This report is meant to serve as a "working man's" introduction to resultants. It is aimed at engineers, computer scientists, and applied mathematicians who encounter systems of polynomial equations in their practice. As such, it is more of a "how to" manual than a theoretical study.

Most of the techniques and results presented here can be found in the classical literature. Unfortunately, those results are scattered in numerous, sometimes out of print, sources. We have brought them all together for the practitioner's use. Simple examples illustrate each technique, and the reader should have little difficulty in applying the various methods to his or her particular problem.

Applicability

Resultants are used to solve systems of polynomial equations, to determine whether or not solutions exist, or to reduce a given system to one with fewer variables and/or fewer equations.

Input

The typical input will be a system of m equations in n-variables:

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= 0 \\ &\vdots \\ f_m(x_1, \ldots, x_n) &= 0. \end{aligned}$$

Each equation has an associated degree $d_i \geq 1$. Recall that $f_i(x_1, \ldots, x_n)$ has degree d_i if all monomials $x_1^{e_1} x_2^{e_2} \ldots x_n^{e_n}$ appearing in f_i have $\sum_{i=1}^{n} e_i \leq d_i$ and at least one monomial has $\sum_{i=1}^{n} e_i = d_i$. Example: $f(x_1, x_2, x_3) = 3x_1^2 x_3 + 4x_1 x_2 - x_2 + 7x_3 - 1$ has degree $d = 3$. The integers $m, n, d_1, \ldots, d_m$ are important indicators of the specific resulant that will need to be employed.

Output

There are two essentially different cases:

Case 1: $m > n$ (overdetermined) This is the case where we have more equations than unknowns, and where we generally expect to have no solutions. The resultant will be a system of equations (one equation when $m = n+1$) in the symbolic coefficients of the f_i that has the following property: when we substitute the specific numerical coefficients of the f_i, we will get zero in every equation in the resultant system if and only if the original overdetermined system has a solution.

Case 2: $m \leq n$ (exact and underdetermined) In this case the number of equations is less than or equal to the number of variables, and we expect to have solutions. In fact, if we allow complex solutions and solutions at infinity, we are guaranteed to have solutions.

*Professor of Mathematics and Computer Science, Texas A&M University, College Station, TX 77843–3363

Of course, only when $m = n$ do we expect a finite number s of solutions. Bezout's Theorem then provides a count of $s = d_1 d_2 \dots d_m$ solutions (counting complex solutions, solutions at infinity, and counting with appropriate multiplicities). Unfortunately, the possibility also exists (even when $m = n$) that there will be an infinite number of solutions.

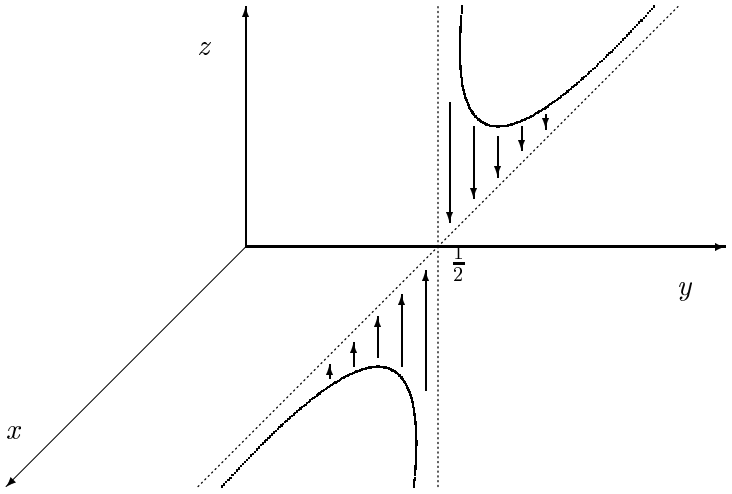
In general, for $m \leq n$, the resultant will be the one equation in $n - m + 1$ of the variables. In effect, the resultant makes it possible for us to eliminate $m - 1$ of the variables. For example, if we choose to eliminate $x_{n-m+2}, \dots, x_n$, then the resultant R will be a polynomial $R(x_1, \dots, x_{n-m+1})$ in the remaining variables. If $(\alpha_1, \dots, \alpha_{n-m+1})$ is a solution to $R = 0$, then there will exist values $\alpha_{n-m+2}, \dots, \alpha_n$ such that $(\alpha_1, \dots, \alpha_{n-m+1}, \alpha_{n-m+2}, \dots, \alpha_n)$ is a solution to the original system. (One must be a little careful here. The system should be modified to make it homogeneous with respect to $x_{n-m+2}, \dots, x_n$ by adding appropriate powers of a variable w. The values $\alpha_{n-m+2}, \dots, \alpha_n$ should be regarded as the coordinates of a point $(\alpha_{n-m+2} : \cdots : \alpha_n : 1)$ in projective $m - 1$ space $\mathbb{P}^{m-1}$. We must allow for the possibility that this point will be at infinity, where $w = 0$. In that case, a solution to $R = 0$ would not necessarily give rise to a solution of the original system.)

For example, consider the system of $m = 2$ equations in $n = 3$ variables: $4xyz - 1 = 0$ and $y + xz - 1 = 0$. The resultant eliminating z is $R(x, y) = x(4y^2 - 4y + 1)$. When $x = 0$ we will have $R = 0$, but clearly our system has no solution when $x = 0$. However, homogenizing with respect to z gives the system

$$4xyz - w = 0 \quad \text{and} \quad (y - 1)x + xz = 0.$$

Now when we look at the condition $x = 0$, we find that $(z, w) = (1 : 0)$ is a solution. This is a point at infinity.

Notice that we also have solutions to $R = 0$, when $x \neq 0$ by taking $y = \frac{1}{2}$. This yields $z = \frac{1}{2x}$. Geometrically the solution set is a hyperbola in the plane $y = \frac{1}{2}$ in space. The resultant "projects" that hyperbola to the line $y = \frac{1}{2}$ in the xy-plane, except that $(x, y) = (0, \frac{1}{2})$ is not hit.



In this context (the underdetermined case) the resultant can be viewed as a projection of the nominally $n - m$ dimensional locus of solutions in $\mathbb{R}^n$ to an $n - m$ dimensional locus (hypersurface) in $\mathbb{R}^{n-m+1}$. Note that in our example $n = 3$, $m = 2$, and we are projecting the one-dimensional locus of solutions in $\mathbb{R}^3$ to a one-dimensional locus in $\mathbb{R}^2$, where the locus is described by one equation $y - \frac{1}{2} = 0$.

Approach in This Paper

We begin with the first major distinction in methods, namely the one based on the number of variables n. The case $n = 1$ of a single variable is discussed in §1. We then move on in §2 to the multivariate case $n \geq 2$. The final two sections, §3 and §4, cover various geometric and combinatorial issues.

Table of Resultants

n	m	Type of resultant to use	Notes
1	2	Determinant of the Sylvester matrix	This is what is most commonly thought of as the resultant.
1	≥ 3	Requires a system of equations	See the discussion in van der Waerden [**?**].
≥ 2	$m = n + 1$	Macaulay resultant	This is computed as the quotient of two determinants. It is a polynomial in the symbolic coefficients and is zero if and only if the system has a solution.
≥ 2	$m \geq n + 2$	Requires a system of equations	See van der Waerden [**?**].
≥ 2	$m = n$	U-resultant or generalized characteristic polynomial	This resultant is designed to find the finite set of all solutions to the system of equations.
≥ 2	$m < n$	Macaulay resultant using $m - 1$ variables, while treating the other $n - m + 1$ variables as included in the coefficients.	The result is a single polynomial in the remaining $n-m+1$ variables.

Note: One can also employ the standard Sylvester resultant in the multivariate case, using it iteratively to successively eliminate variables. For example, with three equations in three unknowns $f(x, y, z) = 0$, $g(x, y, z) = 0$, and $h(x, y, z) = 0$, we can take the resultant of f and g treating z as the only variable to get $R_1(x, y)$. Likewise, we can take the resultant of g and h again treating z as the only variable to get $R_2(x, y)$. Finally, the resultant of R_1 and R_2 with y as the variable yields $R(x)$, whose roots can then be found using standard root finding methods.

1 Resultants of Polynomials in One Variable

1.1 The Basic Case – Two Polynomials and the Sylvester Matrix

Given two positive integers $r, s \geq 1$ and two polynomials in one variable

$$f(x) = a_r x^r + \cdots + a_1 x + a_0 \quad \text{and} \quad g(x) = b_s x^s + \cdots + b_1 x + b_0$$

of degree less than or equal to r and s respectively, we define their resultant $R_{r,s}(f,g)$ by Sylvester's formula:

$$R_{r,s}(f,g) = \det \begin{pmatrix} a_0 & a_1 & & \cdots & a_r & 0 & \cdots & & 0 \\ 0 & a_0 & a_1 & \cdots & \cdots & a_r & 0 & \cdots & 0 \\ \vdots & & & & & & & & \\ 0 & 0 & \cdots & 0 & a_0 & a_1 & & \cdots & a_r \\ b_0 & b_1 & \cdots & & b_{s-1} & b_s & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & & \cdots & & b_s & \cdots & 0 \\ \vdots & & & & & & & & \\ 0 & 0 & \cdots & & 0 & b_0 & b_1 & \cdots & b_s \end{pmatrix}$$

which is the determinant of an $r+s$ by $r+s$ matrix with s rows involving the a's and r rows involving the b's.

Example 1:

$$\begin{aligned} &R_{2,2}(a_2x^2 + a_1x + a_0, b_2x^2 + b_1x + b_0) \\ &\quad = a_0^2b_2^2 + a_0a_2b_1^2 - a_0a_1b_1b_2 + a_1^2b_0b_2 - a_1a_2b_0b_1 + a_2^2b_0^2 - 2a_0a_2b_0b_2. \end{aligned}$$

Note that in this example each monomial in the resultant has total degree $r+s = 4$ and is bihomogeneous of bidegree $(s,r) = (2,2)$ in the a's and b's respectively. This is true in general. Notice also that the general bihomogeneous polynomial of bidegree $(2,2)$ has 36 terms—any one of $a_0^2, a_1^2, a_2^2, a_0a_1, a_0a_2, a_1a_2$ times any one of $b_0^2, b_1^2, b_2^2, b_0b_1, b_0b_2, b_1b_2$. However, only seven of these monomials occur in $R_{2,2}$. □

Basic Properties of the Resultant $R_{r,s}(f,g)$

1. Relationship to Common Roots: $R_{r,s}(f,g) = a_r^s b_s^r \prod_{i,j}(x_i - y_j)$ where $x_1, \ldots, x_r$ are the roots of f and $y_1, \ldots, y_s$ are the roots of g. (Here we are assuming $a_r \neq 0$ and $b_s \neq 0$.) Thus $R_{r,s}(f,g)$ will be zero if and only if f and g have a root in common.

2. Irreducibility: $R_{r,s}(f,g) \in \mathbb{Z}[a_0, \ldots, a_r, b_0, \ldots, b_s]$ is irreducible, i.e., the resultant is an irreducible polynomial with integer ($\mathbb{Z}$) coefficients in $(r+1)(s+1) = rs+s+r+1$ variables.

3. Symmetry: $R_{r,s}(f,g) = (-1)^{rs} R_{s,r}(g,f)$

4. Factorization: $R_{r_1+r_2,s}(f_1f_2, g) = R_{r_1,s}(f_1,g)R_{r_2,s}(f_2,g)$.

Example 2: $R_{1,2}(a_1x + a_0, b_2x^2 + b_1x + b_0) = a_0^2b_2 - a_0a_1b_1 + a_1^2b_0$. Now consider

$$\begin{aligned} &R_{2,2}((a_1x + a_0)(c_1x + c_0), b_2x^2 + b_zx + b_0) \\ &\quad = R_{2,2}(a_1c_1x^2 + (a_0c_1 + a_1c_0)x + a_0c_0, b_2x^2 + b_1x + b_0). \end{aligned}$$

This can be computed using Example 1 or by using property 4 above:

$$\begin{aligned} &R_{2,2}((a_1x+a_0)(c_1x+c_0), b_2x^2+b_1x+b_0) \\ &\qquad = R_{1,2}(a_1x+a_0, b_2x^2+b_1x+b_0)R_{1,2}(c_1x+c_0, b_2x^2+b_1x+b_0). \end{aligned}$$

Thus if the polynomials you are taking the resultant of can be factored, then the resultant can be factored! □

Other Formulas for the Resultant – Method of Bezout:

Suppose $f = a_rx^r + \cdots + a_0$ and $g = b_sx^s + \cdot + b_0$ and that $a_0 = 1$, then letting

$$\frac{g(x)}{f(x)} = r_0 + r_1x + r_2x^2 + \cdots$$

we have

$$R_{r,s}(f,g) = \det \begin{pmatrix} r_s & \cdots & r_{s+r-1} \\ r_{s-1} & \cdots & r_{s+r-2} \\ r_{s-r+1} & \cdots & r_s \end{pmatrix}$$

which is an $r \times r$ determinant. Note that $a_0 = 1$ is not a serious restriction, because as long as $a_0 \neq 0$, we can scale f to make $a_0 = 1$. Also note that the r_i's are polynomial expressions in the a_j's and b_k's.

Example 3:

$$\begin{aligned} f(x) &= 2x^2 - 3x + 1 \\ g(x) &= 5x^2 + x - 6 \\ \frac{g(x)}{f(x)} &= (-6 + x + 5x^2)(1 + 3x + 7x^2 + 15x^3 + \cdots) = -6 - 17x - 34x^2 - 68x^3 + \cdots \end{aligned}$$

and

$$R_{2,2}(f,g) = \det \begin{pmatrix} r_2 & r_3 \\ r_1 & r_2 \end{pmatrix} = \det \begin{pmatrix} -34 & -68 \\ -17 & -34 \end{pmatrix} = 0$$

which is correct because $x = 1$ is a common root. □

Suppose now that f and g have the same degree, so $r = s$, and let $[ij]$ stand for the expression $a_ib_j - b_ia_j$. The Bezout-Cayley formula for the resultant is the $r \times r$ determinant

$$R_{r,r}(f,g) = \det \begin{pmatrix} [01] & [02] & [03] & [0r] \\ [02] & [03]+[12] & [04]+[13] & [1r] \\ [03] & [04]+[13] & [05]+[14]+[23] & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ [0r] & [1r] & [2r] & [r-1r] \end{pmatrix}$$

Example 4:

$$R_{2,2}(f,g) = \det \begin{pmatrix} a_0b_1 - a_1b_0 & a_0b_2 - a_2b_0 \\ a_0b_2 - a_2b_0 & a_1b_2 - a_2b_1 \end{pmatrix}$$

which can be checked against Example 1. □

Various intermediate forms exist that lie between the $r \times r$ Bezout-Cayley form and the $2r \times 2r$ Sylvester form.

1.2 Discriminants and Resultants

The discriminant $\Delta(f)$ of a polynomial $f = a_r x^r + \cdots + a_0$, $a_r \neq 0$, is essentially the resultant of f and its derivative f'. The exact relationship is

$$\Delta(f) = \frac{1}{a_r} R_{r,r-1}(f, f')$$

which is a homogeneous polynomial of degree $2r-2$ in the $r+1$ variables $a_0, \ldots, a_r$.

Example 5:

$$\Delta(a_0 + a_1 x + a_2 x^2 + a_3 x^3) = 27a_0^2 a_3^2 + 4a_0 a_2^3 + 4a_1^3 a_3 - a_1^2 a_2^2 - 18a_0 a_1 a_2 a_3.$$

Notice that only 5 out of a possible 35 terms (the number of monomials of degree 4 in 4 variables) actually occur. □

In general $\Delta(a_0 + \cdots + a_r x^r)$ could consist of as many as $\binom{3r-2}{2r-2} = \frac{(3r-2)!}{(2r-2)!r!}$ terms, but in reality it consists of far fewer. For example when $r = 5$ (i.e., when f is a quintic, the number of monomials of degree $8 (= 2r-2)$ in $6 (= r+1)$ variables is 1287, but only 59 occur in the discriminant.

Just as the discriminant can be defined in terms of the resultant, the resultant can be defined in terms of the discriminant:

$$(R_{r,s}(f,g))^2 = (-1)^{rs} \frac{\Delta(fg)}{\Delta(f)\Delta(g)}$$

when $a_r \neq 0$ and $b_s \neq 0$.

1.3 Finding the Common Roots – Subresultants

Again, suppose we are given two polynomials in a single variable x, say

$$f(x) = a_r x^r + \cdots + a_1 + a_0 \quad \text{and} \quad g(x) = b_s x^s + \cdots + b_1 x + b_0,$$

of degrees $r \geq 1$ and $s \geq 1$ respectively. (We assume that $a_r \neq 0$ and $b_s \neq 0$.) As we saw above, the resultant $R_{r,s}(f,g)$ of f and g will zero if and only if f and g have a common root. Two questions immediately occur:

QUESTION 1: Suppose $R_{r,s}(f,g) = 0$, so that f and g have at least one common root, can we determine how many roots they have in common? This is the same as asking for the degree $1 \leq d \leq \min(r,s)$ of the greatest common divisor $h(x)$ of $f(x)$ and $g(x)$.

