Resultant of two polynomials

Euclid's algorithm for two polynomials A and B in one variable is closely connected to the Sylvester matrix. If

$A = a_m x^m + \dots + a_1 x + a_0$ and $B = b_m x^n + \dots + b_1 x + b_0$ $(b_m \neq 0)$

are two polynomials in $R[x]$, Sylvester matrix is the $(n+m) \times (n+m)$ matrix

$$Syl(A,B) = \begin{pmatrix} a_m & \cdots & a_1 & a_0 & & \\ & \ddots & & \ddots & \ddots & \\ & & a_m & \cdots & a_1 & a_0 \\ b_n & \cdots & b_1 & b_0 & & \\ & \ddots & & \ddots & \ddots & \\ & & b_n & \cdots & b_1 & b_0 \end{pmatrix} \begin{matrix} \} n \\ \\ \\ \} m \\ \\ \\ \end{matrix}$$

where the first n rows are the coefficients of A and the next m rows are the coefficients of B. The transpose of this matrix represents the linear map

$$\varphi_{A,B} : (U,V) \longmapsto AU + BV$$

where we consider the pairs (U,V) s.t. $\deg U < \deg B$ and $\deg V < \deg A$, using the basis $((x^{n-1},0),(x^{n-2},0),\dots,(1,0),(0,x^{m-1}),(0,x^{m-2}),\dots,(0,1))$ at the beginning and the basis $(x^{m+n-1}, x^{m+n-2}, \dots, x, 1)$ at the end.

output polynomial basis

input polynomial

Hence linear combinations of the matrix rows give the coefficients of the polynomials which can be obtained as image. When $\mathbb{K}$ is a field, the $\gcd(A,B)$ can be obtained as the invertible element with least degree.

→ The gcd is the polynomial with the smallest degree that can be represented as linear combination of the rows of $Syl(A,B)$

→ The gcd can be read off from the row echelon form of the Sylvester matrix.

The $\dim(Syl(A,B)) = \dim \operatorname{Im}(\varphi_{A,B}) = m+n-\deg(\gcd(A,B))$

By the rank-nullity Theorem, $\deg(\gcd(A,B)) = \dim(\ker(\varphi_{A,B}))$

= # zero rows in the row echelon form of $Syl(A,B)$

Proposition: Let $A,B \in \mathbb{K}[x]$, where $\mathbb{K}$ is a field. The row-reduced echelon form of $Syl(A,B)$ contains the $\gcd(A,B)$ in its last non-zero row. Moreover, the number of zero rows of the row-reduced echelon form of $Syl(A,B)$ is the degree of $\gcd(A,B)$.

Example: $A = x^4 - x^3 - 7x^2 + 2x + 3$

$B = x^3 - 4x^2 + 2x + 3$

$$Syl(A,B) = \begin{pmatrix} 1 & -1 & -7 & 2 & 3 & 0 & 0 \\ 0 & 1 & -1 & -7 & 2 & 3 & 0 \\ 0 & 0 & 1 & -1 & -7 & 2 & 3 \\ 1 & -4 & 2 & 3 & 0 & 0 & 0 \\ 0 & 1 & -4 & 2 & 3 & 0 & 0 \\ 0 & 0 & 1 & -4 & 2 & 3 & 0 \\ 0 & 0 & 0 & 1 & -4 & 2 & 3 \end{pmatrix}$$

Row-reduced echelon form:

$$\begin{pmatrix} 1 & -1 & -7 & 2 & 3 & 0 & 0 \\ 0 & 1 & -1 & -7 & 2 & 3 & 0 \\ 0 & 0 & 1 & -\frac{1}{2} & 7 & 2 & 3 \\ 0 & 0 & 0 & -14 & 45 & -3 & -18 \\ 0 & 0 & 0 & 0 & -\frac{5}{1} & \frac{12}{1} & \frac{9}{1} \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{10} & -\frac{3}{10} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \Rightarrow \gcd(A,B) = x - 3$$

Definition: The resultant of A and B is the determinant of the matrix $Syl(A,B)$. We denote it by $Res(A,B)$ or $Res_x(A,B)$ if we want to insiste on the variable x.

Resultants are tools for eliminating variables from polynomial systems. For multivariate polynomials, the resultant helps in checking whether they share a common root.

Even if we work over rings, the properties of the determinant still holds

Proposition: Let $A, B \in \mathbb{K}[x]$. A, B are coprime $\iff Res(A,B) \neq 0$.

