Sub resultants in Roots

Hoon Hong

hong@math.ncsu.edu

Overview

Subresultants

fundamental in Computational algebra and algebraic geometry

- GCD
- Root isolation
- Root separation bound
- Cylindrical Algebraic Decomposition
- Topology analysis
- ...

Overview

Subresultants

fundamental in Computational algebra and algebraic geometry

Defined in terms of coefficients

Good for computation (algebra)

Bad for reasoning (geometry)

Find other expressions

Good for reasoning (geometry)

- In terms of Roots
- Elegant

Clarification

For notational simplicity
We will consider only

- degree 3
- "principal" coefficients

But the results can be easily extended to

- arbitrary degrees.
- all the coefficients.

Definition of Subresultant

$$A = a_3 x^3 + a_2 x^2 + a_1 x + a_0$$

$$B = b_3 x^3 + b_2 x^2 + b_1 x + b_0$$

$$S_0 = \begin{vmatrix} a_3 & a_2 & a_1 & a_0 & & \\ & a_3 & a_2 & a_1 & a_0 & \\ & & a_3 & a_2 & a_1 & a_0 \\ b_3 & b_2 & b_1 & b_0 & & \\ & b_3 & b_2 & b_1 & b_0 & \\ & & b_3 & b_2 & b_1 & b_0 \end{vmatrix} \begin{matrix} x^2 A \\ x A \\ A \\ x^2 B \\ x B \\ B \end{matrix}$$

0-th subresultant

"resultant"

$$A = a_3 x^3 + a_2 x^2 + a_1 x + a_0$$

$$B = b_3 x^3 + b_2 x^2 + b_1 x + b_0$$

$$S_1 = \begin{vmatrix} a_3 & a_2 & a_1 & a_0 & & \\ & a_3 & a_2 & a_1 & a_0 & \\ & & a_3 & a_2 & a_1 & a_0 \\ b_3 & b_2 & b_1 & b_0 & & \\ & b_3 & b_2 & b_1 & b_0 & \\ & & b_3 & b_2 & b_1 & b_0 \end{vmatrix}$$

$$A = a_3 x^3 + a_2 x^2 + a_1 x + a_0$$

$$B = b_3 x^3 + b_2 x^2 + b_1 x + b_0$$

$$S_2 = \begin{vmatrix} a_3 & a_2 & a_1 & a_0 & & \\ & a_3 & a_2 & a_1 & a_0 & \\ & & a_3 & a_2 & a_1 & a_0 \\ b_3 & b_2 & b_1 & b_0 & & \\ & b_3 & b_2 & b_1 & b_0 & \\ & & b_3 & b_2 & b_1 & b_0 \end{vmatrix}$$

Importance of Subresultant

Theorem

A and B has k common roots

iff

$$S_0 = S_1 = \cdots = S_{k-1} = 0$$

$$S_k \neq 0$$

Subresultant in Roots

$$A = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$$

$$B = (x-\beta_1)(x-\beta_2)(x-\beta_3)$$

$$S_K = \{\alpha_1\ \alpha_2\ \alpha_3\ \beta_1\ \beta_2\ \beta_3\}\ ?$$

Brute-force Approach

$$a_3 = 1$$
$$a_2 = -\alpha_1 - \alpha_2 - \alpha_3$$
$$a_1 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3$$
$$a_0 = -\alpha_1\alpha_2\alpha_3$$

$$b_3 = 1$$
$$b_2 = -\beta_1 - \beta_2 - \beta_3$$
$$b_1 = \beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3$$
$$b_0 = -\beta_1\beta_2\beta_3$$

See maple

Mess! Useless!

Well known

$$S_0 = (\alpha_1 - \beta_1)(\alpha_2 - \beta_1)(\alpha_3 - \beta_1)$$
$$(\alpha_1 - \beta_2)(\alpha_2 - \beta_2)(\alpha_3 - \beta_2)$$
$$(\alpha_1 - \beta_3)(\alpha_2 - \beta_3)(\alpha_3 - \beta_3)$$

$$= B(\alpha_1)\ B(\alpha_2)\ B(\alpha_3)$$

Elegant ! Useful !