QUESTION 2: Can we find the common roots?

Question 1 can be answered using the notion of a subresultant. To understand this idea, we first recall the source of the Sylvester matrix whose determinant gives us the resultant $R_{r,s}(f,g)$. To say that $f(x)$ and $g(x)$ have one or more common roots is to say that they have a common factor $h(x)$ of degree $d \geq 1$. This means that we can write

$$f(x) = h(x)\tilde{f}(x) \quad \text{and} \quad g(x) = h(x)\tilde{g}(x).$$

It follows that

$$\tilde{g}(x)f(x) + (-\tilde{f}(x))g(x) = 0$$

because

$$\tilde{g}(x)f(x) = \tilde{g}(x)h(x)\tilde{f}(x) = g(x)\tilde{f}(x).$$

Thus when $f(x)$ and $g(x)$ have one or more common roots, there will exist non-zero polynomials

$$s(x) = s_{s-1}x^{s-1} + \cdots + s_1 x + s_0 \quad \text{and} \quad t(x) = t_{r-1}x^{r-1} + \cdots + t_1 x + t_0$$

of degrees at most $s-1 \geq 0$ and $r-1 \geq 0$ respectively, with the property that

$$s(x)f(x) + t(x)g(x) = 0. \tag{1}$$

Conversely, if two such non-zero polynomials $s(x)$ and $t(x)$ can be found that satisfy (**??**), then $f(x)$ and $g(x)$ will have one or more common roots. This is because all r roots of $f(x)$ must then be roots of $t(x)g(x)$, but the degree of $t(x)$ is at most $r-1$, meaning that at least one root of $f(x)$ is also a root of $g(x)$.

If we multiply the left-hand side of (**??**) out and collect terms we get

$$\begin{aligned}
&(s_{s-1}a_r + t_{r-1}b_s)x^{r+s-1} + (s_{s-1}a_{r-1} + s_{s-2}a_r + t_{r-1}b_{s-1} + t_{r-2}b_s)x^{r+s-2} + \cdots \\
&\quad + \left(\sum_{j=1}^{i} s_{s-j}a_{r+j-i} + \sum_{k=1}^{i} t_{r-k}b_{s+k-i} \right) x^{r+s-i} + \cdots \\
&\quad + (s_1 a_0 + s_0 a_1 + t_1 b_0 + t_0 b_1)x + (s_0 a_0 + t_0 b_0)
\end{aligned}$$

where all terms in the summation with negative indices are ignored. In order for this to be the zero polynomial, all of its coefficients must be zero. This leads to a system of linear equations for the $r+s$ variables $s_{s-1}, \ldots, s_0, t_{r-1}, \ldots, t_0$. In matrix form this system is

$$(0, \ldots, 0) = (s_{s-1}, \ldots, s_0, t_{r-1}, \ldots, t_0) \begin{pmatrix}
a_r & a_{r-1} & \cdots & a_1 & a_0 & 0 & 0 & \cdots & 0 \\
0 & a_r & \cdots & & a_1 & a_0 & 0 & \cdots & 0 \\
0 & 0 & \ddots & & & \ddots & & & \\
\vdots & \vdots & & \ddots & & & \ddots & & \\
0 & 0 & & a_r & a_{r-1} & \cdots & & a_1 & a_0 \\
b_s & b_{s-1} & \cdots & b_1 & b_0 & 0 & \cdots & 0 & 0 \\
0 & b_s & b_{s-1} & \cdots & b_1 & b_0 & & 0 & 0 \\
\vdots & & \ddots & & & \ddots & & & \\
0 & \cdots & \cdots & b_s & \cdots & \cdot & & b_1 & b_0
\end{pmatrix}$$

and we immediately recognize the $r+s$ by $r+s$ matrix on the right as the Sylvester matrix. In order for this system to have a non-zero solution (in fact a solution with not all $s_i = 0$ and not all $t_j = 0$), it is necessary and sufficient that the determinant of the Sylvester matrix be zero. This of course is just the resultant $R_{r,s}(f,g)$.

Similarly, if $f(x)$ and $g(x)$ have *two* (or more) roots in common, then we can find non-zero polynomials

$$s(x) = s_{s-2}x^{s-2} + \cdots + s_1 x + s_0 \quad \text{and} \quad t(x) = t_{r-2}x^{r-2} + \cdots + t_1 x + t_0$$

such that

$$s(x)f(x) + t(x)g(x) = 0$$

and conversely. This leads to a system of $r+s-1$ linear equation

$$(0,\ldots,0) = (s_{s-2},\ldots,s_0,t_{r-2},\ldots,t_0)\begin{pmatrix} a_r & a_{r-1} & \cdots & a_0 & 0 & \cdots & & 0 \\ 0 & a_r & \cdots & \cdots & a_0 & \cdots & & 0 \\ & & & & & & & \\ \cdots & \cdots & 0 & a_r & a_{r-1} & \cdots & & a_0 \\ b_s & \cdots & & b_1 & b_0 & \cdots & 0 & 0 \\ 0 & b_s & \cdots & \cdots & b_1 & b_0 & \cdots & 0 \\ & & & & & & & \\ 0 & \cdots & \cdots & b_s & \cdots & \cdots & & b_0 \end{pmatrix}$$

in $r+s-2$ variables. It turns out that a necessary and sufficient condition for this system to have a solution with not all $s_i = 0$ and not all $t_j = 0$, is that the first $r+s-2$ by $r+s-2$ minor (obtained by deleting the last column) has zero determinant. This matrix is a submatrix of the Sylvester matrix. In general, if we write the Sylvester matrix as

$$\begin{pmatrix} a_r & a_{r-1} & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & a_r & \cdots & \cdots & a_0 & \cdots & 0 \\ & & & & & & \\ 0 & \cdots & \cdots & a_r & \cdots & \cdots & a_0 \\ 0 & \cdots & b_s & \cdots & \cdots & \cdots & b_0 \\ & \iddots & & & & \iddots & \\ b_s & \cdots & \cdots & b_0 & \cdots & \cdots & 0 \end{pmatrix}$$

the kth subresultant $R^{(k)}_{r,s}(f,g)$ is the determinant of the $r+s-2k$ by $r+s-2k$ submatrix obtained by deleting the first k rows, the last k rows, the first k columns, and the last k columns.

The answer to Question 1 is given by:

Theorem 1 *If $R^{(0)}_{r,s}(f,g) = R^{(1)}_{r,s}(f,g) = \cdots = R^{(k-1)}_{r,s}(f,g) = 0$ but $R^{(k)}_{r,s}(r,s) \neq 0$ for some $k \geq 0$ then f and g have exactly k roots in common. Here $R_{r,s}(f,g)$ is denoted $R^{(0)}_{r,s}(f,g)$.* □

The answer to Question 2 is more subtle. In general, we cannot expect to be able to express the common roots of f and g (assuming they have a root or roots in common) as rational expressions in the coefficients $a_r,\ldots,a_0,b_s,\ldots,b_0$. For example, if f and g have rational coefficients, i.e., $a_r,\ldots,a_0,b_s,\ldots,b_0 \in \mathbf{Q}$, the field of rational numbers, then any polynomial expression in the coefficients would be a rational number. But polynomials with rational coefficients can have common roots that are not rational.

Example 6: $f(x) = 3x^4+x^3+4x^2+x+1 = (x^2+1)(3x^2+x+1)$ and $g(x) = x^2-1 = (x^2+1)(x^2-1)$ both have rational coefficients, but the common roots $\pm i$ are not rational numbers. □

We can however answer Question 2 in a special case. If $R_{r,s}(f,g) = 0$ and at least one partial derivative of the resultant computed symbolically

$$\frac{\partial R}{\partial a_0},\ldots,\frac{\partial R}{\partial a_r},\frac{\partial R}{\partial b_0},\ldots,\frac{\partial R}{\partial b_s} \tag{2}$$

is non-zero when the coefficients of f and g are substituted, then f and g have exactly *one* common root α and it can be found via the proportions:

$$(1:\alpha:\alpha^2:\cdots:\alpha^r) = \left(\frac{\partial R}{\partial a_0}(f,g) : \frac{\partial R}{\partial \alpha_1}(f,g) : \cdots : \frac{\partial R}{\partial \alpha_r}(f,g)\right)$$
$$(1:\alpha:\alpha^2:\cdots:\alpha^s) = \left(\frac{\partial R}{\partial b_0}(f,g) : \frac{\partial R}{\partial b_1}(f,g) : \cdots : \frac{\partial R}{\partial b_s}(f,g)\right).$$

In particular the common root α can be computed as:

$$\alpha = \frac{\frac{\partial R}{\partial a_1}(f,g)}{\frac{\partial R}{\partial a_0}(f,g)} = \frac{\frac{\partial R}{\partial b_1}(f,g)}{\frac{\partial R}{\partial b_0}(f,g)}.$$

This result also has a geometric interpretation. The space of all pairs of polynomials (f,g) with the degree of f less than or equal to r and the degree of g less than or equal to s can be identified with $\mathbb{R}^{r+s+2}$ having coordinates $(a_r,\ldots,a_0,b_s,\ldots,b_0)$. The symbolic resultant R is a polynomial in these variables, and the locus $R=0$ in $\mathbb{R}^{r+2+2}$ is an irreducible hypersurface (of dimension $r+s+1$) consisting of pairs (f,g) with a root in common. A point on this hypersurface where at least one of the partial derivatives (2) is non-zero is a *smooth point*. At such points we have exactly one common root. Moreover, that root can be expressed as a quotient of polynomial expressions in $a_r,\ldots,a_0,b_s,\ldots,b_0$. We remind the reader that "most" points on the locus $R=0$ are smooth points. Those that are not are called *singular points*, and they occur in dimension $r+s$ or less.

2 Resultant Methods for Systems of Polynomial Equations in Several Variables

2.1 Theory

The linear algebra techniques discussed in this section can be used to solve systems of polynomial equations in several variables. If there are only two equations, then the Sylvester technique (discussed above) can be employed, by treating all but one variable as part of the coefficients. However, when the number of equations exceeds two, the Sylvester approach can be misleading. For example, taking the equations two at a time using the Sylvester determinant can lead the user to the conclusion that there is a common solution, when in fact, there are no common solutions for the system of equations taken as a whole.

What it means to "solve" a given set of polynomial equations depends upon the number of variables and the number of equations. Assuming the equations are inhomogeneous, let "n" be the number of variables and "m" be the number of equations. The expected dimensionality of the set of solutions is $n - m$ when viewed over the complex numbers. For example, if there are three equations ($m = 3$) and five variables ($n = 5$), then the space of solutions is expected to have dimension $n - m = 5 - 3 = 2$. Geometrically, the set of solutions forms a surface. Sometimes, however, components of excess dimension occur in the set of solutions. These are geometric loci of higher dimension than the expected dimension. They occur because, in a very loose sense, the equations have certain dependencies.

Finally a word about homogeneous equations. Recall that a set of polynomial equations is considered homogeneous if in each equation, all the terms have the same degree. If this is not the case, even for only one of the equations, the set is regarded as inhomogeneous. For systems of homogeneous equations, the number n of variables should be taken as one less than the actual number of variables, when computing expected dimensions. This is because we want to regard the solutions as lying in an $(n-1)$-dimensional projective space.

2.2 The Macaulay Resultant, the U-Resultant, and the GCP

The Macaulay resultant is the ratio of two determinants formed from the coefficients of the given polynomials in a manner to be described later in this section. If the number of equations exceeds the number of variables by one ($n - m = -1$), then the Macaulay resultant tests whether or not a common solution exists. (For systems of homogeneous equations where the number of equations equals the number of variables, the expected dimension is still -1, and the Macaulay resultant tests for a non-trivial common solution, i.e. a solution other than $(0, \ldots, 0)$.)

If there are as many inhomogeneous equations as unknowns ($n - m = 0$), then the equations can often be solved by adding the U-equation (explained later in this section) to the homogenized set and forming the Macaulay resultant. The Macaulay resultant is then called the U-resultant.

In some cases, however, there will be a component of excess dimension (≥ 1) which masks some or all of the desired solutions. In this case Canny's Generalized Characteristic Polynomial (GCP) approach is useful (see [**?**]).

In order to illustrate the various methods, the following system of three polynomial equations will be used:

$$\begin{aligned} f_1 &= y - 3x + 5 = 0 \\ f_2 &= x^2 + y^2 - 5 = 0 \\ f_3 &= y - x^3 + 3x^2 - 3x + 1 = 0. \end{aligned}$$

Here we have three inhomogeneous equations in two variables ($n - m = 2 - 3 = -1$). The multiresultant techniques described below can be used to test for the existence of a solution.

Step 1: Homogenization

The equations must first be homogenized. This is done by adding a third variable, z. Specifically x is replaced by x/z and y is replaced by y/z, and the factors of z are cleared from the denominators. In the above example this leads to three equations:

$$\begin{aligned} f_1 &= y - 3x + 5z = 0 \\ f_2 &= x^2 + y^2 - 5z^2 = 0 \\ f_3 &= yz^2 - x^3 + 3x^2z - 3xz^2 + z^3 = 0. \end{aligned}$$

This is the homogenized version of the original system.

Step 2: Degree Determination

Each of the multiresultants being considered involves the coefficients of various monomials that appear in the equations. The variables involved in the monomials are the variables that appear in the homogeneous form of the polynomial equations. For example, the homogeneous polynomial equations above have the variables x, y, and z. All the monomials in a given equation are constrained to have the same degree because we have homogenized. The "overall degree" of the system is determined from the degrees of the individual homogeneous equations by the following rule:

$$d = 1 + \sum_{i=1}^{m} (d_i - 1)$$

where

$$\begin{aligned} m &= \text{the number of equations} \\ d_i &= \text{the degree of the "}i\text{'th" equation.} \end{aligned}$$

For the homogeneous polynomials above (f_1, f_2, and f_3) the degrees are:

Equation	Degree
f_1	$d_1 = 1$
f_2	$d_2 = 2$
f_3	$d_3 = 3$.

Therefore,

$$d = 1 + (1 - 1) + (2 - 1) + (3 - 1) = 4.$$

Step 3: Matrix Size Determination

Each of the multiresultants to be discussed involves the ratio of two determinants. The numerator is the determinant of a matrix, the formation of which will be discussed in subsequent sections. The denominator determinant is formed from a submatrix of the numerator matrix.

The number of variables in the inhomogeneous equations is n. Since one additional variable has to be added to homogenize the equations, the number of variables in the homogeneous equations is $n + 1$. The size of the numerator matrix equals the number of monomials in the $n + 1$ variables that have overall degree d (discussed in the previous section).

$$\text{Numerator Matrix Size} = \binom{n+d}{d}.$$

For the three polynomial equations (f_1, f_2, f_3) we have already calculated that $d = 4$. Since the original set of inhomogeneous variables consisted of x and y, we have that n equals 2. Thus for our example,

$$\text{Numerator Matrix Size} = \binom{2+4}{4} = \binom{6}{4} = \frac{6!}{(2!)(4!)} = 15,$$

i.e. it is a 15×15 matrix.

Step 4: Determining "Big" vs. "Small" Exponents

A few of the 15 monomials involving the variables x, y, and z with an overall degree of 4, include:

$$yz^3 \qquad \text{and} \qquad x^2y^2.$$

In the next section, we will discuss whether certain of these monomials are reduced. This will be determined by whether the exponents are "big" or "small". In this section we discuss how "bigness" is defined.

Each variable will be associated with a particular equation. For example the first variable, x, will be associated with the first equation, f_1. The second variable, y, will be associated with the second equation, f_2, etc. The degrees of the associated equations define "bigness" for the exponents of that variable. Specifically, since d_1 (the degree of f_1) is 1, if the exponent of x is greater than or equal to 1, it is considered big. Since $d_2 = 2$, whenever the exponent of y is greater than or equal to 2, it is considered big. The degree of f_3 is 3, therefore, whenever the exponent of z is greater than or equal to 3, it is considered big.

For example, consider the monomial yz^3. The exponent of y is 1. This is *less than* d_2, and is considered *small*. The exponent of z is 3. This is *equal to* d_3, and is therefore *big*. On the other hand, consider the monomial x^2y^2. The exponent of x is 2. This is *greater than* d_1, and is *big*. The exponent of y is 2. This is *equal to* d_2, and is *big*.

Step 5: Determining the Reduced Monomials

If for a particular monomial of degree d the exponent of *only one* variable is big, the monomial is said to be reduced. In the previous step only the monomial yz^3 is reduced. For that monomial only the exponent of z is big; whereas for x^2y^2, both the exponent of x and the exponent of y are big. Thus the monomial x^2y^2 is not reduced.

