Polynomial Resultants

Com S 477/577

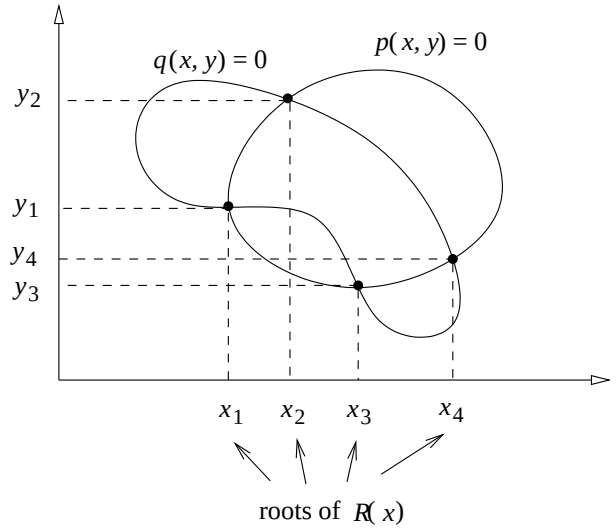
Sep 27, 2007

1 Introduction

A resultant of a set of polynomials is an expression involving the polynomial coefficients such that the vanishing of the expression is necessary and sufficient for the set of polynomials to have a common zero. A resultant is a generalization of the idea of a determinant, which is an expression involving the coefficients of a set of linear equations. There are several situations where the technique of polynomial resultants has been found very useful.

1.1 Isolating Simultaneous Zeros

Let $p(x, y)$ and $q(x, y)$ be bivariate polynomials in variables x and y. We would like to seek their simultaneous zeros. The equations $p(x, y) = 0$ and $q(x, y) = 0$ each defines a curve[1]. The simultaneous zeros thus correspond to the coordinates of the intersections of the two curves. In the example shown below, the two curves intersect at four points (x_i, y_i), $i = 1, 2, 3, 4$, which are the simultaneous zeros of $p(x, y)$ and $q(x, y)$.



The method of resultants will produce a single univariate polynomial $R(x)$ such that

$$R(x) = 0 \qquad \text{if and only if} \qquad p(x, y) = 0 \quad \text{and} \quad q(x, y) = 0$$

[1]Such a curve does not need to be connected, as in the case of a hyperbola $\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$.

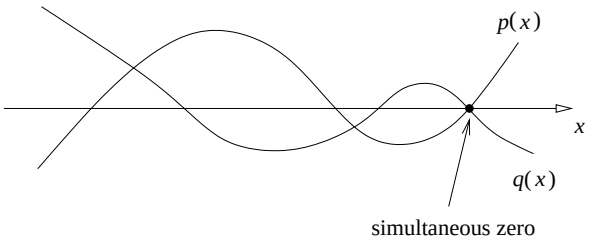
for some y. In the above example, the abscissas x_1, x_2, x_3, x_4 of the intersection points are all the zeros of $R(x)$. Generally, we first find the zeros of $R(x)$. And for each zero found, solve one of $p(x, y)$ and $q(x, y)$ in y to get a simultaneous root of the two polynomials.

1.2 Singular Simultaneous Zeros

The method of resultants can also tell us when an over-constrained algebraic system has a simultaneous zero. Consider the following system of equations:

$$\begin{aligned} p(x) &= 0, \\ q(x) &= 0. \end{aligned}$$

There are two equations in only one unknown. The simultaneous zero is where both curves $p(x)$ and $q(x)$ cross the x axis, as shown below.



Finding simultaneous zeros can be viewed as elimination of the parameter x. What we really get is a resultant R constructed over the coefficients of p and q that tells us whether or not these two polynomials have a simultaneous zero. If $R = 0$, then the answer is yes; otherwise, the answer is no. If the coefficients are symbols, then the equation $R = 0$ provides constraints on the coefficients to be satisfied in order for a simultaneous zero to exist.

1.3 Implicitizing Parametric Equations

Suppose we are presented with a parameterized curve in the plane

$$\alpha(t) = \Big(p(t), q(t)\Big),$$

where $p(t)$ and $q(t)$ are polynomials. Sometimes we might want an implicit equation

$$F(x, y) = 0$$

to represent the same curve, with F a polynomial in x and y.