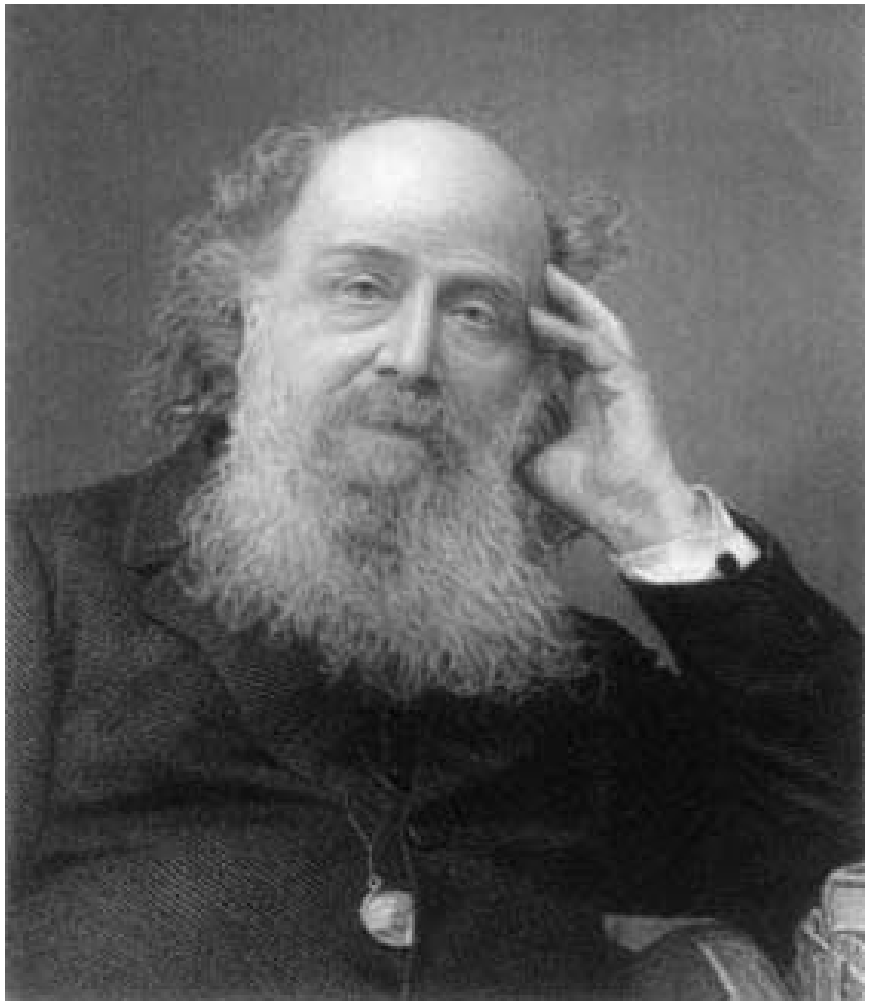
Question

$$S_1 = ?$$

$$S_2 = ?$$

$$\vdots$$

Sylvester (1814 - 1897)



Sylvester 1853

$$S_2 = \frac{(\alpha_1 - \beta_1)\quad(\alpha_2 - \beta_2)(\alpha_2 - \beta_3)(\alpha_3 - \beta_2)(\alpha_3 - \beta_3)}{(\alpha_1 - \alpha_2)\ (\alpha_1 - \alpha_3)\quad (\beta_1 - \beta_2)\ (\beta_1 - \beta_3)}$$

$+ \cdots$ Symmetrize

Tran. Roy. Soc. Lodon

" On a theory of sy zygetic relations.... " 150 pages

- Lascoux & Pragacz 2003 JSC
- D'Andrea, Hong, krick, Szanto 2006 JSC
  2008

Sylvester 1853

$$S_2 = \frac{(\alpha_1 - \beta_1)\quad(\alpha_2 - \beta_2)(\alpha_2 - \beta_3)(\alpha_3 - \beta_2)(\alpha_3 - \beta_3)}{(\alpha_1 - \alpha_2)\ (\alpha_1 - \alpha_3)\quad (\beta_1 - \beta_2)\ (\beta_1 - \beta_3)}$$