The Macaulay Resultant

The Macaulay Resultant is the ratio of two determinants. The numerator is the determinant of a matrix which we will call the A matrix. The denominator is the determinant of a matrix which we will call the M matrix

$$R = \frac{\det|A|}{\det|M|}.$$

Step 6: Creating the A Matrix:

We have discussed above how the size of the A matrix is determined. In this section we will show how the matrix entries are obtained.

Each row and column of the matrix should be thought of as being labeled by one of the monomials of degree d. Recall that for f_1, f_2, and f_3 in our example there were 15 possible monomials of degree 4 in x, y, z, and therefore the A matrix would be 15×15.

There are three rules for determining the elements of the A matrix. After presenting the rules, the example involving f_1, f_2, and f_3, will be used to illustrate the process. The reader may find it helpful to read the example simultaneously with the rules.

Rules for the elements of each column:

(1) Search the monomial labeling that column from left to right for the *first* variable with a big exponent. Such a variable must exist. Call it the marker variable.

(2) Form a new polynomial from the polynomial associated with this marker variable by multiplying the associated polynomial by the monomial and dividing by the marker variable raised to the degree of the associated polynomial.

(3) The coefficients of the new polynomial are the elements of the columns. Each coefficients goes in the row labeled by the monomial it multiples. All the other rows get zeroes.

Example 7: Recall that for the system of equations f_1, f_2, f_3 there are 15 monomials of degree 4 that can be formed from x, y, and z. Two of these were considered above, namely yz^3 and x^2y^2.

- For the column labeled by yz^3:

  (1) The first variable with a big exponent is z, so z is the marker variable.

  (2) The polynomial associated with z is f_3. Multiply f_3 by the monomial yz^3, and divide this product by z^3.

$$\frac{f_3(yz^3)}{z^3} = \frac{(yz^2 - x^3 + 3x^2z - 3xz^2 + z^3)(yz^3)}{z^3} = y^2z^2 - x^3y + 3x^2yz - 3xyz^2 + yz^3.$$

  (3) The coefficient of y^2z^2 is $+1$. Therefore the element of the row labeled y^2z^2 is $+1$. The coefficient of x^3y is -1. Therefore the element of the row labeled x^3y is -1. The coefficient of x^2yz is $+3$. Therefore the element of the row labeled x^2yz is $+3$. The coefficient of xyz^2 is -3. Therefore the element of the row labeled xyz^2 is -3. The coefficient of yz^3 is $+1$. Therefore the element of the row labeled yz^3 is $+1$. All other entries in the column are zero.

- For the column labeled by x^2y^2:

  (1) The first variable with a big exponent is x, so x is the marker variable.

  (2) The polynomial associated with x is f_1. Multiply f_1 by the monomial x^2y^2, and divide this product by x.

$$\frac{f_1(x^2y^2)}{x} = \frac{(y - 3x + 5z)(x^2y^2)}{x} = xy^3 - 3x^2y^2 + 5xy^2z.$$

  (3) The coefficient of xy^3 is $+1$. Therefore the element of the row labeled xy^3 is $+1$. The coefficient of x^2y^2 is -3. Therefore the element of the row labeled x^2y^2 is -3. The coefficient of xy^2z is $+5$. Therefore the element of the row labeled xy^2z is $+5$. □

When all the columns are determined, the A matrix in our example takes the form:

A Matrix

			x^4	x^3y	x^3z	x^2y^2	x^2yz	x^2z^2	xy^3	xy^2z	xyz^2	xz^3	y^4	y^3z	y^2z^2	yz^3	z^4
x^4			−3	0	0	0	0	0	0	0	0	0	0	0	0	0	0
x^3	y		1	−3	0	0	0	0	0	0	0	0	0	0	0	−1	0
x^3		z	5	0	−3	0	0	0	0	0	0	0	0	0	0	0	−1
x^2	y^2		0	1	0	−3	0	0	0	0	0	0	0	1	0	0	0
x^2	y	z	0	5	1	0	−3	0	0	0	0	0	0	1	0	3	0
x^2		z^2	0	0	5	0	0	−3	0	0	0	0	0	0	1	0	3
x	y^3		0	0	0	1	0	0	−3	0	0	0	0	0	0	0	0
x	y^2	z	0	0	0	5	1	0	0	−3	0	0	0	0	0	0	0
x	y	z^2	0	0	0	0	5	1	0	0	−3	0	0	0	0	−3	0
x		z^3	0	0	0	0	0	5	0	0	0	−3	0	0	0	0	−3
	y^4		0	0	0	0	0	0	1	0	0	0	1	0	0	0	0
	y^3	z	0	0	0	0	0	0	5	1	0	0	0	1	0	0	0
	y^2	z^2	0	0	0	0	0	0	0	5	1	0	−5	0	1	1	0
	y	z^3	0	0	0	0	0	0	0	0	5	1	0	−5	0	1	1
		z^4	0	0	0	0	0	0	0	0	0	5	0	0	−5	0	1

The determinant of the above A matrix is zero. If the determinant of the M matrix is nonzero, this would imply that the system has a solution.

Step 7: Creating the M Matrix

The denominator of the Macaulay Resultant is the determinant of the M matrix. The M matrix is a submatrix of the A matrix. It consists of the elements which have row and column monomial labels which are *not reduced*. Recall that a monomial is not reduced if it has more than one variable with a big exponent.

The size of the M matrix equals the size of the A matrix minus D, where

$$D = \sum_{i=1}^{m} \prod_{i \neq j} d_j.$$

In our example,

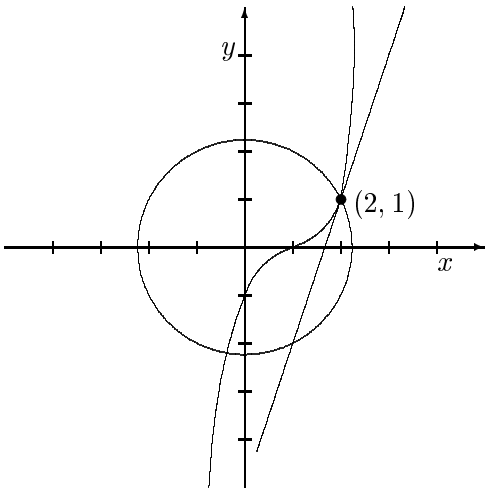
$$D = d_2d_3 + d_1d_3 + d_1d_2 = (2)(3) + (1)(3) + (1)(2) = 11,$$

so that the size of the M matrix is $15 - 11 = 4$. The actual M matrix for f_1, f_2, and f_3 is:

M Matrix

	x^2y^2	xy^3	xy^2z	xz^3
x^2y^2	−3	0	0	0
xy^3	1	−3	0	0
xy^2z	5	0	−3	0
xz^3	0	0	0	−3

The determinant of this M matrix yields a value of 81. Since the determinant of the A matrix was zero, the Macaulay Resultant is zero, which implies that there is a solution to our system. The following plot of the three polynomials (f_1, f_2, and f_3) confirms that there is a common point at $x = 2$ and $y = 1$.



Sometimes both the A matrix and the M matrix have zero determinant. This indeterminacy can often be circumvented if the polynomials are first written with symbolic coefficients. The determinants of the A and M matrices are obtained, polynomial division is performed, and then at the end, the symbolic coefficients are replaced by their numerical values to check if the resultant is zero. Since one does not know ahead of time whether or not this "division by zero" condition will arise, the symbolic coefficient approach is the best strategy. It is also often sufficient to treat just a subset of the coefficients symbolically—sometimes as few as a single symbolic coefficient will remove the indeterminacy.

The U-Resultant

For problems with as many inhomogeneous equations as variables, the U-resultant can often be used to solve for the point solutions. The three polynomial equations f_1, f_2, f_3 do not satisfy these conditions, since there are three equations in two inhomogeneous variables, x and y. However, if we take just the first two equations, namely f_1 and f_2, we would have a system with as many equations as variables.

The given equations must first be homogenized. This adds one additional variable. We then add one additional equation to the system. This equation is called the U-equation. If x and y are the given variables and z is the homogenizing variable, then the U equation takes the form:

$$u_1 x + u_2 y + u_3 z = 0.$$

The Macaulay Resultant, R, is then computed for these $m + 1$ equations, treating the u_i as symbolic coefficients. The result is called the U-resultant. Notice that R will be a polynomial in the u_i's and the coefficients of the original equations.

After R is determined, it is factored into linear factors. For each linear factor there is a point solution of the original system of equations. The coordinates of each solution are given as ratios of the coefficients of the u_i's. The denominator is always the coefficient of the u_i associated with the homogenizing variable. In our example, this is the coefficient of u_3. Thus

$$x = \frac{\text{coeff. of } u_1}{\text{coeff. of } u_3} \quad \text{and} \quad y = \frac{\text{coeff. of } u_2}{\text{coeff. of } u_3}.$$

For example, if a linear factor turned out to be

$$u_1 - u_2 - u_3,$$

then the coordinates of the associated solution would be

$$x = \frac{+1}{-1} = -1 \quad \text{and} \quad y = \frac{-1}{-1} = +1.$$

Example 8: As mentioned above, the polynomial equation system f_1, f_2, f_3 is overdetermined ($n - m = -1$). However, we can use the U-resultant to solve f_1 and f_2 for x and $y (n - m = 0)$. In this example, we will also demonstrate the symbolic approach alluded to in the previous section. Recall that the homogenized form of f_1 and f_2 is:

$$f_1 = y - 3x + 5z = 0$$
$$f_2 = x^2 + y^2 - 5z^2 = 0.$$

Rewriting these two equations with symbolic coefficients and including the U-equation yields:

$$f_1 = a_1 x + b_1 y + c_1 z = 0$$
$$f_2 = a_2 x^2 + b_2 y^2 + c_2 z^2 = 0$$
$$U = u_1 x + u_x y + u_3 z = 0$$

where, $a_1 = -3$, $b_1 = 1$, $c_1 = 5$, $a_2 = 1$, $b_2 = 1$, and $c_2 = -5$.

The U-resultant is calculated in the same way as the Macaulay resultant, i.e., with the A matrix and the M matrix, except now we are using symbolic coefficients.

A Matrix

	x^2	xy	xz	y^2	yz	z^2
x^2	a_1	0	0	a_2	0	0
xy	b_1	a_1	0	0	u_1	0
xz	c_1	0	a_1	0	0	u_1
y^2	0	b_1	0	b_2	u_2	0
yz	–	c_1	b_1	0	u_3	u_2
z^2	0	0	c_1	c_2	0	u_3

The corresponding M matrix is a single element, namely a_1.

The determinant of M is divided into the determinant of A to obtain the U-resultant. Finally, the symbolic coefficients are replaced by their numeric equivalents. (This could have been done from the outset, unless a_1 had been zero.) The result is

$$10(u_1 - 2u_2 + u_3)(2u_1 + u_2 + u_3).$$

This yields two solutions:

SOLUTION #1:

$$x = \frac{\text{coeff. of } u_1}{\text{coeff. of } u_3} = \frac{+1}{-1} = -1 \quad \text{and} \quad y = \frac{\text{coeff. of } u_2}{\text{coeff. of } u_3} = \frac{-2}{+1} = -2.$$

SOLUTION #2:

$$x = \frac{\text{coeff. of } u_1}{\text{coeff. of } u_3} = \frac{+2}{+1} = +2 \quad \text{and} \quad y = \frac{\text{coeff. of } u_2}{\text{coeff. of } u_3} = \frac{+1}{+1} = +1.$$

We remark that the U-resultant will be identically zero and give no information, if the set of common solutions contains a component of excess dimension one or more. Moreover, this component may be at infinity where the homogenizing variable is zero.

The GCP Approach

The Generalized Characteristic Polynomial (GCP) approach [**?**] avoids the problem of components of excess dimension in the set of solutions. It can be used together with the U-resultant which was discussed above. If the U-resultant leads to an indeterminant (0/0) form even when symbolic coefficients are used, an "excess" solution exists. The GCP takes the form

$$R = \frac{\det|A - sI|}{\det|M - sI|} \text{ evaluated at } s = 0 \text{ after division}$$

where A and M are the matrices defined above, s is a perturbation parameter, and I is the identity matrix.

One way to carry out the above operation is the following:

(1) Set up the A matrix (as described above). Subtract s along the diagonal. Evaluate the determinant. Retain the coefficient of the lowest surviving power of s.

(2) Repeat (1) for the M matrix.

(3) Divide the result of (1) by the result (2).

All of these multiresultant techniques have one thing in common. They require that there be one more equation than variable, $n - m = -1$. If there are as many equations as variables $n - m = 0$, the the U equation is added and the effective situation is again $n - m = -1$. If there are more variables than equations ($n - m$ is a positive integer), then enough of these variables must be regarded as parameters in the coefficients, so that effectively $n - m = -1$. Geometrically this amounts to projecting the locus of solutions to a hypersurface in a lower dimensional space. Finally, if the number of equations exceeds the number of variables by more than one ($n - m \leq -2$), then some technique other than the above multiresultant techniques (e.g., a system of multiresultants) must be employed to determine if a solution exists.

2.3 The Jacobian Method of Salmon

Consider a system of m polynomial equations in n variables

$$\begin{aligned} f_1(x_1, \ldots, x_n) &= 0 \\ &\vdots \\ f_m(x_1, \ldots, x_n) &= 0. \end{aligned} \tag{3}$$

For example, take a system of three quadratic equations in three variables x, y, z:

$$0 = a_k x^2 + b_k y^2 + c_k z^2 + d_k xy + e_k xz + f_k yz + g_k x + h_k y + i_k z + j_k, \quad k = 1, 2, 3.$$

Geometrically, this amounts to 3 quadratic surfaces intersecting in 3-space.

From Bezout's Theorem we expect this system to have 8 solutions (counting complex solutions, solutions at infinity, and counting each solution the appropriate number of times, namely its multiplicity). Of course, it is possible in a degenerate situation for the above system to have an infinite number of solutions. This can occur if all the surfaces have a common (surface) component (i.e., the polynomials have a common factor), or if they intersect in a common curve.

We can add to our system of equations any equation of the form

$$f_j(x_1, \ldots, x_n) x_1^{e_1} \ldots x_n^{e_n}.$$

In fact, any equation of the form

$$\sum_{j=1}^{m} g_j(x_1, \ldots, x_n) f_j(x_1, \ldots, x_n),$$

for arbitrary polynomials $g_j(x_1, \ldots, x_n)$, can be added without changing the set of common solutions.

Our goal is to convert problem (**??**) into a system of linear equations where the methods of linear algebra can be applied. To accomplish this, we begin by writing each of our quadratic equations as

$$0 = a_k x^2 + b_k y^2 + d_k xy + (e_k z + g_k)x + (f_k z + h_k)y + (c_k z^2 + i_k z + j_k), \quad k = 1, 2, 3,$$

where we are thinking of them as quadratic equations in two variables x and y with coefficients that vary with z. We have six monomials in x and y, namely

$$x^2,\ y^2,\ xy,\ x,\ y,\ 1,$$

which we would like to treat as *independent* variables, giving us a system of linear equations. Unfortunately, this would be a system of only 3 equations in the "six variables", and we would prefer six equations. If we try to increase the number of equations by multiplying the existing three by various monomials, we invariably end up introducing new monomials in x and y—in effect increasing the number of "variables". Sometimes this method can be made to work (see Roth [**?**] for examples).

The trick, at least for the case of three quadratic equations in three variables, goes back to a result of Salmon.