Elimination theory will do the job for us if applied to the system of equations

$$\begin{aligned} p(t) - x &= 0; \\ q(t) - y &= 0. \end{aligned}$$

If we think of the above as two equations in one unknown t, then we are back in the "singular simultaneous zeros" scenario. Namely, we have two polynomial equations in t. And we think x and y as part of the coefficient set of these equations. The result will be a polynomial equation $F(x, y) = 0$ that provides constraints on x and y for a simultaneous zero in t to exist. In other words, it will give us the desired implicit equation.

2 Resultants

Recall that the linear system of equations

$$\begin{array}{ccccccccc} a_{11}x_1 & + & a_{12}x_2 & + & \cdots & + & a_{1n}x_n & = & 0 \\ a_{21}x_1 & + & a_{22}x_2 & + & \cdots & + & a_{2n}x_n & = & 0 \\ \vdots & & \vdots & & \ddots & & \vdots & & \vdots \\ a_{n1}x_1 & + & a_{n2}x_2 & + & \cdots & + & a_{nn}x_n & = & 0 \end{array}$$

or in short, $Ax = 0$, has a non-trivial solution if and only if the coefficient matrix A is singular, that is, if and only if the determinant $\det(A) = 0$. Furthermore, if we have a reduced system with $n-1$ equations and n unknowns:

$$\begin{array}{ccccccccc} a_{11}x_1 & + & a_{12}x_2 & + & \cdots & + & a_{1n}x_n & = & 0 \\ \vdots & & \vdots & & \ddots & & \vdots & & \vdots \\ a_{n-1,1}x_1 & + & a_{n-1,2}x_2 & + & \cdots & + & a_{n-1,n}x_n & = & 0 \end{array}$$

then the ratio $\frac{x_i}{x_j}$ of any solution is given by

$$\frac{x_i}{x_j} = (-1)^{i+j}\frac{\det(A_i)}{\det(A_j)},$$

where the matrix A_i is generated by removing the ith column from the $(n-1)\times n$ coefficient matrix, that is,

$$A_i = \begin{pmatrix} a_{11} & \cdots & a_{1,i-1} & a_{1,i+1} & \cdots & a_{1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{n-1,1} & \cdots & a_{n-1,i-1} & a_{n-1,i+1} & \cdots & a_{n-1,n} \end{pmatrix}.$$

Example 1. Consider the system of equations

$$\begin{array}{rcl} x+y+z & = & 0, \\ 2x+y & = & 0. \end{array}$$

Thus

$$A_1 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \qquad A_2 = \begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix}, \qquad \text{and} \qquad A_3 = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}.$$

Their determinants are

$$\det(A_1) = -1, \qquad \det(A_2) = -2, \qquad \text{and} \qquad \det(A_3) = -1.$$

The solutions of the system have the form $c(1,-2,1)$; they constitute a line. In fact, we could also obtain the solutions easily with some linear algebra by hand on the two equations.

But how do we generalize the approach to a system of polynomial equations of higher orders? Resultants and elimination theory are our answers.

2.1 Sylvester Resultants

To start small, we look at two univariate quadratics:

$$\begin{aligned} a_1x^2 + b_1x + c_1 &= 0, \quad (1) \\ a_2x^2 + b_2x + c_2 &= 0, \quad (2) \end{aligned}$$

where $a_1, a_2 \neq 0$. The above system has a simultaneous zero if (and only if) there is some x value such that

$$\begin{pmatrix} a_1 & b_1 & c_1 & 0 \\ 0 & a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 & 0 \\ 0 & a_2 & b_2 & c_2 \end{pmatrix} \begin{pmatrix} x^3 \\ x^2 \\ x \\ 1 \end{pmatrix} = 0. \quad (3)$$

Write this equation for short as $Q\boldsymbol{z} = 0$ where

$$\boldsymbol{z} = \begin{pmatrix} x^3 \\ x^2 \\ x \\ 1 \end{pmatrix}.$$

By analogy to the linear case, we can show that

Claim 1 *The equation $Q\boldsymbol{z} = 0$ if any only if $R = \det(Q) = 0$.*

Here $R = \det(Q)$ is called the *resultant* of the two equations (1) and (2).