$+ \cdots$ Symmetrize

Difficult to generalize to

- non-commutative
- multi-variate

$$A(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

Recall

$$S_0 = \begin{vmatrix} B(\alpha_1) & B(\alpha_2) & B(\alpha_3) \end{vmatrix}$$

Observe

$$S_0 = \frac{\begin{vmatrix} \alpha_1^0 B(\alpha_1) & \alpha_2^0 B(\alpha_2) & \alpha_3^0 B(\alpha_3) \\ \alpha_1^1 B(\alpha_1) & \alpha_2^1 B(\alpha_2) & \alpha_3^1 B(\alpha_3) \\ \alpha_1^2 B(\alpha_1) & \alpha_2^2 B(\alpha_2) & \alpha_3^2 B(\alpha_3) \end{vmatrix}}{\begin{vmatrix} \alpha_1^0 & \alpha_2^0 & \alpha_3^0 \\ \alpha_1^1 & \alpha_2^1 & \alpha_3^1 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \end{vmatrix}}$$

Theorem 1 (Hong 1999)

$$S_1 = \frac{\begin{vmatrix} \alpha_1^0 & \alpha_2^0 & \alpha_3^0 \\ \alpha_1^0 B(\alpha_1) & \alpha_2^0 B(\alpha_2) & \alpha_3^0 B(\alpha_3) \\ \alpha_1^1 B(\alpha_1) & \alpha_2^1 B(\alpha_2) & \alpha_3^1 B(\alpha_3) \end{vmatrix}}{\begin{vmatrix} \alpha_1^0 & \alpha_2^0 & \alpha_3^0 \\ \alpha_1^1 & \alpha_2^1 & \alpha_3^1 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \end{vmatrix}}$$

Theorem 1

B does not have to be a polynomial !

$$S_2 = \frac{\begin{vmatrix} \alpha_1^0 & \alpha_2^0 & \alpha_3^0 \\ \alpha_1^1 & \alpha_2^1 & \alpha_3^1 \\ \alpha_1^0 B(\alpha_1) & \alpha_2^0 B(\alpha_2) & \alpha_3^0 B(\alpha_3) \end{vmatrix}}{\begin{vmatrix} \alpha_1^0 & \alpha_2^0 & \alpha_3^0 \\ \alpha_1^1 & \alpha_2^1 & \alpha_3^1 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \end{vmatrix}}$$

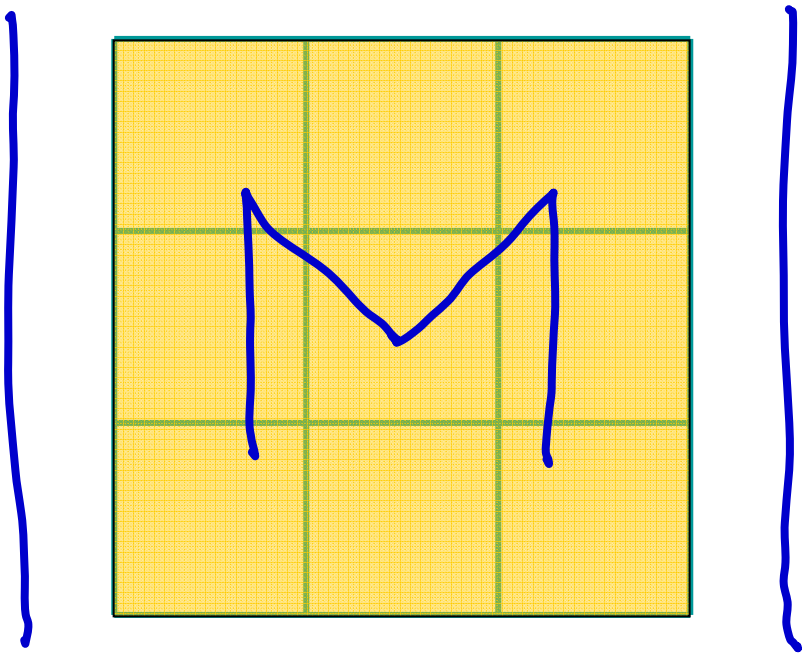
Theorem 2

divided difference

Let $M = \begin{bmatrix} B_0(\alpha_1) & B_0(\alpha_1,\alpha_2) & B_0(\alpha_1,\alpha_2,\alpha_3) \\ B_1(\alpha_1) & B_1(\alpha_1,\alpha_2) & B_1(\alpha_1,\alpha_2,\alpha_3) \\ B_2(\alpha_1) & B_2(\alpha_1,\alpha_2) & B_2(\alpha_1,\alpha_2,\alpha_3) \end{bmatrix}$