Theorem 2 *(Salmon [**?**, pg. 88]): If we have a system of m homogeneous equations in m variables*

$$\begin{aligned} f_1(x_1, \ldots, x_m) &= 0 \\ &\vdots \\ f_m(x_1, \ldots, x_m) &= 0 \end{aligned} \tag{4}$$

(note: $m = n$), then any non-trivial common solution is also a solution of the Jacobian polynomial

$$J(x_1, \ldots, x_m) = det \begin{pmatrix} \partial f_1/\partial x_1 & \cdots & \partial f_1/\partial x_m \\ \vdots & & \vdots \\ \partial f_m/\partial x_1 & \cdots & \partial f_m/\partial x_m \end{pmatrix}.$$

*Moreover, if the f_i all have the same degree, then any non-trivial common solution to the system (**??**) is also a solution of all the polynomials*

$$\frac{\partial J}{\partial x_i}(x_1, \ldots, x_m), \quad i = 1, \ldots, m.$$

Proof. We do the case of three variables. Thus we consider a system of 3 homogeneous equations

$$\begin{aligned} f(x,y,w) &= 0 \\ g(x,y,w) &= 0 \\ h(x,y,w) &= 0 \end{aligned}$$

in the variables x, y, and w. Recall that for homogeneous polynomials we have the identities

$$\begin{aligned} x\frac{\partial f}{\partial x} + y\frac{\partial f}{\partial y} + w\frac{\partial f}{\partial w} &= (\deg f)f \\ x\frac{\partial g}{\partial x} + y\frac{\partial g}{\partial y} + w\frac{\partial g}{\partial w} &= (\deg g)g \\ x\frac{\partial h}{\partial x} + y\frac{\partial h}{\partial y} + w\frac{\partial h}{\partial w} &= (\deg h)h \end{aligned}$$

Consider this as a system of equations

$$\begin{pmatrix} \frac{\partial f}{\partial x} & \frac{\partial f}{\partial y} & \frac{\partial f}{\partial w} \\ \frac{\partial g}{\partial x} & \frac{\partial g}{\partial y} & \frac{\partial g}{\partial w} \\ \frac{\partial h}{\partial x} & \frac{\partial h}{\partial y} & \frac{\partial h}{\partial w} \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} (\deg f)f \\ (\deg g)g \\ (\deg h)h \end{pmatrix}. \tag{5}$$

Let $\begin{pmatrix} u_1 & v_1 & w_1 \\ u_2 & v_2 & w_2 \\ u_3 & v_3 & w_3 \end{pmatrix}$ be the matrix of cofactors of the Jacobian, so

$$\begin{aligned} u_1 &= \frac{\partial g}{\partial y}\frac{\partial h}{\partial w} - \frac{\partial h}{\partial y}\frac{\partial g}{\partial w} \\ v_1 &= -\frac{\partial f}{\partial y}\frac{\partial h}{\partial w} + \frac{\partial h}{\partial y}\frac{\partial f}{\partial w} \\ w_1 &= \frac{\partial f}{\partial y}\frac{\partial g}{\partial w} - \frac{\partial g}{\partial y}\frac{\partial f}{\partial w} \end{aligned}$$

etc. Multiplying both sides of (**??**) by this matrix yields

$$\begin{aligned} J_x &= u_1(\deg f)f + v_1(\deg g)g + w_1(\deg h)h \\ J_y &= u_2(\deg f)f + v_2(\deg g)g + w_2(\deg h)h \\ J_w &= u_3(\deg f)f + v_3(\deg g)g + w_3(\deg h)h. \end{aligned}$$

Now if $(x : y : w)$ is a non-trivial solution to f, g, and h, then $Jx = 0$, $Jy = 0$, and $Jw = 0$. But at least one of x, y, and w is non-zero (otherwise the solution is trivial) so $J = 0$. Algebraically this means that J is in the radical of the ideal generated by f, g, and h.

Now if $\deg f = \deg g = \deg \mathrm{h} = d$, we can differentiate Jx again with respect to x, y, and w, to get

$$J + x\frac{\partial J}{\partial x} = df\frac{\partial u_1}{\partial x} + dg\frac{\partial v_1}{\partial x} + dh\frac{\partial w_1}{\partial x} + d\left(\frac{\partial f}{\partial x}u_1 + \frac{\partial g}{\partial x}v_1 + \frac{\partial h}{\partial x}w_1\right).$$

and

$$x\frac{\partial J}{\partial y} = df\frac{\partial u_1}{\partial y} + dg\frac{\partial v_1}{\partial y} + dh\frac{\partial w_1}{\partial y} + d\left(\frac{\partial f}{\partial y}u_1 + \frac{\partial g}{\partial y}v_1 + \frac{\partial h}{\partial y}w_1\right)$$

and

$$x\frac{\partial J}{\partial w} = df\frac{\partial u_1}{\partial w} + dg\frac{\partial v_1}{\partial w} + dh\frac{\partial w_1}{\partial w} + d\left(\frac{\partial f}{\partial w}u_1 + \frac{\partial g}{\partial w}v_1 + \frac{\partial h}{\partial w}w_1\right)$$

But remember

$$\begin{aligned}\frac{\partial f}{\partial x}u_1 + \frac{\partial g}{\partial x}v_1 + \frac{\partial h}{\partial x}w_1 &= J\\ \frac{\partial f}{\partial y}u_1 + \frac{\partial g}{\partial y}v_1 + \frac{\partial h}{\partial y}w_1 &= 0\\ \frac{\partial f}{\partial w}u_1 + \frac{\partial g}{\partial w}v_1 + \frac{\partial h}{\partial w}w_1 &= 0\end{aligned}$$

so that

$$J + x\frac{\partial J}{\partial x} = df\frac{\partial u_1}{\partial x} + dg\frac{\partial v_1}{\partial x} + dh\frac{\partial w_1}{\partial x} + dJ$$

and

$$\begin{aligned}x\frac{\partial J}{\partial y} &= df\frac{\partial u_1}{\partial y} + dg\frac{\partial v_1}{\partial y} + dh\frac{\partial w_1}{\partial y}\\ x\frac{\partial J}{\partial w} &= df\frac{\partial u_1}{\partial w} + dg\frac{\partial v_1}{\partial w} + dh\frac{\partial w_1}{\partial w}.\end{aligned}$$

Now when we have a common solution, i.e., when f, g, and h are all zero, then so is J by what we have already showed. Thus

$$\begin{aligned}x\frac{\partial J}{\partial x} &= 0\\ x\frac{\partial J}{\partial y} &= 0\\ x\frac{\partial J}{\partial w} &= 0.\end{aligned}$$

Likewise differentiating Jy and Jw yields:

$$\begin{aligned}y\partial J/\partial x &= 0\\ y\partial J/\partial y &= 0\\ y\partial J/\partial w &= 0\\ w\partial J/\partial x &= 0\\ w\partial J/\partial y &= 0\\ w\partial J/\partial w &= 0.\end{aligned}$$

From these nine expressions and the fact that $(x : y : w) \neq (0 : 0 : 0)$, we conclude

$$\partial J/\partial x = 0, \quad \partial J/\partial y = 0, \quad \text{and} \quad \partial J/\partial w = 0$$

as required. Again, algebraically, this says that $\partial J/\partial x$, $\partial J/\partial y$, and $\partial J/\partial w$ are in the radical of the ideal generated by f, g, and h. □

We now apply this to our system

$$a_k x^2 + b_k y^2 + d_k xy + (e_k z + g_k)xw + (f_k a + h_k)yw + (c_k z^2 + i_k z + j_k)w^2, \quad k = 1, 2, 3 \qquad (6)$$

after making it homogeneous by inserting the variable w as appropriate. Keep in mind that z is treated as a parameter in the coefficients, not as one of our variables.

Since each entry in the 3×3 Jacobian matrix of our system is homogeneous linear in x, y, w, it is easy to see that J is homogeneous cubic in x, y, w and that therefore $\frac{\partial J}{\partial x}$, $\frac{\partial J}{\partial y}$, and $\frac{\partial J}{\partial w}$ are homogeneous quadratic. Adding these three quadratic equations to (**??**) yields the following system:

$$\begin{pmatrix} a_1 & b_1 & d_1 & (e_1 z + g_1) & (f_1 z + h_1) & (c_1 z^2 + i_1 z + j_1) \\ a_2 & b_2 & d_2 & (e_2 z + g_2) & (f_2 z + h_2) & (c_2 z^2 + i_2 z + j_2) \\ a_3 & b_3 & d_3 & (e_3 z + g_3) & (f_3 z + h_3) & (c_3 z^2 + i_3 z + j_3) \\ 3A(z) & D(z) & 2B(z) & 2C(z^2) & F(z^2) & E(z^3) \\ B(z) & 3G(z) & 2D(z) & F(z^2) & 2H(z^2) & I(z^3) \\ C(z^2) & H(z^2) & F(z^2) & 2E(z^3) & 2I(z^3) & 3J(z^4) \end{pmatrix} \begin{pmatrix} x^2 \\ y^2 \\ xy \\ xw \\ yw \\ w^2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \qquad (7)$$

where

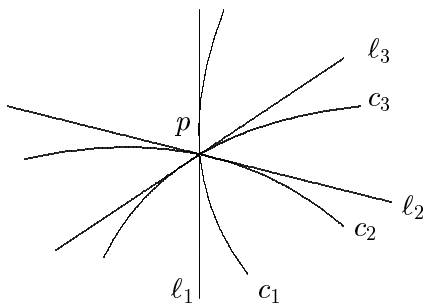
$$\begin{aligned} J =& A(z)x^3 + B(z)x^2 y + C(z^2)x^2 w + D(z)xy^2 + E(z^3)xw^2 \\ &+ F(z^2)xyw + G(z)y^3 + H(z^2)y^2 w + I(z^3)yw^2 + J(z^4)w^4 \end{aligned}$$

and the exponents on z indicate the degree of the polynomial in z (so $I(z^3)$ is a cubic expression in z).

In order for the system (**??**) to have a solution the determinant of the 6×6 matrix must be zero. This determinant is an eighth degree polynomial in z whose roots are the z-coordinates of the eight sought after points (x, y, z) that are the common solutions of our original three quadrics. Once such a z is found, we can set $w = 1$ and solve (**??**) for x and y.

While of limited use, this trick does allow one to generate additional equations that can be added to the system without creating new monomials in the expressions.

Geometrically, we can explain why J vanishes if f, g, and h do. Each of $f = 0$, $g = 0$, and $h = 0$ can be viewed as a curve in the projective plane $\mathbb{P}^2$ (using the fact that f, g, and h are homogeneous in x, y, w). Each row of the Jacobian matrix gives the coefficients of the tangent line to this curve. If we have a point p common to all three curves:



then the three tangent lines at that point cannot be "independent" because we are in dimension 2. Thus one line is a linear combination of the other two, i.e., one row of the Jacobian matrix is a linear combination of the other two, making the Jacobian determinant J equal to zero.

Example 9: Consider the system of equations

$$\begin{aligned} x^2 + y^2 - 2 &= 0 \\ x^2 + y^2 + z^2 - 3 &= 0 \\ x^2 - y^2 &= 0. \end{aligned}$$

The set of common solutions is easily seen to consist of the eight points $(x, y, z) = (\pm 1, \pm 1, \pm 1)$. We begin by homogenizing the system with respect to x and y:

$$\begin{aligned} 1x^2 + 1y^2 + 0xy + 0xw + 0yw + (-2)w^2 &= 0 \\ 1x^2 + 1y^2 + 0xy + 0xw + 0yw + (z^2 - 3)w^2 &= 0 \\ 1x^2 + (-1)y^2 + 0xy + 0xw + 0yw + 0w^2 &= 0. \end{aligned}$$

The Jacobian is

$$J = \det \begin{pmatrix} 2x & 2y & -4w \\ 2x & 2y & (2z^2 - 6)w \\ 2x & -2y & 0 \end{pmatrix} = 16xyw(z^2 - 1)$$

and

$$\begin{aligned} \frac{\partial J}{\partial x} &= 16yw(z^2 - 1) \\ \frac{\partial J}{\partial y} &= 16xw(z^2 - 1) \\ \frac{\partial J}{\partial w} &= 16xy(z^2 - 1). \end{aligned}$$

Adding these last three equations to our original three yields the following "linearized" system:

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & -2 \\ 1 & 1 & 0 & 0 & 0 & z^2 - 3 \\ 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 16(z^2 - 1) & 0 \\ 0 & 0 & 0 & 16(z^2 - 1) & 0 & 0 \\ 0 & 0 & 16(z^2 - 1) & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x^2 \\ y^2 \\ xy \\ xw \\ yw \\ w^2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

The determinant of the 6×6 matrix is $8192(z^2 - 1)^4$ which is of degree eight as expected. The roots of this polynomial in z are $z = \pm 1$. Both cases lead to the system (after setting $w = 1$):

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & -2 \\ 1 & 1 & 0 & 0 & 0 & -2 \\ 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x^2 \\ y^2 \\ xy \\ x \\ y \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

This must now be solved for x and y yielding $x = \pm 1$ and $y = \pm 1$.

This example points up one defect of the method. While z is eliminated, we are left in general with a system of six quadratic equations in x and y that must be solved. This system may not have a solution, or may not have a solution with $w = 1$. In the later case we may get a solution with $w = 0$, but that is a solution at infinity.

3 Geometric Aspects of Elimination Theory and the Theory of Equations

3.1 Intersections of Curves in the Plane

A curve C in the plane of degree $d \geq 1$ is described by the zeros of a single polynomial $f(x, y)$ of degree d. If $f(x, y)$ factors, say as

$$f(x, y) = g(x, y)h(x, y)$$

where the degree of g is $d_1 \geq 1$, and the degree of h is $d_2 \geq 1$, then C can be written as the union of two curves C_1 and C_2 of degrees d_1 and d_2 respectively. We can continue factoring until $f(x, y)$ is written as a product of irreducible (non-factorable) polynomials each of degree ≥ 1. C is then just the union of a finite number of irreducible curves. For that reason, we often assume that $f(x, y)$ is irreducible to begin with, and when that is the case C will be called an irreducible plane curve.

Let (x_0, y_0) be the coordinates of a point P on C, i.e., let (x_0, y_0) be a solution to $f(x, y) = 0$. We can make a change of coordinates by letting

$$x' = (x - x_0) \quad \text{and} \quad y' = (y - y_0)$$

which will put P at the origin. Recall that the multivariate Taylor expansion of $f(x, y)$ around (x_0, y_0) yields

$$f(x, y) = f(x_0, y_0) + \frac{\partial f}{\partial x}(x_0, y_0)(x - x_0) + \frac{\partial f}{\partial y}(x_0, y_0)(y - y_0) + \text{higher order terms.}$$

In these new coordinates C is given by the equation

$$0 = f(x' + x_0, y' + y_0) = \frac{\partial f}{\partial x}(x_0, y_0)x' + \frac{\partial f}{\partial y}(x_0, y_0)y' + \text{higher order terms in } x' \text{ and } y'$$

and the point P has coordinates $(x', y') = (0, 0)$.

In what follows, we will assume that this has already been done so that $P = (0, 0)$ and

$$f(x, y) = f_1(x, y) + f_2(x, y) + \cdots + f_d(x, y)$$

where $f_i(x, y)$ is a homogeneous polynomial of degree i. In particular $f_1(x, y) = \frac{\partial f}{\partial x}(0, 0)x + \frac{\partial f}{\partial y}(0, 0)y$.

Definition 1 *We say that $P \in C$ is a singular point if f_1 is identically zero. Otherwise P is a nonsingular (or smooth) point of C and the line $f_1(x, y) = 0$ is called the tangent line to C to P.*

Note that in the original coordinates, where P has coordinates (x_0, y_0), the tangent line is given by

$$0 = \frac{\partial f}{\partial x}(x_0, y_0)(x - x_0) + \frac{\partial f}{\partial y}(x_0, y_0)(y - y_0).$$

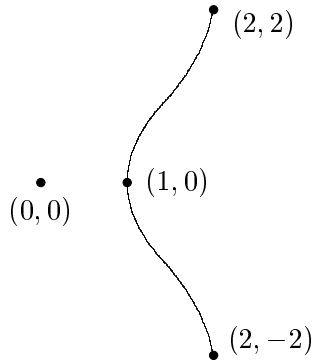
Definition 2 *A singular point $P \in C$ is called an m-fold singular point on C (double point, triple point, etc.) if $f_1 = f_2 = \cdots = f_{m-1} = 0$ but f_m is not zero.*

Since f_m is homogeneous in two variables, it can be completely factored (over $\mathbb{C}$, the complex numbers) into linear factors

$$f_m = \prod_{i=1}^{m} (\mu_i x - v_i y).$$

Definition 3 *If the lines $\mu_i x - v_i y = 0$ are all distinct, we say that P is an ordinary m-fold point. An ordinary double point is also called a node.*

Example 10: Consider the point $(0,0)$ on $y^2 + x^2 - x^3 = 0$.