Proof: $Det(Syl(A,B)) \neq 0 \iff rk(Syl(A,B)) = n+m \iff deg(gcd(A,B)) = 0$

Example The discriminant of a polynomial $A = a_m x^m + \dots + a_1 x + a_0$ of degree m with coefficients in a field is the polynomial defined by

$$Res(A, A') = (-1)^{\frac{m(m-1)}{2}} a_m \, disc(A)$$

This is zero if A, A' have a root in common in the algebraic closure of $\mathbb{K}$. In characteristic zero, A has multiple root.

Example: Compute the discriminant of ax^2+bx+c by taking the determinant of Sylvester matrix.

$A = ax^2+bx+c$
$B = 2ax+b$

$$Syl(A,B) = \begin{pmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{pmatrix}$$

Gaussian elimination:

$$\begin{pmatrix} a & b & c \\ 0 & 2a & b \\ 2a & b & 0 \end{pmatrix}$$

$$\begin{pmatrix} a & b & c \\ 0 & 2a & b \\ 0 & b & 2c \end{pmatrix} \rightarrow \begin{pmatrix} a & b & c \\ 0 & 2a & b \\ 0 & 0 & \frac{b^2}{2a} - 2c \end{pmatrix}$$

$$Det(Syl(A,B)) = 2a^2\left(\frac{b^2-4ac}{2a}\right)$$

In particular, $Dis(A) = \frac{Res(A,B)}{a} = b^2-4ac$

Applications of the resultant

Resolution of polynomial systems. This is done by eliminating variables and geometrically this corresponds to finding projections. We see now how to use the resultant for solving systems of 2 equations in two unknowns. This is the basis for more general techniques.

Take two curves: $A: (x^2+y^2)^3 - 4x^2y^2 = 0$

$B: x^2(1+y) - (1-y)^3 = 0$

These polynomials are irreducible and $gcd(A,B) = 1$, so it does not provid any information on their common roots

BUT the resultants wrt x and y on the other hand will provid info.

$\text{Res}_x(A,B) = \det \text{Syl}(A,B)$

$A = x^6 + 3x^4y^2 + 3x^2y^4 + y^6 - 4x^2y^2 = 0$

$x^6 + 3x^4y^2 + (3y^4 - 4y^2)x^2 + y^6$

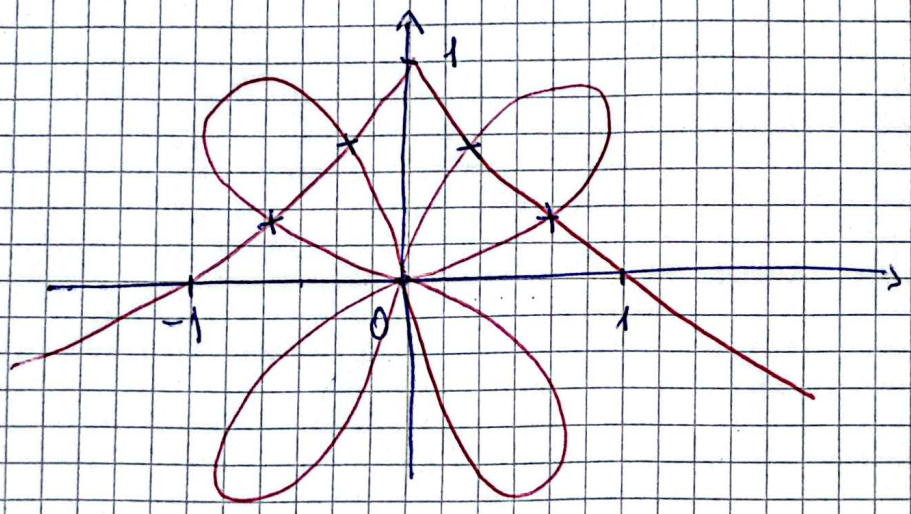
$B = x^2 + x^2y - 1 + 3y - 3y^2 + y^3$

$= x^2(1+y) - (1-y)^3$

$$\text{Res}_x(A,B) = \det \begin{pmatrix} 1 & 0 & +3 & 0 & (3y^4-4y^2) & 0 & y^6 & 0 \\ 0 & 1 & 0 & 3 & 0 & 3y^4-4y^2 & 0 & y^6 \\ 1+y & -(1-y) & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1+y & -(1-y) & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1+y & -(1-y) & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1+y & -(1-y) & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1+y & -(1-y) & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1+y & -(1-y) & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1+y & -(1-y) \end{pmatrix} =$$

$$= (4y^7 + 60y^6 - 152y^5 + 164y^4 - 95y^3 + 35y^2 - 9y + 1)^2$$

$\text{Res}_y(A,B) = 16x^{14} + 6032x^{12} - 1624x^{10} + 4192x^8 - 815x^6 - 301x^4 - 9x^2 + 1$