More generally, suppose we are given two polynomials

$$\begin{aligned} f(x) &= a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0, \\ g(x) &= b_mx^m + b_{m-1}x^{m-1} + \cdots + b_0. \end{aligned}$$

To avoid triviality, we assume that the leading coefficients $a_n, b_m \neq 0$. It is known that $f(x)$ and $g(x)$ have a non-constant common factor $\phi(x)$ (and hence a non-trivial common zero) if and only if

$$h(x)f(x) = k(x)g(x) \quad (4)$$

for some polynomials $h(x)$ of degree at most $m-1$ and $k(x)$ of degree at most $n-1$.

In order to investigate equation (4) further, we let

$$\begin{aligned} h(x) &= c_{m-1}x^{m-1} + c_{m-2}x^{m-2} + \cdots + c_0, \\ k(x) &= d_{n-1}x^{n-1} + d_{n-2}x^{n-2} + \cdots + d_0. \end{aligned}$$

A comparison of the coefficients of $x^{n+m-1}, x^{n+m-2}, \ldots, x, 1$ on both sides of (4) yields

$$\begin{aligned} c_{m-1}a_n &= d_{n-1}b_m \\ c_{m-1}a_{n-1} + c_{m-2}a_n &= d_{n-1}b_{m-1} + d_{n-2}b_m \\ c_{m-1}a_{n-2} + c_{m-2}a_{n-1} + c_{m-3}a_n &= d_{n-1}b_{m-2} + d_{n-2}b_{m-1} + d_{n-3}b_m \\ &\vdots \quad \vdots \\ c_1a_0 + c_0a_1 &= d_1b_0 + d_0b_1 \\ c_0a_0 &= d_0b_0 \end{aligned}$$

Now regard the quantities c_i and $-d_j$ as unknowns. There are $n+m$ linear equations for the $n+m$ quantities c_i and $-d_j$. The coefficient matrix is A with transpose

$$A^T = \begin{pmatrix} a_n & a_{n-1} & \cdots & a_0 & & \\ & \ddots & & \vdots & & \\ & & a_n & a_{n-1} & \cdots & a_0 \\ b_m & b_{m-1} & \cdots & b_0 & & \\ & \ddots & & \vdots & & \\ & & b_m & b_{m-1} & \cdots & b_0 \end{pmatrix}.$$

This is a $(m+n) \times (m+n)$ matrix consisting of m rows of coefficients a_i followed by n rows of coefficients b_j. If the determinant $\det(A) \neq 0$, then the inverse A^{-1} exists and all c_is and d_js must be zero. Thus a necessary condition for f and g to share a non-constant common factor is $\det(A) = \det(A^T) = 0$.

The resultant $R = \det(A)$ is homogeneous of degree m in a_i and homogeneous of degree n in b_j. The "principal term" of the resultant is $a_n^m b_0^n$ (principal diagonal). The method of elimination was devised by Euler. But the form of the resultant is usually named after Sylvester.

Theorem 2 *If the resultant R vanishes, the polynomials f and g have a common non-constant factor (thus a common nontrivial zero), and conversely.*

3 Examples

In this section we look at six examples where resultants and elimination theory are applied.

Example 2.

$$\begin{aligned} p(x) &= x^2 - 6x + 2 \\ q(x) &= x^2 + x + 5 \end{aligned}$$

We obtain the resultant

$$R = \begin{vmatrix} 1 & -6 & 2 & 0 \\ 0 & 1 & -6 & 2 \\ 1 & 1 & 5 & 0 \\ 0 & 1 & 1 & 5 \end{vmatrix} = 233.$$

Since the resultant is not zero, we know that p and q do not have a common zero.[2]

Example 3.

$$\begin{aligned} p(x) &= x^2 - 4x - 5 \\ q(x) &= x^2 - 7x + 10 \end{aligned}$$

It is easy to find the common root $x = 5$ by hand. But let us illustrate the method of resultants here. Since

$$R = \begin{vmatrix} 1 & -4 & -5 & 0 \\ 0 & 1 & -4 & -5 \\ 1 & -7 & 10 & 0 \\ 0 & 1 & -7 & 10 \end{vmatrix} = 0,$$