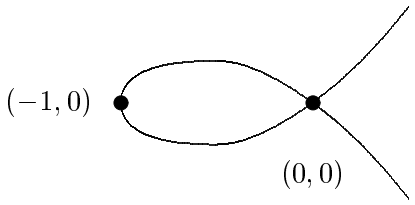


The real solutions to this equation are picture above. Notice that $(0,0)$ appears to be an isolated point. This an artifact of working over $\mathbb{R}$; over $\mathbb{C}$ it is not isolated. In this example $f(x,y) = y^2 + x^2 - x^3$ and at $(0,0)$ we have:

$$f_1 = 0, \quad f_2 = y^2 + x^2, \quad \text{and} \quad f_3 = -x^3.$$

We see that $(0,0)$ is a singular point because $f_1 = 0$, and that it is in fact a double point because $f_2 \neq 0$. Moreover $f_2 = y^2 + x^2 = (y + ix)(y - ix)$ so that f_2 factors into two distinct linear factors which means that P is an ordinary double point. □

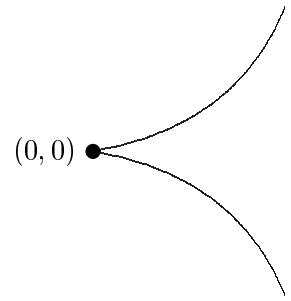
Example 11: $y^2 - x^2 - x^3 = 0$



This is the more typical picture of an ordinary double point at $(0,0)$. □

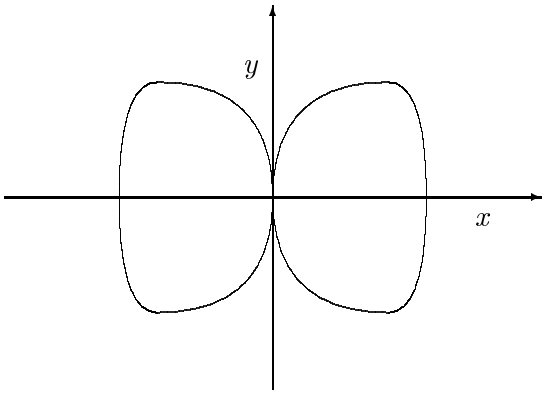
Definition 4 *A double point is called a cusp if $f_2 = (ax + by)^2$ and the intersection multiplicity of the line $ax + by = 0$ with the curve is 3 (see below).*

Example 12: $y^2 - x^3 = 0$



This curve has a cusp at $(0,0)$.

Example 13: The singularity pictured below is a double point called a tacnode:



We will be interested in solving systems like

$$f(x,y) = 0$$
$$g(x,y) = 0.$$

Let's begin by considering the case where $g(x,y) = ax+by+c$. This means that we are intersecting the curve C given by $f(x,y) = 0$ and the line L given by $g(x,y) = 0$. If $b \neq 0$, we can solve for y:

$$y = -\frac{a}{b}x - \frac{c}{b}.$$

If we substitute this into f:

$$0 = f\left(x, -\frac{a}{b}x - \frac{a}{c}\right) = h(x)$$

the result is a polynomial $h(x)$ in the one variable x, of degree at most $d =$ degree f. Notice that h could be identically zero if $f(x,y)$ factors into $ax + by + c$ times another polynomial. We will assume that this is not the case. Then we have at most d intersection points whose x coordinates can be found by solving $h(x) = 0$.

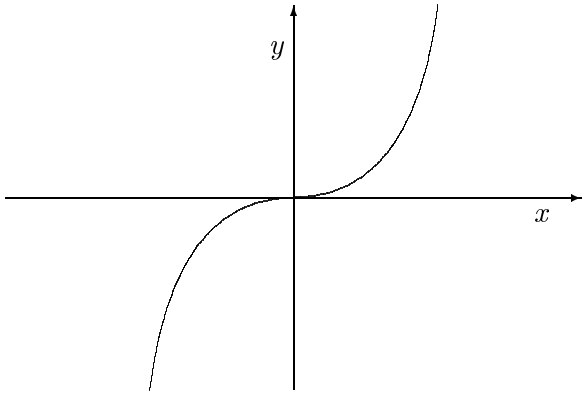
Let's consider the following special case. Namely, let P be a smooth point on a curve C (we assume $P = (0,0)$ by changing coordinates) given by $f(x,y) = 0$. We have that

$$g(x,y) = \frac{\partial f}{\partial x}(0,0)x + \frac{\partial f}{\partial y}(0,0)y = 0$$

is the tangent line L to C at P. After another change of coordinates, we can assume that $g(x,y) = y = 0$ is the tangent line to C at $(0,0)$. We define the intersection multiplicity of $P \in L \cap C$ to be the order of vanishing of $f(x,0)$ at x=0. This amounts to restricting the polynomial $f(x,y)$ to the x-axis which is of course the tangent line given by $y = 0$.

Definition 5 *If this order of vanishing is 3, then P is called an ordinary flex.*

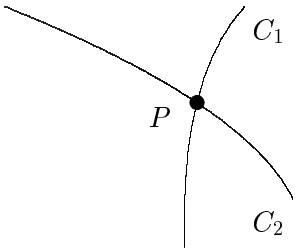
Example 14: $y - x^3 = 0$ has an ordinary flex at $(0,0)$.



Generally a tangent line to a curve at a nonsingular point meets the curve with intersection multiplicity 2. If a tangent line has higher than expected order of contact at P, then P is called a flex of the curve.

Now suppose we have two curves C_1 given by $f(x,y) = 0$ of degree $d_1 \geq 1$ and C_2 given by $g(x,y) = 0$ of degree $d_2 \geq 1$. We will assume f, g have no common factor so that $C_1 \cap C_2$ consists of a finite set of points. Let P be one of those points and change coordinates to that $P = (0,0)$.

Definition 6 *If P is a nonsingular point on both C_1 and C_2, and the two tangent lines are distinct, then we define the intersection multiplicity $I_P(C_1, C_2)$ of $P \in C_1 \cap C_2$ to be 1. The picture is:*



*If P is singular on either curve or if C_1 and C_2 have a common tangent line, then $I_P(C_1, C_2) \geq 2$. The actual definition of $I_P(C_1, C_2)$ is a technical one and details can be found in Fulton [**?**]. In particular, if P is an m_f-fold singularity on C_1 and an m_g-fold singularity on C_2 then $I_P(C_1, C_2) \geq m_f m_g$ with equality if f_{m_f} and g_{m_g} have no line in common.*

The basic theorem in intersection theory is:

Bezout's Theorem:
$$\sum_{P \in C_1 \cap C_2} I_P(C_1, C_2) = d_1 d_2.$$

In other words, the number of common solutions to $f(x,y) = 0$ and $g(x,y) = 0$ is the product of their degrees $d_1 d_2$. Counting is done with multiplicity, complex solutions are counted, and solutions at infinity must also be counted.

Example 15: Let $f = (X^2 + Y^2)^2 + 3X^2Y - Y^3$ and $g = (X^2 + Y^2)^3 - 4X^2Y^2$. The two curves C_1 defined by $f = 0$ and C_2 defined by $g = 0$ intersect at $P = (0,0)$. Fulton [**?**] shows that the intersection multiplicity $I_P(C_1, C_2) = 14$. □

Finally, we want to introduce a fundamental invariant of a smooth projective curve C. If C is given by a homogeneous polynomial $F(Z_0, Z_1, Z_2) = 0$ of degree $d \geq 1$, and C is smooth, i.e., C has no singular points including at ∞, then we define the genus g_C of C to be

$$g_C = \frac{(d-1)(d-2)}{2}.$$

The genus is actually a topological invariant of C viewed as a one-dimensional complex manifold. Notice that for $d = 1, 2, 3, 4, 5, \ldots$, we have $g = 0, 0, 1, 3, 6, \ldots$, so that certain values of g, notably 4, do not occur as the genus of a *smooth* plane curve.

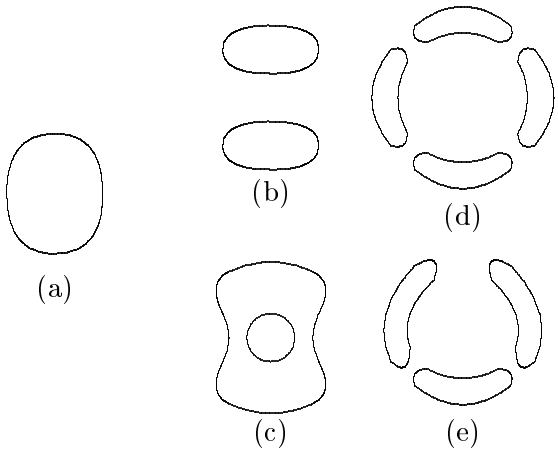
There is also a notion of genus for singular projective plane curves. The formula involves subtracting a correction term from $\frac{(d-1)(d-2)}{2}$ depending on the nature of the singularities, specifically

$$g = \frac{(d-1)(d-2)}{2} - \sum_P \frac{m_P(m_P-1)}{2}$$

where the sum is taken over all singular points P on the curve and over all singular points P that arise during successive steps in the resolution process (these are known as infinitely near singular points). The value m_P is the multiplicity of the singularity, i.e. P is an m_P-fold singular point. This g is actually the genus of the curve $\hat{C}$ obtained by resolving the singularities of C.

Example 16: A curve of degree four with two ordinary double points has $g = 1$. This case is particularly relevant to an example we have in mind, that illustrates some geometric artifacts that can be introduced when using resultants (see below). □

We conclude this section by mentioning Harnack's theorem on real plane curves. A smooth real plane curve consists of a number of ovals (see Harris [**?**, pp. 247–248]). Some cases look like those pictured below:



Note that we are looking at things projectively, so in the ordinary plane $\mathbb{R}^2$ some of the ovals may go off to infinity.

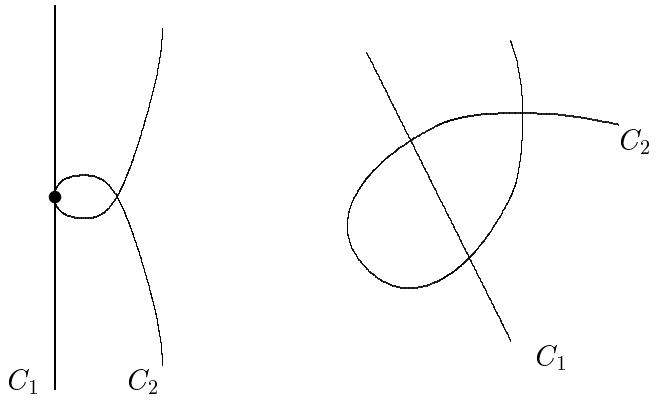
Theorem 3 *The maximum number of ovals a smooth plane curve of degree d can have is* $M_0 = \frac{(d-1)(d-2)}{2} + 1$.

3.2 Intersections of Surfaces in Space

In this section, we examine the intersection of two surfaces in space. This is critical for an example we have in mind. As before, we will frequently need to work over the complex numbers, and we will also want to "compactify" our curves and surfaces by working in complex projective three-space $\mathbb{P}^3_{\mathbb{C}}$.

Since the intersection of two surfaces S_1 and S_2, given by $f(x,y,z) = 0$ and $g(x,y,z) = 0$ respectively, is a union of curves $C_1 \cup \cdots \cup C_r$, it will be useful to say a few words about curves in space before discussing surface intersections. (Note that in the projective setting S_1 and S_2 would be given by the homogeneous polynomials $F(X,Y,Z,W) = 0$ and $G(X,Y,Z,W) = 0$ obtained by "homogenizing" $f(x,y,z)$ and $g(x,y,z)$.)

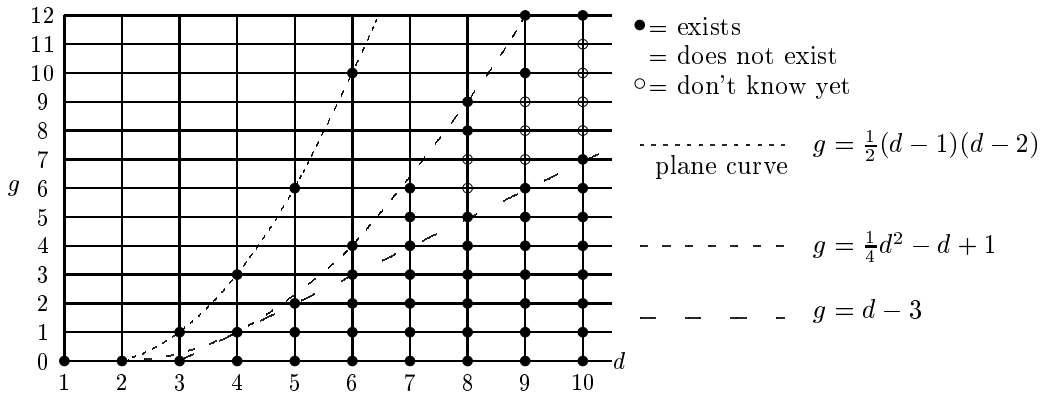
Example 17: The surfaces given by $xz - y^2 = 0$ and $y - x^2 = 0$ intersect in two curves. One, C_1, is the z-axis defined by $x = 0$, $y = 0$, and the other, C_2, is the so-called "twisted cubic" given parametrically by $x = t$, $y = t^2$, and $z = t^3$. For this same example in $\mathbb{P}^3_{\mathbb{C}}$, we would consider the homogeneous quadratic equations $XZ - Y^2 = 0$ and $YW - X^2 = 0$. At infinity ($W = 0$) the only solution is $(X : Y : Z : W) = (0 : 0 : 1 : 0)$. So the two curves C_1 and C_2 join at two points—the origin $(0,0,0)$ and this one point at infinity.



Curves in Space

Every smooth irreducible curve C in space has two fundamental invariants, its degree d and its genus g. The degree is defined to be the number of points in $C \cap H$ for a general plane H in three space. For certain planes, $C \cap H$ will contain fewer points (or perhaps C will be contained in H), but for most planes, $C \cap H$ will consist of d points. The genus g is harder to define. For smooth projective curves $C \subset \mathbb{P}^3_{\mathbb{C}}$ it is the usual topological genus. What we want however is a second notion of genus, called the arithmetic genus $p_a(C)$, which equals g for smooth curves, but which can be defined for any curve. One important aspect of $p_a(C)$ is that it is a birational invariant and so remains unchanged if the space curve C is appropriately projected into a plane.

Below is a table which illustrates possible combinations of d and g that can occur for a curve in space:



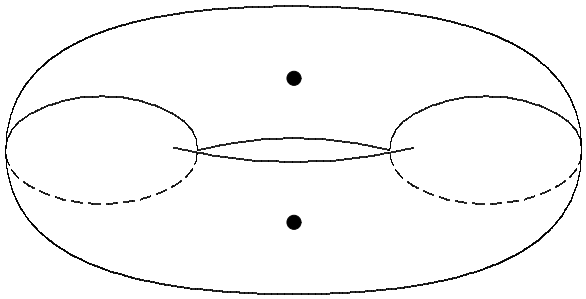
The most important example occurs when a curve C is the complete intersection of two surfaces of degrees a and b. In that case, we have:

Proposition 1 *If C is the complete intersection of two surfaces of degrees a and b respectively, then the arithmetic genus of C, $p_a(C) = \frac{1}{2}ab(a+b-4)+1$ and the degree of C is ab.*

Example 18: Consider the intersection of the cone $x^2+y^2-z^2=0$ with the cylinder $(x-2)^2+y^2-1=0$. These two surfaces intersect transversally because the Jacobian matrix

$$\begin{pmatrix} 2x & 2y & -2z \\ 2(x-2) & 2y & 0 \end{pmatrix}$$

has rank two at any point of the intersection. (To get all three 2×2 minors to have zero determinant, one would need either $y=0$, $z=0$, or $y=0$, $x=2$, and it is easy to see that no point on the intersection has these values.) Viewing things in $\mathbb{P}^3_{\mathbb{C}}$, where we must use the equations $X^2+Y^2-Z^2=0$ and $(X-2W)^2+Y^2-W^2=0$, we find that the surfaces intersect in two points at ∞, namely $(X:Y:Z:W)=(1:\pm i:0:0)$. The intersection is also transverse at these points. (Use the equations $1+y^2-z^2=0$ and $(1-2w)^2+y^2-w^2=0$ to compute the Jacobian $\begin{pmatrix} \pm 2i & 0 & 0 \\ \pm 2i & 0 & -4 \end{pmatrix}$ which clearly has rank 2.) Thus the intersection is a smooth curve C of degree 4 and arithmetic genus $p_a(C)=1$. Because C is smooth, the topological genus g is also 1. The topological picture is:



where the two ovals are the real points. The two points at ∞ are also shown.

There is an analogue of Bezout's Theorem for the intersection of two surfaces S_1 and S_2 of degrees a and b respectively. It says that

$$ab = \sum_C I_C(S_1, S_2)\text{deg}C$$

where the sum is taken over all irreducible curves C that occur in the intersection and $I_C(S_1, S_2)$ is the intersection multiplicity of S_1 and S_2 along C. For example, we previously considered two quadrics $xz - y^2 = 0$ and $y - x^2 = 0$ intersecting in a line C_1 which has degree 1 and the twisted cubic C_2 which has degree 3. The above formula gives $2 \cdot 2 = 3 + 1$. It follows that $I_{C_1}(S_1, S_2)$ and $I_{C_2}(S_1, S_2)$ are both 1 and that no other curves appear in the intersection.