→ There are 14 points of intersection, but on the figure we see only 4. This means that the other 10 have complex coordinate

Applications of the resultant

Recall that the resultant of two univariate polynomials is the determinant of the sylvester matrix :

Let $A = a_m x^m + \dots + a_1 x + a_0$ and $B = b_n x^n + \dots + b_1 x + b_0$ then

$$Syl(A,B) = \begin{matrix} n \\ \{ \\ \\ \\ m \\ \{ \\ \\ \\ \end{matrix} \begin{pmatrix} a_m & a_{m-1} & \cdots & a_1 & a_0 & & \\ & \ddots & & & \ddots & \ddots & \\ & & a_m & a_{m-1} & \cdots & a_1 & a_0 \\ b_n & b_{n-1} & \cdots & b_1 & b_0 & & \\ & \ddots & & & \ddots & \ddots & \\ & & b_n & \cdots & & b_1 & b_0 \end{pmatrix}$$

Theorem: $A, B \in \mathbb{K}[x]$ have a common zero if and only if $Res(A,B) = \det Syl(A,B) = 0$.

Or equivalently, A, B coprime $\iff Res(A,B) \neq 0$

Proof: $Det(Syl(A,B)) \neq 0 \iff rk(Syl(A,B)) = m+n$

$\iff \deg(\gcd(A,B)) = 0$. ∎

If we have bivariate polynomials then we can use the resultant to "eliminate" one of the two variables.

Some properties of the resultant.

Thm (Multiplicativity of the resultant) For every polynomials $A, B, C \in \mathbb{K}[x]$, we have $Res(AB, C) = Res(A,C) \cdot Res(B,C)$.

Proof: Use Poisson formula to verify.

If $m > 0$, $n = 0$, we get $B = b_0$ on the diagonal and $Syl(A,B) = n \times n$ diag. $\Rightarrow Res(A,B) = b_0^m$

Property:
- $Res(A,B) \in R$
- $Res(A,B) = (-1)^{mn} Res(B,A)$
- $Res(\bar{a}A, B) = \bar{a}^m Res(A,B)$, $Res(A, \bar{b}B) = \bar{b}^n Res(A,B)$ $\forall \bar{a}, \bar{b} \in R$

Proof: From multilinearity of determinant.

Theorem (Poisson formula) If $A = a(x-\alpha_1)\cdots(x-\alpha_m)$ and $B = b(x-\beta_1)\cdots(x-\beta_n)$, Then
In a field $\alpha_i, \beta_j \in \mathbb{K}$

$$\mathrm{Res}(A,B) = a^n b^m \prod_{i,j} (\alpha_i - \beta_j)$$

$$= (-1)^{mn} b^m \prod_{1\le j\le m} A(\beta_j)$$

$$= (+a^n) \prod_{1\le i\le m} B(\alpha_i) = (-1)^{mn} \mathrm{Res}(B,A)$$

Proof: The factor $a^n b^m$ derives directly from the multilinearity of the determinant. Hence we restrict ourselves to consider $a=b=1$. Consider α_i, β_j as indeterminates and work over the ring $\mathbb{Z}[\alpha_1,\dots,\alpha_m,\beta_1,\dots,\beta_n]$. If the resultant satisfy the identity in this ring, Then it is True by specializing for arbitrary values of α_i, β_j.
Consider The field $\mathbb{K} = \mathbb{Q}(\alpha_1,\dots,\alpha_m,\beta_1,\dots,\beta_n)$ and apply the fact that the two polynomials are coprime if the Resultant is nonzero. If we substitute the variable β_j with α_i in the resultant, we will get 0, hence $\alpha_i - \beta_j$ divides the resultant.
Moreover, the degree in α_i of each of The first n ~~rows~~ rows of $\mathrm{Syl}(A,B)$ is 1 and this degree is 0 for the other m rows
$\Rightarrow$ the resultant has degree $\le m$ in each α_i.
Similarly, in each β_j has degree $\le m$. Hence the resultant is equal to the product of $\alpha_i - \beta_j$ up to a constant factor, independent of α_i and β_j.
By choosing $\alpha_1 = \cdots = \alpha_m = 0$, i.e. $A = x^m$, the Sylvester matrix is Triangular and its determinant is $B(0)^m$, which yields the factor 1 and concludes the proof.

Proposition: There exist U, V in $\mathbb{K}[x]$ with $\deg U < \deg B$ and $\deg V < \deg A$ s.t. $\mathrm{Res}(A,B) = UA + VB$.

