EE464 Resultants

companion matrix

write $p = x^n + p_{n-1}x^{n-1} + \cdots + p_1 x + p_0$ in terms of its roots $x_1, \ldots, x_n$

$$p(x) = \prod_{k=1}^{n} (x - x_k)$$

define the $n \times n$ companion matrix

$$C_p = \begin{bmatrix} 0 & 0 & \ldots & 0 & -p_0 \\ 1 & 0 & \ldots & 0 & -p_1 \\ 0 & 1 & \ldots & 0 & -p_2 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \ldots & 1 & -p_{n-1} \end{bmatrix}$$

the characteristic polynomial of C_p is p

$$\det(xI - C_p) = p$$

eigenvectors of the companion matrix

define the Vandermonde matrix

$$V = \begin{bmatrix} 1 & x_1 & \dots & x_1^{n-1} \\ 1 & x_2 & \dots & x_2^{n-1} \\ \vdots & & \vdots & \\ 1 & x_n & \dots & x_n^{n-1} \end{bmatrix}$$

- $VC_p = \mathbf{diag}(x_1, \dots, x_n)V$
- V is nonsingular iff the x_i are distinct
- columns of V^{-1} are coefficients of *Lagrange polynomials* $L_j(x_i) = \delta_{ij}$ because $\begin{bmatrix} 1 & x_1 & \dots & x_1^{n-1} \end{bmatrix} V^{-1} = e_1^T V V^{-1} = e_1^T$

example

- $p = (x-1)(x-2)(x-5)$
- $C_p = \begin{bmatrix} 0 & 0 & 10 \\ 1 & 0 & -17 \\ 0 & 1 & 7 \end{bmatrix}$
- $V = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 5 & 25 \end{bmatrix} \qquad V^{-1} = \frac{1}{12} \begin{bmatrix} 30 & -20 & 2 \\ -21 & 24 & -3 \\ 3 & -4 & 1 \end{bmatrix}$
- $L_1(x) = (30 - 21x + 3x^2)/12 = (x-2)(x-5)/4$

trace of the companion matrix

for any $A \in \mathbb{C}^{n\times n}$ we have

$$\mathbf{trace}\, A = \sum_{i=1}^{n} \lambda_i(A) \qquad \lambda_i(A^k) = \lambda_i(A)^k$$

hence trace of powers of companion matrix gives sum of root powers

$$\mathbf{trace}\, C_p^k = \sum_{i=1}^{n} x_i^k$$

symmetric functions of roots

if $q = q_0 + q_1 x + \ldots q_m x^m$ then

$$\sum_{i=1}^{n} q(x_i) = \mathbf{trace}\, q(C_p)$$

because

$$\sum_{i=1}^{n} q(x_i) = \sum_{i=1}^{n} \sum_{j=0}^{m} q_j x_i^j = \sum_{j=0}^{m} q_j\, \mathbf{trace}\, C_p^j = \mathbf{trace} \sum_{j=0}^{m} q_j C_p^j = \mathbf{trace}\, q(C_P)$$

Hermite form

given polynomials p and q, the Hermite form is the symmetric matrix

$$H_q(p) = V^T \,\mathbf{diag}(q(x_1), \ldots, q(x_n))V$$

- with $q(x) = 1$, we have

$$H_1(p) = V^T V = \begin{bmatrix} s_0 & s_1 & \cdots & s_{n-1} \\ s_1 & s_2 & \cdots & s_n \\ \vdots & & & \vdots \\ s_{n-1} & s_n & \cdots & s_{2n-2} \end{bmatrix} \qquad s_k = \sum_{j=1}^{n} x_j^k$$

- can compute using $s_k = \mathbf{trace}\, C_p^k$
- signature of M is the number of positive eigenvalues minus the number of negative eigenvalues
- theorem: signature of $H_1(p) =$ the number of real roots of p.