Curves on Quadric Surfaces

In the examples above, the curves involved all lie on quadric surfaces. In this section, we will briefly consider curves on smooth quadrics. As described in [**?**], any smooth quadric surface is projectively equivalent to the one defined by $Z_0Z_3 - Z_1Z_2 = 0$ in $\mathbb{P}^3_{\mathbb{C}}$. This surface, known as the Serge surface is the image of the map

$$\begin{array}{ccccc} \mathbb{P}^1 & \times & \mathbb{P}^1 & \longrightarrow & \mathbb{P}^3 \\ (X_0 : X_1) & & (Y_0 : Y_1) & \longmapsto & (X_0Y_0 : X_0Y_1 : X_1Y_0 : X_1Y_1). \end{array}$$

To describe a curve on this surface, one specifies a bihomogeneous polynomial $F(X_0, X_1, Y_0, Y_1)$ of bidegree (r, s). This means that F should be homogeneous of degree r in the X variables and homogeneous of degree s in the Y variables. The degree of the curve defined by an F of bidegree (a, b) is $a + b$.

Example 19: $F(X_0, X_1, Y_0, Y_1) = X_0^2Y_1 - X_1^2Y_0$ has bidegree $(2, 1)$.

Example 20: Suppose $F(X_0, X_1, Y_0, Y_1)$ has bidegree $(m, m-1)$. The resulting curve C on $\mathbb{P}^1 \times \mathbb{P}^1$ can be described as a determinantal variety in $\mathbb{P}^3$. Namely, $C \subset \mathbb{P}^3$ is just the set of 2×3 matrices of the form

$$\begin{pmatrix} Z_0 & Z_1 & G(Z_0, Z_1, Z_2, Z_3) \\ Z_2 & Z_3 & H(Z_0, Z_1, Z_2, Z_3) \end{pmatrix}$$

that have rank ≤ 1. Here G and H are homogeneous polynomials of degree $m - 1$. For example, using $F(X_0, X_1, Y_0, Y_1) = X_0^2Y_1 - X_1^2Y_0$ as above, the matrices in question take the form

$$\begin{pmatrix} Z_0 & Z_1 & Z_2 \\ Z_2 & Z_3 & Z_1 \end{pmatrix}$$

Those of rank one are precisely the points on the quadric surface that lie on the curve cut out by F.

Plane Projections of Space Curves

Linear projection is a technique for reducing the number of variables in a problem. In general a linear projection is defined as follows: Select a linear subspace $L^d \subset \mathbb{P}^n$ of dimension d and a second linear subspace $\tilde{L}^{n-d-1}$ disjoint from L^d. The projection φ is a mapping

$$\varphi : \mathbb{P}^n - L^d \longrightarrow \tilde{L}^{n-d-1} \cong \mathbb{P}^{n-d-1}.$$

Specifically, for $p \in \mathbb{P}^n - L^d$ consider the linear space Λ_p of dimension $d + 1$ spanned by L^d and p, and define $\varphi(p)$ to be the point of $\tilde{L}^{n-d-1}$ which is the intersection of Λ_p with $\tilde{L}^{n-d-1}$. This is called the projection from L^d.

Example 21: In space, $\mathbb{P}^3$, let L be the point (zero dimensional linear subspace) $[x:y:t:w] = [1:0:0:0]$, and let $\tilde{L}$ be the plane, $\mathbb{P}^2$, defined by $x=0$. The projection φ is just the map

$$\begin{aligned} \mathbb{P}^3 - \{[1:0:0:0]\} &\xrightarrow{\varphi} \mathbb{P}^2 \\ [x:y:t:w] &\longmapsto [y:t:w]. \end{aligned}$$

Now if X is a subvariety of projective space $\mathbb{P}^n$ which doesn't meet L^d, we can consider its image $\varphi(X) \subset \mathbb{P}^{n-d-1}$ under the projection. X is usually described by a system of (homogeneous) polynomial equations $f_1(X_0,\ldots,X_n)=0,\ldots,f_s(X_0,\ldots,X_n)=0$. The standard tool to go from this system of equations to a system of equations in $n-d$ variables which describe $\varphi(X)$ is the resultant!

Example 22: Suppose C is a curve in space described by two equations:

$$a_r(y,t)x^r + a_{r-1}(y,t)x^{r-1} + \cdots + a_0(y,t) = 0$$

and

$$b_s(y,t)x^s + b_{s-1}(y,t)x^{s-1} + \cdots + b_0(y,t) = 0.$$

If we project C to the y,t-plane, we get a curve $\varphi(C)$ described by one equation, $R(y,t)=0$, in two variables. $R(y,t)$ is computed via the resultant:

$$R(y,t) = \det \begin{pmatrix} a_r(y,t) & a_{r-1}(y,t) & \cdots & \cdots & a_0(y,t) & \cdots & 0\cdots 0 \\ 0 & a_r(y,t) & a_{r-1}(y,t) & \cdots & & a_0(y,t) & 0\cdots 0 \\ & & & & & & \\ 0 & \cdots & \cdots & a_r(y,t) & \cdots & \cdots & a_0(y,t) \\ b_s(y,t) & b_{s-1}(y,t) & \cdots & & & & 0\cdots 0 \\ 0 & b_s(y,t) & \cdots & & & & 0\cdots 0 \\ \vdots & & & & & & 0 \\ 0 & 0 & \cdots & b_s(y,t) & \cdots & \cdots & b_0(y,t) \end{pmatrix}$$

which is the determinant of an $r+s$ by $r+s$ matrix.

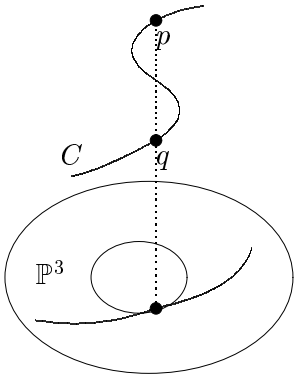
Now suppose $C \subset \mathbb{P}^3$ is a smooth irreducible curve of degree d and arithmetic genus g. We can project from any point $p \notin C$ to a plane also disjoint from p. The result of this projection is an irreducible plane curve $\varphi(C)$ also of degree d and arithmetic genus g. The curve $\varphi(C)$ however may be singular. In fact, if $g \neq \frac{(d-1)(d-2)}{2}$ then $\varphi(C)$ will be *forced* to have singularities. We have the following:

Theorem 4 *The general linear projection of a smooth irreducible curve $C \subset \mathbb{P}^3$ from a point $p \in \mathbb{P}^3$, $p \notin C$ is a plane curve having at worst only ordinary double points (nodes) for singularities.*

From our formula for the arithmetic genus above, we see that the number of nodes must be $\frac{(d-1)(d-2)}{2} - g$.

Example 23: If a non-singular curve C is the intersection of two quadrics in space, it will have degree four and arithmetic genus one. The general projection will be a plane curve $\varphi(C)$ of degree four with two ordinary double points.

Away from these double points the map from C to $\varphi(C)$ is one-to-one. The picture is:



Note that for projections in special directions things might become bad. □

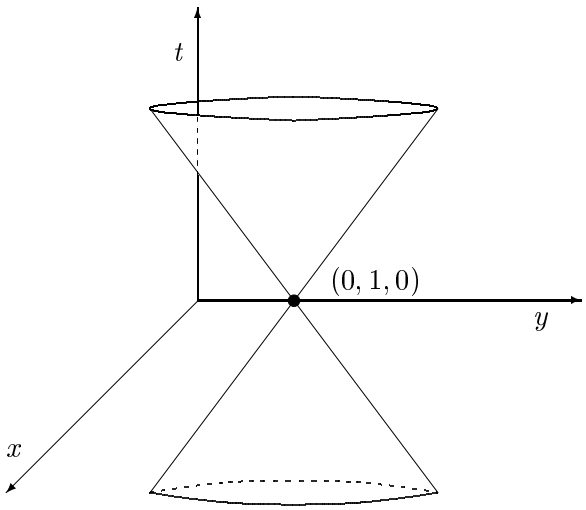
Detailed Example

We conclude this section with a lengthy example. For the most part we will work in ordinary three space, as opposed to projective three space. Thus our equations will *not* be homogeneous in four variables, but rather just polynomials in three variables. To analyze behavior at infinity it will be necessary to homogenize the equations.

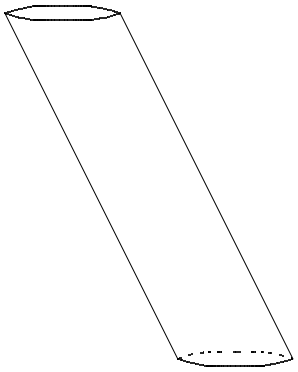
Our example starts with the curve C defined by the intersection of two conics:

$$\begin{aligned} x^2 + (y-1)^2 - t^2 &= 0 \\ \left(x - \left(4 - \frac{t}{2}\right)\right)^2 + \left(y - \frac{t}{2}\right)^2 - 1 &= 0. \end{aligned} \tag{8}$$

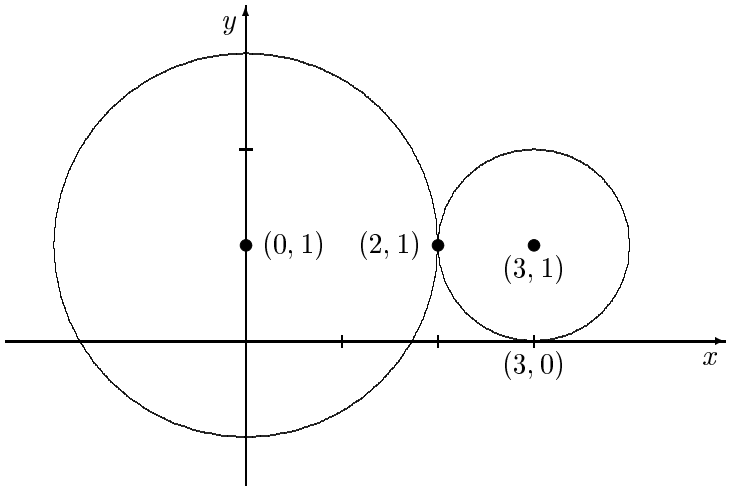
In $\mathbb{R}^3$ with coordinates x, y, t, the first equation represents a cone with vertex at $(0, 1, 0)$



and the second equation represents a slanted cylinder:



Another interpretation is that the first equation represents an expanding circle in the plane and that the second equation represents a moving circle. Pictured below is the situation at time $t = 2$:



Notice that $x = 2$, $y = 1$, $t = 2$ is the point of "first contact".

Projectively, we would need to work with the homogenized versions of the equations (**??**):

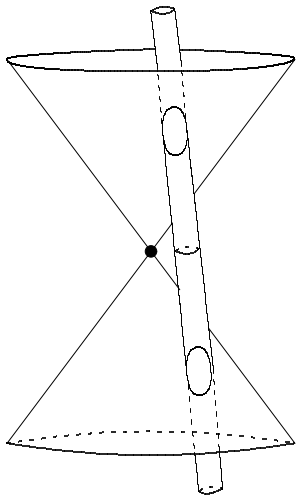
$$x^2 + (y - w)^2 - t^2 = 0$$
$$\left(x - \left(4w - \frac{t}{2}\right)\right)^2 + \left(y - \frac{t}{2}\right)^3 - w^2 = 0.$$

The points at infinity in $\mathbb{P}^3$ correspond to solutions with $w = 0$. There are exactly four such points in $\mathbb{P}^3$, namely

$$(x : y : z : t) = (-i : 1 : 0 : 0), \quad (i : 1 : 0 : 0), \quad \left(-\frac{3}{4} + \frac{i}{4} : \frac{3}{4} + \frac{i}{4} : 1 : 0\right)$$
$$\text{or} \quad \left(-\frac{3}{4} - \frac{i}{4} : \frac{3}{4} - \frac{i}{4} : 1 : 0\right).$$

With a little work one can show that $C \subset \mathbb{P}^3$ is a smooth irreducible curve (as usual we are assuming that we are working over the complex numbers $\mathbb{C}$).

The real solutions form two ovals in $\mathbb{R}^3$:



Now we will project C into the y,t-plane, the plane defined by $x=0$. This is a linear projection φ from the point $(1:0:0:0)$ in $\mathbb{P}^3$ to the plane $x=0$. Note that $(1:0:0:0)\notin C$ so that the projection φ is well-defined on all of C. To find the equation for $\varphi(C)\subset\mathbb{P}^2$, we write our equations as polynomials in x:

$$\begin{aligned} x^2+(y^2-t^2) &= 0 \\ 4x^2+(4t-32)x+((t-8)^2+(2y-t)^2-4) &= 0. \end{aligned}$$

We then eliminate x by taking the resultant:

$$\det\begin{pmatrix} 1 & 0 & y^2-t^2 & 0 \\ 0 & 1 & 0 & y^2-t^2 \\ 4 & 4t-32 & \star & 0 \\ 0 & 4 & 4t-32 & \star \end{pmatrix} \qquad \star=((t-8)^2+(2y-t)^2-4).$$

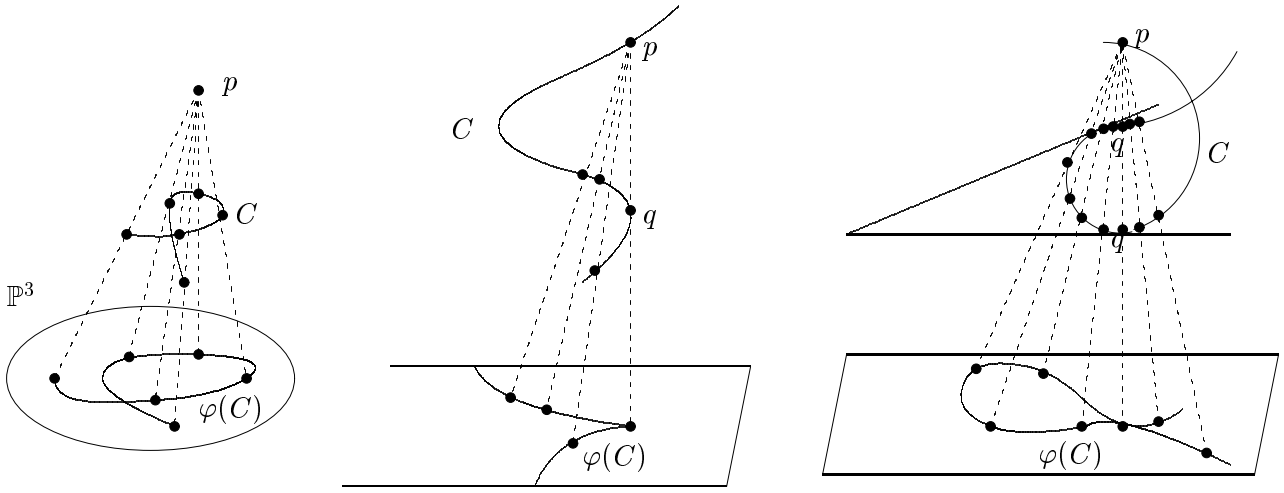
The result (after dividing by 4) is

$$g(y,t)=(8t^2-80t+272)y^2+(-12t^3+48t^2-48t-288)y+(5t^4+16t^3-20t^2-512t+1040) \tag{9}$$

and the projection $\varphi(C)$ is described by $g(y,t)=0$, or in projective space $\mathbb{P}^2$ with homogeneous coordinates y,t,w by:

$$\begin{aligned} 0 =& 8t^2y^2-80ty^2w+272y^2w^2-12t^3y+48t^2yw-48tyw^2 \\ & -288yw^3+5t^4+16t^3w-20t^2w^2-512tw^3+1040w^4. \end{aligned} \tag{10}$$

This is a plane curve of degree 4. We expect this degree because the original $C\subset\mathbb{P}^3$ had degree 4, being the intersection of two quadrics. Now a *smooth* plane curve of degree 4 has arithmetic genus 3 while our curve has arithmetic genus 1. This means our curve has some singularities. In general, we expect it to have two ordinary double points (nodes), but it could have cusps instead, or it could have a single tacnode. These singularities occur as a result of the projection:



We will see below that $\varphi(C)$ does in fact have two nodes.

What do the real points on $\varphi(C)$ in $\mathbb{R}^2$ look like. We can view

$$0 = (8t^2 - 80t + 272)y^2 + (-12t^3 + 48t^2 - 48t - 288)y + (5t^4 + 16t^3 - 20t^3 - 512t + 1040)$$

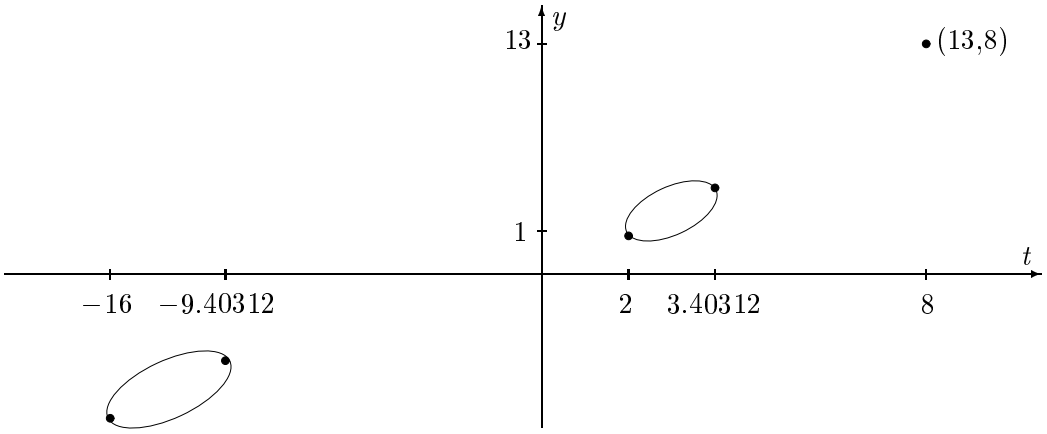
as a quadratic equation in y of the form

$$Ay^2 + By + C = 0.$$

The discriminant is $B^2 - 4AC$, which equals

$$-16t^6 - 64t^5 + 3776t^4 - 5120t^3 - 200704t^2 + 917504t - 1048576.$$

The roots of the discriminant are -16, -9.40312, 2, 3.40312, and a double root at 8. This double root is a bit curious. It is an isolated point at $(y, t) = (13, 8)$.