Proof: Add to the last columns of the Sylvester matrix the product of the previous columns by suitable powers of x in order to have as last columns the polynomials

$$x^{\deg B - 1}A, \dots, xA, A, x^{\deg A - 1}B, \dots, xB, B$$

without changing the determinant. Expanding the determinant with respect to the last column then allows to conclude.

(*) **Remark**: $f = ax^2 + bx + c$ and $dx + e = g$

$\mathrm{Res}(f,g) = ae^2 + cd^2 - bde$

For $a = 0$, $\mathrm{Res}(f,g) = cd^2 - bde = d(cd - be)$

But $\mathrm{Res}(bx + c, dx + e) = be - cd$, which shows that the resultant and its specialization do not always commute.

A useful result that illustrates when this happens is given below without proof.

Proposition: Let R_1 and R_2 be two commutative rings with identities 1_{R_1} and 1_{R_2}. Let φ be a morphism from $\varphi : R_1 \longrightarrow R_2$, which naturally extends $1_{R_1} \longrightarrow 1_{R_2}$ to polynomials in $R_1[x]$

Let $A, B \in R_1[x]$. If A is monic, then $\varphi(\mathrm{Res}(A,B)) = \mathrm{Res}(\varphi(A), \varphi(B))$.

(*) **Corollary**: $\mathrm{Res}(A,B) \in (A,B) \cap R$.

Proposition: Let $A = a_m y^m + \dots + a_0$, $B = b_n y^n + \dots + b_0$ $\Big\} \in \mathbb{K}[x][y]$

where a_i, b_j are in $\mathbb{K}[x]$ with $a_m \neq 0$, $b_n \neq 0$ and $\mathbb{K}$ is algebraically closed.

Then the roots of the polynomial $\mathrm{Res}_y(A,B) \in \mathbb{K}[x]$ are, on the one hand, the x-coordinates of the solutions to the system $A = B = 0$ and, on the other hand, the common roots of the leading terms a_m and b_n.

Proof: First, the common roots of a_m and b_n are roots of the resultant, since the first column of $\mathrm{Syl}(A,B)$ is zero at such a root.

By evaluating this identity at (α, β) s.t. $A(\alpha,\beta) = B(\alpha,\beta) = 0$ we see that such an α is a root of $\mathrm{Res}_y(A,B)$

Conversely, if α is a root of $\mathrm{Res}(A,B)$ but not symultaneously cancels a_m and b_n, we show that $\exists\, \bar{y} \in \mathbb{K}$ s.t. $(\alpha, \bar{y})$ is a solution of $A = B = 0$.

Assume $a_m(\alpha) \neq 0$. Then specialize to the resultant of A and B at $x = \alpha$, obtaining $\mathrm{Res}_y(A(\alpha,y), B(\alpha,y)) = 0$.

Then observe that $A(\alpha, y)$ and $B(\alpha, y)$ have gcd of degree at least 1. Since $\mathbb{K}$ is algebraically closed, $\exists\, \bar{y} \in \mathbb{K}$, root of such gcd, such that $A(\alpha, \bar{y}) = B(\alpha, \bar{y}) = 0$. ∎

→ Resultant is used to find the common roots of two univariate polynomials and it is used to find the common points of two plane curves (zero locus of bivariate polynomials)

Implicitation: Another geometric application of the resultant is implicitation, i.e. finding the polynomial that defines a curve in the plane given in parametric form.

For example the unit circle is $\begin{cases} x = \cos t \\ y = \sin t \end{cases}$ and the curve is

$x^2 + y^2 = 1$.

Let $\mathcal{C}$ be a curve defined by

$$\begin{cases} x = A(t) \\ y = B(t) \end{cases} \quad \text{where } A, B \in \mathbb{K}(T)$$

We want to compute a polynomial in the variables x and y, whose zero locus gives the curve. For this, it is sufficient to take the resultant of the numerators of $x - A(t)$ and $y - B(t)$ with respect to t.

Example: $x = \frac{4t(1-t^2)^2}{(1+t^2)^3}$, $y = \frac{8t^2(1-t^2)}{(1+t^2)^3}$

to obtain the curve we compute

$$\mathrm{Res}_t\left((1+t^2)^3 x - 4t(1-t^2)^2,\ (1+t^2)^3 y - 8t^2(1-t^2)\right)$$

for finding the polynomial

$$(x^2+y^2)^3 - 4x^2y^2.$$

We can use the Euclidean algorithm for computing the resultant.

Let $A, B \in \mathbb{K}[x]$, $m = \deg A$, $n = \deg B$.