  $\mathbf{rank}\, H_1(p) =$ the number of distinct complex roots of p

Hermite form

- $p = x^2 + 2x^2 + 3x + 4$
- $H_1(p) = \begin{bmatrix} 3 & -2 & -2 \\ -2 & -2 & -2 \\ -2 & -2 & 18 \end{bmatrix}$
- $H_1(p)$ has one negative and two positive eigenvalues
- hence p has three simple roots, one of them is real

scalar polynomials

when do two polynomials $f, g \in \mathbb{C}[x]$ have a common root?

$$\mathbf{gcd}\{f, g\} = 1 \qquad \Longleftrightarrow \qquad \text{there exist } a, b \in \mathbb{C}[x] \text{ such that } af + bg = 1$$

- theorem: can always choose $\deg a < \deg g$ and $\deg b < \deg f$

linear equations

suppose $\deg f = l$, $\deg g = m$, and the above degree bounds

then the linear equation $af + bg = 1$ is

$$
l+m \left\{ \begin{array}{c} \begin{bmatrix} f_0 & & & & g_0 & & \\ f_1 & \ddots & & & g_1 & \ddots & \\ \vdots & \ddots & \ddots & & \vdots & \ddots & g_0 \\ f_l & & \ddots & f_0 & \vdots & & g_1 \\ & \ddots & & f_1 & g_m & & \vdots \\ & & \ddots & \vdots & & \ddots & \vdots \\ & & & f_l & & & g_m \end{bmatrix} \\ \underbrace{\hspace{8em}}_{m}\underbrace{\hspace{7em}}_{l} \end{array} \right.
\begin{bmatrix} a_0 \\ \vdots \\ \vdots \\ a_{m-1} \\ b_0 \\ \vdots \\ b_{l-1} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ \\ \vdots \\ 0 \end{bmatrix}
$$

this matrix is called the *Sylvester matrix* of f and g, written $\mathbf{syl}(f, g, x)$

its determinant is called the *resultant* of f and g, written $\mathbf{res}(f, g, x)$

example

suppose

$$f = 2x^2 + 3x + 1 \qquad g = 7x^2 + x + 3$$

is $1 \in \mathbf{ideal}\{f, g\}$, or equivalently, does $\mathbf{gcd}\{f, g\} = 1$?

the resolvent is

$$\mathbf{res}(f, g, x) = \det \begin{bmatrix} 1 & 0 & 3 & 0 \\ 3 & 1 & 1 & 3 \\ 2 & 3 & 7 & 1 \\ 0 & 2 & 0 & 7 \end{bmatrix} = 153$$

since this is nonzero, we have $\mathbf{gcd}\{f, g\} = 1$

multivariable polynomials

we can compute the resultant for *multivariable* polynomials, with respect to a *single* variable, e.g.,

$$f = xy - 1 \qquad g = x^2 + y^2 - 4$$

to compute $\mathbf{res}(f, g, x)$, view f, g as polynomials in x with coeffs. in $\mathbb{K}[y]$

$$\begin{aligned}\mathbf{res}(f, g, x) &= \det \begin{bmatrix} -1 & 0 & -4 + y^2 \\ y & -1 & 0 \\ 0 & y & 1 \end{bmatrix} \\ &= y^4 - 4y^2 + 1\end{aligned}$$

$\mathbf{res}(f, g, x)$ *eliminates* x leaving a polynomial in y

example

with $f = xy - 1$ and $g = x^2 + y^2 - 4$ we have $af + bg = 1$ of appropriate degrees is equivalent to

$$\begin{bmatrix} -1 & 0 & -4+y^2 \\ y & -1 & 0 \\ 0 & y & 1 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ b_0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

using the explicit formula for the matrix inverse gives

$$\begin{bmatrix} a_0 \\ a_1 \\ b_0 \end{bmatrix} = \frac{1}{\mathbf{res}(f,g,x)} \begin{bmatrix} -1 & -4\,y+y^3 & -4+y^2 \\ -y & -1 & -4\,y+y^3 \\ y^2 & y & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