[2]In fact, by solving them directly, p has zeros $3 \pm \sqrt{7}$ while q has zeros $-\frac{1}{2} \pm \frac{\sqrt{19}}{2} i$.

p and q have a common zero. To find it, consider the system

$$\begin{pmatrix} 1 & -4 & -5 & 0 \\ 0 & 1 & -4 & -5 \\ 1 & -7 & 10 & 0 \end{pmatrix} \begin{pmatrix} x^3 \\ x^2 \\ x \\ 1 \end{pmatrix} = 0.$$

Using our earlier linear algebra result,

$$\begin{aligned} x &= \frac{x^3}{x^2} \\ &= (-1)^{1+2} \frac{\begin{vmatrix} -4 & -5 & 0 \\ 1 & -4 & -5 \\ -7 & 10 & 0 \end{vmatrix}}{\begin{vmatrix} 1 & -5 & 0 \\ 0 & -4 & -5 \\ 1 & 10 & 0 \end{vmatrix}} \\ &= (-1) \cdot \frac{-375}{75} \\ &= 5. \end{aligned}$$

If some of the coefficients are unknown parameters, then we could use the method of resultants to provide a constraint on the unknown parameters, in order for a common zero to exist.

Example 4. Suppose there are two polynomials:

$$\begin{aligned} p(x) &= x^2 - 4x - 5, \\ q(x) &= x^2 - 7x + c. \end{aligned}$$

Then we can determine for what value of c the system have a common root. Essentially, we will eliminate x from the system and determine a constraint on c. The resultant of p and q is

$$\begin{vmatrix} 1 & -4 & -5 & 0 \\ 0 & 1 & -4 & -5 \\ 1 & -7 & c & 0 \\ 0 & 1 & -7 & c \end{vmatrix} = c^2 - 2c - 80.$$

So a common zero exists if and only if

$$c^2 - 2c - 80 = 0,$$

that is, if and only if $c = 10$ or $c = -8$. The case $c = 10$ was treated in Example 3, yielding a common zero $x = 5$. The case $c = -8$ results in the system

$$\begin{aligned} x^2 - 4x - 5 &= 0, \\ x^2 - 7x - 8 &= 0, \end{aligned}$$

which has a simultaneous root $x = -1$.

From the above example we see that a simple test merely to decide the existence of a common zero for an over-constrained system is actually quite powerful if some of the coefficients are left

symbolic. In the next example, we will apply the method of resultants to solve two simultaneous equations in two unknowns.

EXAMPLE 5. Suppose we would like to intersect a circle and an ellipse given by the equations

$$\begin{aligned} p(x,y) &= x^2+y^2-16 = 0, \\ q(x,y) &= 9x^2+25y^2-225 = 0. \end{aligned}$$

In order to apply the method of resultants, we will think of p and q as two univariate polynomials in y with coefficients including the symbol x. The resultant will then be a single polynomial in x, which vanishes if and only if the original system has a common zero. Next we solve for x and last for y.

Rewrite p and q as polynomials in variable y only:

$$r(y) = y^2 + 0\cdot y + (x^2-16), \tag{5}$$
$$s(y) = 25y^2 + 0\cdot y + (9x^2-225). \tag{6}$$

The resultant of the two univariate polynomials r and s is

$$\begin{vmatrix} 1 & 0 & x^2-16 & 0 \\ 0 & 1 & 0 & x^2-16 \\ 25 & 0 & 9x^2-225 & 0 \\ 0 & 25 & 0 & 9x^2-225 \end{vmatrix} = (175-16x^2)^2.$$

It equals zero when $16x^2 = 175$, i.e., $x = \pm\frac{5}{4}\sqrt{7}$. This is the sufficient and necessary condition for p and q to have a simultaneous zero.