Let $A = QB + R$ be the Euclidean division in $\mathbb{K}[x]$.

If $r = \deg R$ and b_n is the leading coefficient of B, show that

$\mathrm{Res}(A,B) = (-1)^{m \cdot n} b_n^{m-r} \mathrm{Res}(B,R)$. → in TD

We can modify the extended Euclidean algorithm to obtain the Resultant in $O(nm)$.

Remark: When the coefficients of A and B are integers, rationals or polynomials, the computation of the resultant using the Euclidean algorithm requires a number of gcd computations of coefficients which is of the same order and makes the algorithm inefficient. In order to solve this problem, the subresultant pseudo-remainder sequences were introduced to avoid fractions and gcd computations of the coefficients.

Definition If A, B are polynomials in $R[x]$ and if b is the leading coefficient of B, the pseudo-remainder $\bar{R}$ of A and B is defined by

$$b^{\deg A - \deg B + 1} A = \bar{Q}B + \bar{R},$$

where $\bar{Q}, \bar{R} \in R[x]$ with $\deg \bar{R} < \deg \bar{Q}$.

Remark: Replacing the remainder computation of the Euclidean division with pseudoremainder calculations avoids introducing denominators.

Example Let $A = 115x^5 + 7x^4 + 117x^3 + 30x^2 + 87x + 44$

$B = 91x^4 + 155x^3 + 3x^2 + 143x + 115$

Apply the Euclidean algorithm and obtain the following remainders:

$$\frac{3601622}{8281}x^3 - \frac{1196501}{8281}x^2 + \frac{151912}{637}x + \frac{2340984}{8281},$$

$$\frac{1898860276268 41}{129716810308 84}x^2 - \frac{57448278681703}{3242920257721}x - \frac{17501090665331}{3242920257721}$$

⋮

On the same example, compute the pseudo-remainders.

$$3601622x^3 - 1196501x^2 + 1974856x + 2340984$$

$$1898860276268 41x^2 - 22979311472681 2x + - 7000436266 1324$$

⋮

From the example it is clear that the coefficients are quite huge!

Def: A pseudo-remainder sequence is the sequence of pseudo-remainders r_i obtained by replacing the instruction

$r_{i+1} := \text{rem}(r_{i-1}, r_i)$ with

$$r_{i+1} = \frac{\text{prem}(r_{i-1}, r_i)}{\alpha}$$

where α is an element that divides exactly the coefficient of the numerator. Different choices of α give different pseudo-remainders sequences.

If we divide by $\alpha = \text{gcd}(\text{coefficients})$ we talk about primitive pseudo-remainders.

We use the following modified Euclidean division algorithm to find this sequence of pseudo-remainders. We call them sub-resultant

Input: $A, B \in R[x]$ with $\deg B < \deg A$

Output: The last non-zero subresultant

$f = g = s = 1$

while $\deg B > 0$ do

$d = \deg A - \deg B$

Compute the pseudo-remainder $R = \text{prem}(A, B)$

If $\deg(A)$ and $\deg(B)$ are odd, then

$s = -s$

$A := B$

$B = \text{Quo}(R, fg^d)$

$f = \text{lc}(A)$

$g = \text{Quo}(f^d, g^{d-1})$

end while;

$d = \deg A$

Return $\text{Quo}(sB^d, g^{d-1})$

Example: Always on the same polynomials, the computation of the subresultant gives

$$3601622x^3 - 1196501x^2 + 1974856x + 2340984$$
$$22930325761x^2 - 27749440252x - 84536122204$$
$$288979986761465x + 1421430027077719$$

As the Resultant, also the subresultant are related to the Sylvest matrix and the Euclidean division algorithm.

By applying Cramer's formula on submatrices of the Sylvester matrix, we get the following result.

Proposition: All the divisions performed during the subresultant algorithm are exact.

The proof is difficult and technical so we omit it.

Input: $A, B \in R[x]$ with $\deg B < \deg A$

Output: Last non-zero resultant

$r_0 = A$

$r_1 = B$

while $r_i \neq 0$ do

$d_i = \deg(r_{i-1}) - \deg(r_i)$

$\gamma_i = lc(r_i)$

if $i = 1$ then

$\sigma_i = (-1)^{d_1+1}$

$\psi_1 = -1$

else

$\psi_i = (-\gamma_{i-1})^{d_{i-1}} / \psi_{i-1}^{d_{i-1}-1}$

$\sigma_i = -\gamma_{i-1} \psi_i^{d_i}$

end if

$r_{i+1} = \text{rem}(\gamma_i^{d_i+1} r_{i-1}, r_i) / \sigma_i$