hence

$$a = \frac{-xy-1}{\mathbf{res}(f,g,x)} \qquad b = \frac{y^2}{\mathbf{res}(f,g,x)}$$

example continued

so we have $f = xy - 1$ and $g = x^2 + y^2 - 4$ and

$$af + bg = 1$$

where

$$a = \frac{-xy - 1}{y^4 - 4y^2 + 1} \qquad b = \frac{y^2}{y^4 - 4y^2 + 1}$$

multiplying by $\mathbf{res}(f, g, x) = y^4 - 4y^2 + 1$ gives

$$\hat{a} f + \hat{b} g = \mathbf{res}(f, g, x)$$

where $\hat{a} = -xy - 1$ and $\hat{b} = y^2$

elimination and resultants

we have

$$\boxed{\mathbf{res}(f, g, x) \in \mathbf{ideal}\{f, g\}}$$

because the explicit formula for the matrix inverse gives

$$\mathbf{syl}(f, g, x_1)^{-1} = \frac{1}{\mathbf{res}(f, g, x_1)} \mathbf{adjoint}\big(\mathbf{syl}(f, g, x_1)\big)^T$$

and since the entries of $\mathbf{adjoint}(A)$ are polynomials in the entries of A, the polynomials $\hat{a} = a\,\mathbf{res}(f, g, x)$ and $\hat{b} = b\,\mathbf{res}(f, g, x)$ satisfy

$$\hat{a}f + \hat{b}g = \mathbf{res}(f, g, x)$$

elimination and resultants

therefore the resultant is a member of the first elimination ideal

$$f, g \in \mathbb{K}[x_1, \ldots, x_n] \qquad \Longrightarrow \qquad \mathbf{res}(f, g, x_1) \in I_1$$

where $I_1 = \mathbf{ideal}\{f, g\} \cap \mathbb{K}[x_2, \ldots, x_n]$

- implicitization of paramaterized curves
- solution of two polynomial equations in two variables

another view of resultants

if $p(x_0) = q(x_0) = 0$ then

$$\begin{bmatrix} p_n & p_{n-1} & \cdots & p_1 & p_0 & & & \\ & p_n & & & \ddots & & & \\ & & \ddots & & & & & \\ & & & & & p_1 & p_0 & \\ & & & & & p_2 & p_1 & p_0 \\ q_m & q_{m-1} & \cdots & q_0 & & & & \\ & q_m & & & \ddots & & & \\ & & \ddots & & & & & \\ & & & & & q_1 & q_0 & \\ & & & & & q_2 & q_1 & q_0 \end{bmatrix} \begin{bmatrix} x_0^{n+m-1} \\ x_0^{n+m-2} \\ \vdots \\ \\ \\ x_0 \\ 1 \end{bmatrix} = \begin{bmatrix} p(x_0)x_0^{m-1} \\ p(x_0)x_0^{m-2} \\ \vdots \\ p(x_0)x_0 \\ p(x_0) \\ q(x_0)x_0^{n-1} \\ q(x_0)x_0^{n-2} \\ \vdots \\ q(x_0)x_0 \\ q(x_0) \end{bmatrix} = 0$$

resultants and companion matrices

$$\mathbf{res}(p, q, x) = p_n^m \det q(C_p)$$

- no proofs today . . .

discriminants

for a univariate polynomial p, the discriminant is

$$\mathbf{dis}(p) = (-1)^{\binom{n}{2}} \frac{1}{p_n} \mathbf{res}(p, p', x)$$

- if p and its derivative p' have a common root, then p has a root of multiplicity 2 or more

discriminants

- if $p = ax^2 + bx + c$ then $\mathbf{dis}(p) = b^2 - 4ac$

- if $p = ax^3 + bx^2 + cx + d$ then

$$\mathbf{dis}(p) = -27a^2d^2 + 18adcb + b^2c^2 - 4b^3d - 4ac^3$$