We see the two ovals we expect. When $t = 2$, we have $(y, t) = (1, 2)$ being the point of "first contact" discussed above. The other times $t = -16$, -9.40312, and 3.40312 also correspond to when the two circles are tangent.

One can easily show that $(y,t) = (13,8)$ is an ordinary double point. We change coordinates to move this point to the origin by setting

$$t = r + 8 \quad \text{and} \quad y = s + 13$$

in $g(y,t)$. This leads to

$$12(43r^2 - 28rs + 12s^2) + \text{ higher order terms.}$$

Since no linear term is present $(13,8)$ is a singular point, and because $43r^2 - 28rs + 12s^2$ factors into two distinct (complex) linear factors, it is an ordinary double point. Two points on C project to $(y,t) = (13,8)$; they are $(x,y,t) = (4\sqrt{-5}, 13, 8)$ and $(-4\sqrt{-5}, 13, 8)$.

C must have another singularity, which in this case occurs at infinity. Setting $w = 0$ in (**??**) gives us the points of C at infinity. They are $(y : t : w) = (1 : 0 : 0)$, $\left(\frac{3}{4} + \frac{i}{4}, : 1 : 0\right)$, and $\left(\frac{3}{4} - \frac{i}{4} : 1 : 0\right)$. It is clear that $(x : y : t : w) = (i : 1 : 0 : 0)$ and $(-i : 1 : 0 : 0)$ on C both project to $(y : t : w) = (1 : 0 : 0)$.

To see what $\varphi(C)$ looks like near $(1 : 0 : 0)$, we set $y = 1$ in (**??**) to get:

$$8t^2 + 272w^2 - 80tw + \text{ higher order terms.}$$

Again, $8t^2 + 272w^2 - 80tw$ factors into two distinct complex lines showing that $(1 : 0 : 0)$ is a second node on $\varphi(C)$.

Apart from these two points $(y : t : w) = (13 : 8 : 1)$ and $(1 : 0 : 0)$ on $\varphi(C)$ and the four points above them on C, the projection from C to $\varphi(C)$ can be shown to be one-to-one. Each smooth point on $\varphi(C)$ has exactly one point on C projecting to it. This concludes our example. It is an excellent example of the kinds of geometric, algebraic, and numerical phenomena that can occur when we use resultants to eliminate variables.

4 Complexity and Computational Issues

4.1 Resultants and Combinatorial Methods

In this section we briefly address certain complexity and computational issues related largely to the number of terms that can appear in the classical Sylvester resultant.

Terms and Coefficients in the Resultant

We begin by attempting to understand what monomials and what coefficients can occur in a resultant. As easy examples show (see section 1 above), the number of monomials that actually occur is far less than the maximum (the total number of monomials of the appropriate degree and homogeneity).

Let $f(x) = a_m x^m + \cdots + a_1 x + a_0$ and $g(x) = b_n x^n + \cdots + b_1 x + b_0$ and write

$$R_{m,n}(f,g) = \sum_{p,q} c_{pq} a^p b^q$$

where

$$\begin{aligned} p &= (p_0, \ldots, p_m), & q &= (q_0, \ldots, q_n) \\ a^p &= a_0^{p_0} a_1^{p_1} \ldots a_m^{p_m}, & b^q &= b_0^{q_0} b_1^{q_1} \ldots b_n^{q_n} \end{aligned}$$

and $p \in \mathbb{Z}_+^{m+1}$ with $\sum_{i=0}^m p_i = n$ and $q \in \mathbb{Z}_+^{n+1}$ with $\sum_{j=0}^n q_j = m$. Here $\mathbb{Z}_+$ is the set of non-negative integers.

We denote by $\Delta^m(n)$ the set of all $p = (p_0, \ldots, p_m) \in \mathbb{Z}_+^{m+1}$ with $\sum_{i=0}^m p_i = n$.

Example 24:

$$\Delta^2(2) = \{(2,0,0), (0,2,0), (0,0,2), (1,1,0), (0,1,1), (1,0,1)\}.$$

□

Note that $c_{pq} = 0$ unless $p \in \Delta^m(n)$ and $q \in \Delta^n(m)$.

Now given $q \in \Delta^n(m)$ define a symmetric polynomial $M_q(x_1, \ldots, x_m)$ as the sum of all monomials $x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_m^{\alpha_m}$ such that q_0 of the exponents α_i are equal to n, q_1 of the exponents are equal to $n-1$, etc., down to q_n of the exponents equaling 0.

Example 25: If $m = n = 2$ and $q = (q_0, q_1, q_2) = (1, 0, 1)$, then

$$M_q(x_1, x_2) = x_1^2 x_2^0 + x_1^0 x_2^2 = x_1^2 + x_2^2$$

because we must have all monomials with one exponent equal to 2 and one equal to 0.

Example 26: If $m = n = 2$ and $q = (q_0, q_1, q_2) = (0, 2, 0)$, then

$$M_q(x_1, x_2) = x_1^1 x_2^1 = x_1 x_2$$

because we must have two exponents equal to 1.

The $M_q(x_1, \ldots, x_m)$ are clearly symmetric polynomials and so can be written in terms of the elementary symmetric functions $e_i(x_1, \ldots, x_m) = \sum_{1 \le j_1 < \cdots < j_i \le m} x_{j_1} \ldots x_{j_i}$, for $i = 0, \ldots, m$.

Example 27: $m = 2$, $e_0 = 1$, $e_1 = x_1 + x_2$, and $e_2 = x_1 x_2$.

The next result tells how to compute the coefficients c_{pq}, $p \in \Delta^m(n)$, $q \in \Delta^n(m)$ in the resultant $R_{m,n}(f,g)$.

Theorem 5 *For $p = (p_0, \ldots, p_m)$ with $p_i \geq 0$ and $\sum_{i=0}^m p_i = n$ and $q = (q_0, \ldots, q_n)$ with $q_j \geq 0$ and $\sum_{j=0}^n q_j = m$, the coefficient c_{pq} of the monomial $a_0^{p_0} \ldots a_m^{p_m} b_0^{q_0} \ldots b_n^{q_n}$ in the resultant $R_{m,n}(f,g)$ where $f(x) = a_m x^m + \cdots + a_0$ and $g(x) = b_n x^n + \cdots + b_0$ is $(-1)^{\sum_{i=0}^m i p_i}$ times the coefficient of $\prod_{i=1}^m e_i(x_1, \ldots, x_m)^{p_i}$ in the expansion of $M_q(x_1, \ldots, x_m)$ in terms of the elementary symmetric functions $e_i(x_1, \ldots, x_m)$.*

Example 28: $m = 2$, $n = 2$, $p = (p_0, p_1, p_2) = (1, 0, 1)$ and $q = (q_0, q_1, q_2) = (1, 0, 1)$. We are looking for the coefficient of $a_0 a_2 b_0 b_2$ in the resultant of two quadratic polynomials. (Note $a_0 a_2 b_0 b_2 = a_0^1 a_1^0 a_2^1 b_0^1 b_1^0 b_2^1$.) Example 25 shows $M_q(x_1, x_2) = x_1^2 + x_2^2$ and in terms of the elementary symmetric functions (Example 27),

$$M_q(x_1, x_2) = x_1^2 + x_2^2 = (x_1 + x_2)^2 - 2x_1 x_2 = e_1^2 - 2e_2.$$

The coefficient c_{pq} we are looking for is $(-1)^2$ times the coefficient of e_2. Thus $c_{pq} = -2$ which is correct (see the last term in Example 1).

Algorithm. This yields an algorithm for finding the coefficients of the resultant based on the algorithm for writing a symmetric polynomial in terms of the elementary symmetric polynomials.

4.2 Partitions, Symmetric Functions, and Newton Polytopes

Partitions play an important role in the representation theory of the symmetric group. They also play an important role in determining which terms can occur in the resultant.

Definition 7 *A partition of length $\leq m$ is just a sequence of non-negative numbers $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_m$ which we denote by $\lambda = (\lambda_1, \lambda_2, \ldots \lambda_m)$. The numbers λ_i are the parts of λ.*

Each partition gives rise to a symmetric polynomial

$$m_\lambda(x_1, \ldots, x_m) = \sum_{(\alpha_1, \ldots, \alpha_m) = \sigma(\lambda_1, \ldots, \lambda_m)} x_1^{\alpha_1} \ldots x_m^{\alpha_m}$$

where σ runs through all *distinct* permutations of $(\lambda_1, \ldots, \lambda_m)$.

Example 29: $\lambda = (2, 1)$

$$m_{(2,1)}(x_1, x_2) = x_1^2 x_2^1 + x_1^1 x_2^2 = x_1^2 x_2 + x_1 x_2^2.$$

Example 30: $M_q(x_1, \ldots, x_m)$ defined above for $q = (q_0, \ldots, q_n)$, $q_j \geq 0$, $\sum_{j=0}^n q_j = m$ coincides with $m_\lambda(x_1, \ldots, x_m)$ for the partition

$$\lambda = (\underbrace{n, \ldots, n}_{q_0 \text{ times}}, \underbrace{n-1, \ldots, n-1}_{q_1 \text{ times}}, \ldots, \underbrace{1, \ldots, 1}_{q_{n-1} \text{ times}}, \underbrace{0, \ldots, 0}_{q_n \text{ times}}).$$

Notice λ has $\sum_{j=0}^n q_j = m$ parts.

Example 31: The elementary symmetric polynomials $e_i(x_1, \ldots, x_m)$ are also of the form $m_\lambda(x_1, \ldots, x_m)$ for the partition $\lambda = (\underbrace{1, \ldots, 1}_{i \text{ times}}, \underbrace{0, \ldots, 0}_{m-i \text{ times}})$. Notice λ has m parts.

Now the m_λ as λ runs over all partitions with m parts form a basis for the infinite dimensional vector space of symmetric polynomials in m variables $x_1, \ldots, x_m$. A different basis is given by

$$\prod_{i=0}^m e_i(x_1, \ldots, x_m)^{p_i}.$$

We encode this by a partition μ having p_i parts equal to i for $i = 0, \ldots, m$

$$\mu = (\underbrace{m, \ldots, m}_{p_m \text{ times}}, \underbrace{m-1, \ldots, m-1}_{p_{m-1} \text{ times}}, \ldots, \underbrace{1, \ldots, 1}_{p_1 \text{ times}}, \underbrace{0, \ldots, 0}_{p_0 \text{ times}})$$

and we write

$$e_\mu(x_1, \ldots, x_m) = \prod_{i=0}^{m} e_i(x_1, \ldots, x_m)^{p_i}$$

for any partition μ with parts $\leq m$ but of any length. Note: we define $e_0(x_1, \ldots, x_m) = 1$.

A key observation is that the coefficients in the resultant are essentially the entries in the change of basis matrix between the m_λ and the e_μ. Unfortunately this doesn't yield much information. However, if we write

$$e_\mu = \sum_\lambda d_{\lambda\mu} m_\lambda$$

much can be said about the $d_{\lambda\mu}$. If $\lambda = (\lambda_1, \ldots, \lambda_m)$ and $\mu = (\mu_1, \ldots, \mu_n)$ with $\mu_j \leq m$ for every j, then $d_{\lambda\mu}$ is equal to the number of $m \times n$ matrices with 0,1 entries having row sums $\lambda_1, \ldots, \lambda_m$ and column sums $\mu_1, \ldots, \mu_n$.

Example 32: $m = 2$, $n = 2$, $\lambda = (2, 0)$, $\mu = (2, 0)$; then $d_{\lambda\mu} = 0$ as no 2×2 matrix can have the required row and column sums, i.e., $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $a, b, c, d \in \{0, 1\}$ with $a + b = 2$, $c + d = 0$, $a + c = 2$, and $b + d = 0$. Notice that

$$e_\mu = \prod_{i=0}^{2} e_i(x_1, x_2)^{p_i} = e_2^1 e_1^0 e_0^1 = e_2 = x_1 x_2$$

because $\mu = (2, 0)$ has one part equal to 2, no parts equal to 1, and one part equal to 0. To check that $d_{\lambda\mu} = 0$, note that

$$m_{(1,1)} = x_1 x_2$$

so that $e_\mu = m_{(1,1)}$ and as $m_\lambda = m_{(2,0)}$ doesn't occur in this relationship, we have $d_{\lambda\mu} = 0$. If we had chosen $\mu = (1, 1)$ then $d_{\lambda\mu}$ would be 1 because the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ has row sums 2,0 and column sums 1,1, and it is the only such matrix. The $d_{\lambda\mu}$ play an important role in combinatorics and in the representation theory of finite groups.

We must define two concepts:

Definition 8 *If $\lambda = (\lambda_1, \ldots, \lambda_m)$ and $v = (v_1, \ldots, v_m)$ are two partitions of length m. We say that v dominates λ and write $v \geq \lambda$ if $v_1 + \cdots + v_i \geq \lambda_1 + \cdots + \lambda_i$ for $i = 1, \ldots, m-1$ and $v_1 + \cdots + v_m = \lambda_1 + \ldots + \lambda_m$.*

Example 33: $(4, 1, 1)$ dominates $(3, 2, 1)$ because $4 \geq 3$, $4 + 1 \geq 3 + 2$, and $4 + 1 + 1 = 3 + 2 + 1$.

Definition 9 *If $\mu = (\mu_1, \ldots, \mu_n)$ is a partition with parts $\mu_j \leq m$ for all j and if μ has p_i parts equal to i, then we define the conjugate partition μ^* to be:*

$$u^* = (p_1 + \cdots + p_m, p_2 + \cdots + p_m, \ldots, p_m).$$

Example 34: $m = 3$, $\mu = (3, 2, 2, 0)$ then $u^* = (3, 3, 1)$ because $p_0 = 1$, $p_1 = 0$, $p_2 = 2$, and $p_3 = 1$.

We can now bound which terms appear in the resultant.

Theorem 6 *Let $p = (p_0, \ldots, p_m)$ with $p_i \geq 0$ and $\sum_{i=0}^{m} p_i = n$ and $q = (q_0, \ldots, q_n)$ with $q_j \geq 0$ and $\sum_{j=0}^{n} q_j = m$ and let λ, μ be the following partitions:*

$$\lambda = (\underbrace{n, \ldots, n}_{q_0}, \underbrace{n-1, \ldots, n-1}_{q_1}, \ldots, \underbrace{1, \ldots, 1}_{q_{n-1}}, \underbrace{0, \ldots, 0}_{q_n})$$
$$\mu = (\underbrace{m, \ldots, m}_{p_m}, \underbrace{m-1, \ldots, m-1}_{p_{m-1}}, \ldots, \underbrace{1, \ldots, 1}_{p_1}).$$

(Note: λ has length m and μ has parts $\mu_j \leq m$.) Then $c_{pq} = 0$ and the term $a_0^{p_0} \ldots a_m^{p_m} b_0^{q_0} \ldots b_n^{q_n}$ does **not** *appear in the resultant unless $\mu^* \leq \lambda$. Moreover if $\mu^* = \lambda$ then $c_{pq} = (-1)^{\sum_{i=0}^{m} i p_i} = (-1)^{\sum_{i \text{ odd}} p_i}$.*

Theorem 7 *The pairs $(p, q) = (p_0, \ldots, p_m, q_0, \ldots, q_n) \in \mathbb{Z}_+^{n+m+2} \subset \mathbb{R}^{n+m+2}$ with $\mu^* = \lambda$ are exactly the vertices of the Newton polytope of the resultant. Thus a term occurs in $R_{n,m}(f, g)$ only if it is in the convex hull of this set of points.*

Note: Without loss of generality, we can assume μ has p_0 parts equal to 0, so that μ will have length n.