In effect the resultant projects common roots of $p(x,y)$ and $q(x,y)$ onto the x-axis. Now plug the obtained values of x into equations (5) and (6):

$$\begin{aligned} r(y) &= y^2-(x^2-16) \\ &= y^2-\frac{81}{16}, \\ s(y) &= 25y^2+(9x^2-225) \\ &= 25\left(y^2-\frac{81}{16}\right). \end{aligned}$$

Hence r and s have common zeros, namely, $y = \pm\frac{9}{4}$. By now we have obtained the four intersection points between the circle and the ellipse:

$$\left(-\frac{5}{4}\sqrt{7},-\frac{9}{4}\right), \quad \left(\frac{5}{4}\sqrt{7},-\frac{9}{4}\right), \quad \left(-\frac{5}{4}\sqrt{7},\frac{9}{4}\right), \quad \text{and} \quad \left(\frac{5}{4}\sqrt{7},\frac{9}{4}\right).$$

Another application of resultants is in implicitization of parametric curves. In this case the technique is used to eliminate a curve parameter.

EXAMPLE 6. Consider the parametric curve given by

$$\begin{aligned} x(t) &= 5t^2+t+3, \\ y(t) &= 5t^2-t-1. \end{aligned}$$

What is the implicit equation $F(x,y) = 0$ that describes the curve?

Now we look at the system as two equations in only one unknown t, namely,

$$\begin{aligned} 5t^2 + t + (3 - x) &= 0, \\ 5t^2 - t + (-1 - y) &= 0. \end{aligned}$$

Here x and y are seen as symbolic coefficients.

We know that the above system in t has a common zero whenever (x, y) is a point on the curve. In other words, (x, y) is a point if and only if the resultant of the system

$$\begin{vmatrix} 5 & 1 & 3-x & 0 \\ 0 & 5 & 1 & 3-x \\ 5 & -1 & -1-y & 0 \\ 0 & 5 & -1 & -1-y \end{vmatrix} = 5(84 + 38y - 42x + 5x^2 + 5y^2 - 10xy) = 0.$$

Our desired implicit equation is thus in the form

$$5x^2 + 5y^2 - 10xy - 42x + 38y + 84 = 0,$$

which describes a parabola.[3]

Resultants give us a way of converting rational parameterized surfaces into implicit equations. Interestingly, it is not always possible to go the other way, that is, to take an algebraic surface $F(x, y, z) = 0$ and construct a parameterization of that surface by rational functions. We will get back to this point when studying curves in the second half of the course.

EXAMPLE 7. Now suppose we are given a point $(7, 5)$ on the parabola curve in the previous example. Is it possible to determine the parameter t value corresponding to that point? The answer is yes by the use of the reduced system.

To find t, we plug (x, y) into the partial system

$$\begin{pmatrix} 5 & 1 & 3-x & 0 \\ 0 & 5 & 1 & 3-x \\ 5 & -1 & -1-y & 0 \end{pmatrix} \begin{pmatrix} t^3 \\ t^2 \\ t \\ 1 \end{pmatrix} = 0.$$

Then we have

$$\begin{aligned} t &= \frac{t^3}{t^2} \\ &= (-1)^{1+2} \frac{\begin{vmatrix} 1 & 3-x & 0 \\ 5 & 1 & 3-x \\ -1 & -1-y & 0 \end{vmatrix}}{\begin{vmatrix} 5 & 3-x & 0 \\ 0 & 1 & 3-x \\ 5 & -1-y & 0 \end{vmatrix}} \qquad x = 7 \text{ and } y = 5 \\ &= -\frac{\begin{vmatrix} 1 & -4 & 0 \\ 5 & 1 & -4 \\ -1 & -6 & 0 \end{vmatrix}}{\begin{vmatrix} 5 & -4 & 0 \\ 0 & 1 & -4 \\ 5 & -6 & 0 \end{vmatrix}} \end{aligned}$$

[3]Indeed it turns out that all two-variable quadratic parameterizations yield parabola.

$$= \quad -\frac{-40}{-40}.$$

So $t = -1$. To verify it, we have

$$\begin{aligned} x(-1) &= 5 - 1 + 3 &= 7, \\ y(-1) &= 5 + 1 - 1 &= 5. \end{aligned}$$

References

[1] M. Erdmann. Lecture notes for *16-811 Mathematical Fundamentals for Robotics*. The Robotics Institute, Carnegie Mellon University, 1998.

[2] B. L. van der Waerden. *Algebra*, vol 1. Springer-Verlag New York, Inc., 1991