Example 35:

$$f(x) = a_2 x^2 + a_1 x + a_0, \quad a_2 \neq 0$$
$$g(x) = b_2 x^2 + b_1 x + b_0, \quad b_2 \neq 0$$

$p = (p_0, p_1, p_2)$ and $q = (q_0, q_1, q_2)$ must be in the set $\{(2,0,0), (0,2,0), (0,0,2), (1,1,0), (0,1,1), (1,0,1)\}$. Thus there are at most 36 monomials in the resultant $R_{2,2}(f, g)$. We make a table

	λ	μ	u^*
$(2,0,0)$	$(2,2)$	$(0,0)$	$(0,0)$
$(0,2,0)$	$(1,1)$	$(1,1)$	$(2,0)$
$(0,0,2)$	$(0,0)$	$(2,2)$	$(2,2)$
$(1,1,0)$	$(2,1)$	$(1,0)$	$(1,0)$
$(0,1,1)$	$(1,0)$	$(2,1)$	$(2,1)$
$(1,0,1)$	$(2,0)$	$(2,0)$	$(1,1)$.

We then list the partitions which a given λ dominates:

λ	
$(2,2)$	$\{(2,2)\}$
$(1,1)$	$\{(1,1)\}$
$(0,0)$	$\{(0,0)\}$
$(2,1)$	$\{(2,1)\}$
$(1,0)$	$\{(1,0)\}$
$(2,0)$	$\{(2,0)(1,1)\}$.

This leads to seven pairs for which $\lambda \geq \mu^*$, six of which have $\lambda = \mu^*$. We list the corresponding (p_0, p_1, p_2) and (q_0, q_1, q_2). Remember that q goes with λ and that p goes with μ, and that p goes with the a's and q with the b's

$(q_0 q_1 q_2)$	$(p_0 p_1 p_2)$	
$(2,0,0)$	$(0,0,2)$	$a_2^2 b_0^2$
$(0,2,0)$	$(1,0,1)$	$a_0 a_2 b_1^2$
$(0,0,2)$	$(2,0,0)$	$a_0^2 b_2^2$
$(1,1,0)$	$(0,1,1)$	$a_1 a_2 b_0 b_1$
$(0,1,1)$	$(1,1,0)$	$a_0 a_1 b_1 b_2$
$(1,0,1)$	$(0,2,0)$	$a_1^2 b_0 b_2$
$(1,0,1)$	$(1,0,1)$	$a_0 a_2 b_0 b_2$.

The coefficients of the first six terms are given by $(-1)^{\sum_{i=0}^{2} i p_i}$. Thus the resultant is

$$R_{2,2}(f,g) = a_0^2 b_2^2 + a_1^2 b_0 b_2 + a_2^2 b_0^2 - a_0 a_1 b_1 b_2 - a_1 a_2 b_0 b_1 + a_0 a_2 b_1^2 + \gamma a_0 a_2 b_0 b_2$$

which agrees with Example 1 except for the one unknown coefficient γ.

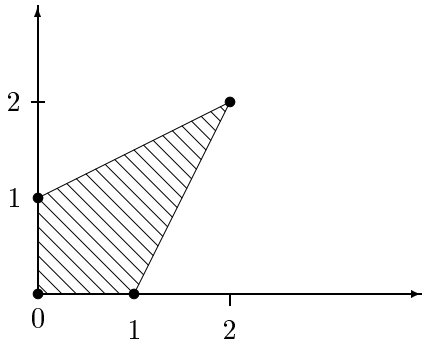
The Newton Polytope of the Resultant

The section above describes an algorithm for finding the Newton polytope of the resultant. Recall that the Newton polytope $N(f)$ of a polynomial in several variables

$$f = f(x_1, \ldots, x_m) = \sum_{\substack{\alpha=(\alpha_1,\ldots,\alpha_n)\in\mathbb{Z}_+^n \\ \text{with only finitely} \\ \text{many } c_\alpha \neq 0}} c_\alpha x_1^{\alpha_1} \ldots x_m^{\alpha_m}$$

is defined to be the convex hull in $\mathbb{R}^m$ of the integral lattice points $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{Z}_+^m$ for which $c_\alpha \neq 0$.

Example 36: $f(x_1, x_2) = 1 + x_1 + x_2 + x_1^2 x_2^2$ has $N(f)$ equal to the convex hull of $\{(0,0), (1,0), (0,1), (2,2)\}$, i.e., $N(f)$ looks like:



Notice that $(1,1)$ is also in $N(f)$ but the monomial $x_1 x_2$ does not occur in f. Thus knowing the Newton polytope of a polynomial only bounds what terms can occur.

We can prove a few facts about the Newton polytope $N_{m,n}$ of the resultant $R_{m,n}(f,g)$.

Theorem 8 *The polytope $N_{m,n}$ has dimension $m+n-1$ in $\mathbb{R}^{m+n+2}$ and lies in the linear space cut out by*

$$\sum_{i=0}^{m} p_i = n, \qquad \sum_{j=0}^{n} q_j = m, \qquad \sum_{i=0}^{m}(m-i)p_i + \sum_{j=0}^{n}(n-j)q_j = mn.$$

□

Example 37: When $m=2$ and $n=2$ the first two equations yield 36 possibilities for (p_0,p_1,p_2) and (q_0,q_1,q_2). The third condition forces

$$2p_0 + p_1 + 2q_0 + q_1 = 4,$$

reducing us to the following possibilities:

(p_0,p_1,p_2)	(q_0,q_1,q_2)	
$(2,0,0)$	$(0,0,2)$	
$(0,2,0)$	$(0,2,0)$	or $(1,0,1)$
$(0,0,2)$	$(2,0,0)$	
$(1,1,0)$	$(0,1,1)$	
$(0,1,1)$	$(1,1,0)$	
$(1,0,1)$	$(1,0,1)$	or $(0,2,0)$

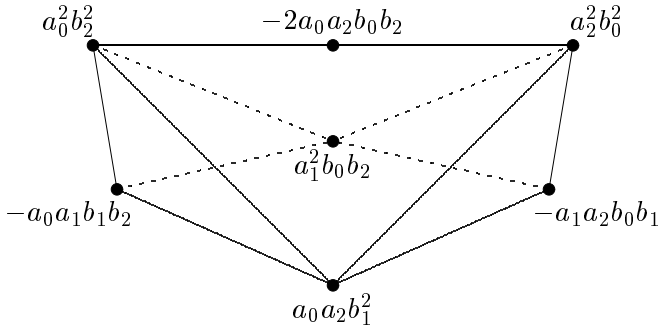
,

for a total of 8 possibilities of which only seven actually occur. The pair that does not appear is $(0,2,0),(0,2,0)$ which corresponds to the monomial $a_1^2b_1^2$.

Example 38: $N_{2,2}$ has dimension 3. It can be realized in $\mathbb{R}^3$ and is pictured below.

Theorem 9 *If $m,n \geq 2$ then $N_{m,n}$ has exactly $mn+3$ faces.*

Example 39: $m=2$, $n=2$, then $N_{2,2}$ has 7 faces. $N_{2,2}$ is pictured below with its 6 vertices. Since it has 7 faces and 6 vertices it must have 11 edges as #vertices − #faces + #edges must equal 2.



Note that the one non-vertex point $(1,0,1,1,0,1)$, which corresponds to $a_0a_2b_0b_2$, is the midpoint between $(2,0,0,0,0,2)$ and $(0,0,2,2,0,0)$.

There are additional combinatorial ways to describe the vertices of $N_{m,n}$ but they involve considerable technicalities.

Example 40: As a final example, we work out the $m = n = 3$ case. Let $f(x) = a_3x^3+a_2x^2+a_1x+a_0$, $a_3 \neq 0$, and $g(x) = b_3x^3 + b_2x^2 + b_1x + b_0$, $b_3 \neq 0$. The resultant $R_{3,3}(f, g)$ is bihomogeneous of bidegree (3,3). There could be as many as 400 terms. We list the 20 possibilities for (p_0, p_1, p_2, p_3) and (q_0, q_1, q_2, q_3), and the associated partitions λ, μ, μ^*.

	λ	μ	μ^*
$(3,0,0,0)$	$(3,3,3)$	$(0,0,0)$	$(0,0,0)$
$(0,3,0,0)$	$(2,2,2)$	$(1,1,1)$	$(3,0,0)$
$(0,0,3,0)$	$(1,1,1)$	$(2,2,2)$	$(3,3,0)$
$(0,0,0,3)$	$(0,0,0)$	$(3,3,3)$	$(3,3,3)$
$(2,1,0,0)$	$(3,3,2)$	$(1,0,0)$	$(1,0,0)$
$(2,0,1,0)$	$(3,3,1)$	$(2,0,0)$	$(1,1,0)$
$(2,0,0,1)$	$(3,3,0)$	$(3,0,0)$	$(1,1,1)$
$(0,2,1,0)$	$(2,2,1)$	$(2,1,1)$	$(3,1,0)$
$(1,2,0,0)$	$(3,2,2)$	$(1,1,0)$	$(2,0,0)$
$(0,2,0,1)$	$(2,2,0)$	$(3,1,1)$	$(3,1,1)$.
$(0,0,2,1)$	$(1,1,0)$	$(3,2,2)$	$(3,3,1)$
$(0,1,2,0)$	$(2,1,1)$	$(2,2,1)$	$(3,2,0)$
$(1,0,2,0)$	$(3,1,1)$	$(2,2,0)$	$(2,2,0)$
$(1,0,0,2)$	$(3,0,0)$	$(3,3,0)$	$(2,2,2)$
$(0,1,0,2)$	$(2,0,0)$	$(3,3,1)$	$(3,2,2)$
$(0,0,1,2)$	$(1,0,0)$	$(3,3,2)$	$(3,3,2)$
$(1,1,1,0)$	$(3,2,1)$	$(2,1,0)$	$(2,1,0)$
$(1,1,0,1)$	$(3,2,0)$	$(3,1,0)$	$(2,1,1)$
$(1,0,1,1)$	$(3,1,0)$	$(3,2,0)$	$(2,2,1)$
$(0,1,1,1)$	$(2,1,0)$	$(3,2,1)$	$(3,2,1)$

We now list the partitions for which $\lambda \geq \mu^*$.

λ	μ^*	μ^*	μ^*
$(3,3,3)$	$(3,3,3)$		
$(2,2,2)$	$(2,2,2)$		
$(1,1,1)$	$(1,1,1)$		
$(0,0,0)$	$(0,0,0)$		
$(3,3,2)$	$(3,3,2)$		
$(3,3,1)$	$(3,3,1)$	$(3,2,2)$	
$(3,3,0)$	$(3,3,0)$	$(3,2,1)$	$(2,2,2)$
$(2,2,1)$	$(2,2,1)$		
$(3,2,2)$	$(3,2,2)$		
$(2,2,0)$	$(2,2,0)$	$(2,1,1)$	
$(1,1,0)$	$(1,1,0)$		
$(2,1,1)$	$(2,1,1)$		
$(3,1,1)$	$(3,1,1)$	$(2,2,1)$	
$(3,0,0)$	$(3,0,0)$	$(2,1,0)$	$(1,1,1)$
$(2,0,0)$	$(2,0,0)$	$(1,1,0)$	
$(1,0,0)$	$(1,0,0)$		
$(3,2,1)$	$(3,2,1)$	$(2,2,2)$	
$(3,2,0)$	$(3,2,0)$	$(3,1,1)$	$(2,2,1)$
$(3,1,0)$	$(3,1,0)$	$(2,2,0)$	$(2,1,1)$
$(2,1,0)$	$(2,1,0)$	$(1,1,1)$	

This leads to 34 terms; 20 terms

(q_0,q_1,q_2,q_3)	(p_0,p_1,p_2,p_3)	
$(3,0,0,0)$	$(0,0,0,3)$	$-a_3^3b_0^3$
$(0,3,0,0)$	$(1,0,0,2)$	$+a_0a_3^2b_1^3$
$(0,0,3,0)$	$(2,0,0,1)$	$-a_0^2a_3b_2^3$
$(0,0,0,3)$	$(3,0,0,0)$	$+a_0^3b_3^3$
$(2,1,0,0)$	$(0,0,1,2)$	$+a_2a_3^2b_0^2b_1$
$(2,0,1,0)$	$(0,0,2,1)$	$-a_2^2a_3b_0^2b_2$
$(2,0,0,1)$	$(0,0,3,0)$	$+a_2^3b_0^2b_3$
$(0,2,1,0)$	$(1,0,1,1)$	$-a_0a_2a_3b_1^2b_2$
$(1,2,0,0)$	$(0,1,0,2)$	$-a_1a_3^2b_0b_1^2$
$(0,2,0,1)$	$(1,0,2,0)$	$+a_0a_2^2b_1^2b_3$
$(0,0,2,1)$	$(2,0,1,0)$	$+a_0^2a_2b_2^2b_3$
$(0,1,2,0)$	$(1,1,0,1)$	$+a_0a_1a_3b_1b^2$
$(1,0,2,0)$	$(0,2,0,1)$	$-a_1^2a_3b_0b_2^2$
$(1,0,0,2)$	$(0,3,0,0)$	$-a_1^3b_0b_3^2$
$(0,1,0,2)$	$(1,2,0,0)$	$+a_0a_1^2b_1b_3^2$
$(0,0,1,2)$	$(2,1,0,0)$	$-a_0^2a_1b_2b_3^2$
$(1,1,1,0)$	$(0,1,1,1)$	$+a_1a_2a_3b_0b_1b_2$
$(1,1,0,1)$	$(0,1,2,0)$	$-a_1a_2^2b_0b_1b_3$
$(1,0,1,1)$	$(0,2,1,0)$	$+a_1^2a_2b_0b_2b_3$
$(0,1,1,1)$	$(1,1,1,0)$	$-a_0a_1a_2b_1b_2b_3$

where the sign $\pm$ is equal to $(-1)^{\sum ipi} = (-1)^{p_1+p_3}$, and 14 terms

$$\begin{array}{ll|c}
(2,0,1,0) & (0,1,0,2) & c_1a_1a_3^2b_0^2b_2 \\
(2,0,0,1) & (0,1,1,1) & c_2a_1a_2a_3b_0^2b_3 \\
(2,0,0,1) & (1,0,0,2) & c_3a_0a_3^2b_0^2b_3 \\
(0,2,0,1) & (1,1,0,1) & c_4a_0a_1a_3b_1^2b_3 \\
(1,0,2,0) & (1,0,1,1) & c_5a_0a_2a_3b_0b_2^2 \\
(1,0,0,2) & (1,1,1,0) & c_6a_0a_1a_2b_0b_3^2 \\
(1,0,0,2) & (2,0,0,1) & -c_3a_0^2a_3b_0b_3^2 \\
(0,1,0,2) & (2,0,1,0) & -c_1a_0^2a_2b_1b_3^2 \\
(1,1,1,0) & (1,0,0,2) & -c_6a_0a_3^2b_0b_1b_2 \\
(1,1,0,1) & (0,2,0,1) & -c_4a_1^2a_3b_0b_1b_3 \\
(1,1,0,1) & (1,0,1,1) & c_7a_0a_2a_3b_0b_1b_3 \\
(1,0,1,1) & (1,0,2,0) & -c_5a_0a_2^2b_0b_2b_3 \\
(1,0,1,1) & (1,1,0,1) & -c_7a_0a_1a_3b_0b_2b_3 \\
(0,1,1,1) & (2,0,0,1) & c_2a_0^2a_3b_1b_2b_3
\end{array}$$

where there are 7 unknown coefficients (due to symmetry).

References

[1] J. Canny, Generalized characteristic polynomials, *Journal of Symbolic Computation* **9** (1990), 241–250.

[2] Cox, Little, and O'Shea, *Ideals, Varieties, and Algorithms*, Undergraduate Texts in Mathematics, Springer-Verlag, 1992.

[3] W. Fulton, *Algebraic Curves*, Benjamin, Inc., 1969.

[4] I.M. Gelfand, M.M. Kapranov, and A.V. Zelevinsky, *Discriminants, Resultants,and Multidimensional Determinants*, Birkhäuser, Boston, 1994.

[5] Gleeson and Williams, *A Primer on Polynomial Resultants*, Naval Air Development Center Technical Report, 1991.

[6] J. Harris, *Algebraic Geometry: A First Course*, Graduate Texts in Mathematics **133**, Springer-Verlag, 1992.

[7] A.P. Morgan, *Solving Polynomial Systems Using Continuation for Engineering and Scientific Problems*, Prentice-Hall, Inc., 1987.

[8] B. Roth, Computation in kinematics, *Computational Kinematics* (J. Angeles *et al.*, eds.), Kluwer Academic Publishers, 1993.

[9] G. Salmon, *Lessons Introductory to the Modern Higher Algebra*, Chelsea Publishing Co., Bronx, New York, 5th edition.

[10] J.P. Serre, *A Course in Arithmetic*, Graduate Texts in Mathematics **7**, Springer-Verlag, 1971.

[11] B.L. van der Waerden, *Modern Algebra* **1** and **2**, Frederick Ungar Publishing Co., 1949 and 1950.