where $B_k = x^k B$

Then

$S_0 =$ 

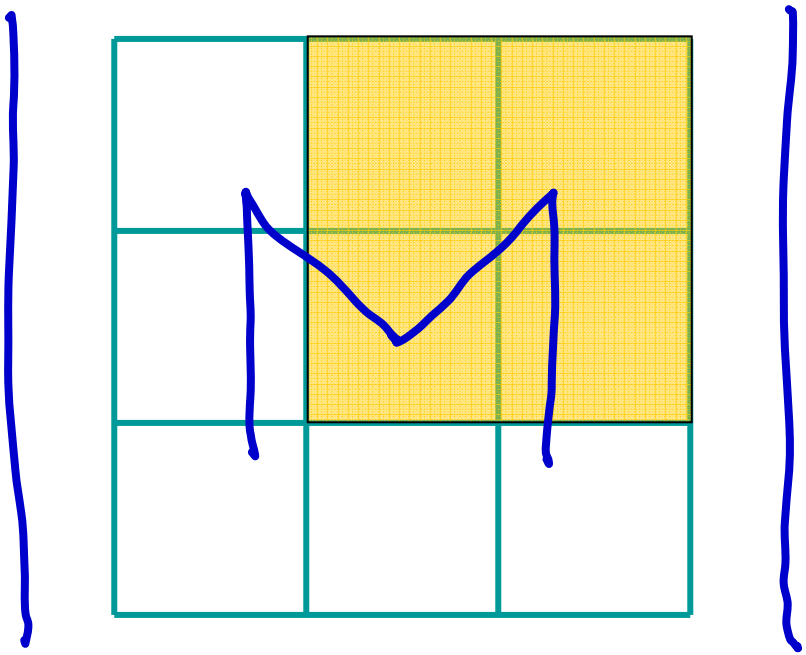
Theorem 2

divided difference

Let $M = \begin{bmatrix} B_0(\alpha_1) & B_0(\alpha_1,\alpha_2) & B_0(\alpha_1,\alpha_2,\alpha_3) \\ B_1(\alpha_1) & B_1(\alpha_1,\alpha_2) & B_1(\alpha_1,\alpha_2,\alpha_3) \\ B_2(\alpha_1) & B_2(\alpha_1,\alpha_2) & B_2(\alpha_1,\alpha_2,\alpha_3) \end{bmatrix}$

where $B_k = x^k B$

Then $S_1 =$



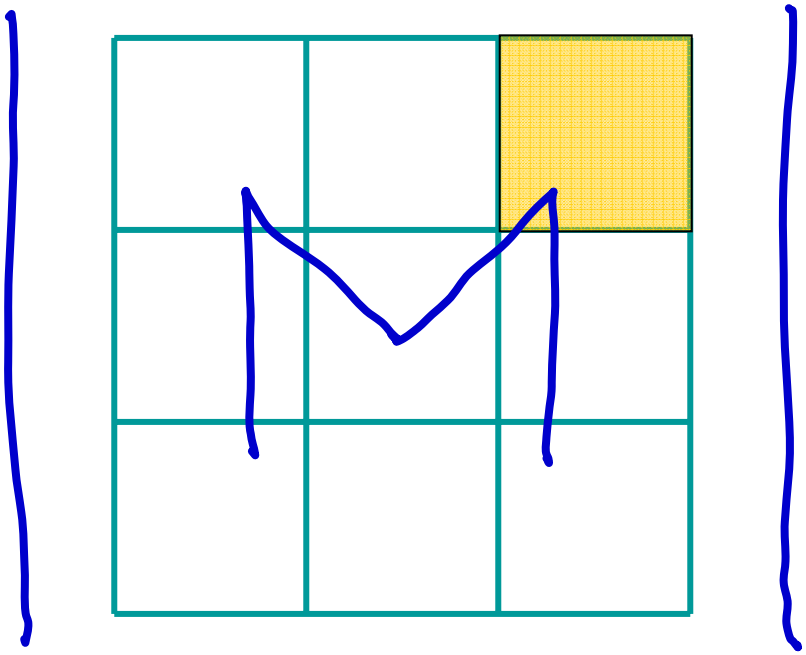
Theorem 2

divided difference

Let $M = \begin{bmatrix} B_0(\alpha_1) & B_0(\alpha_1,\alpha_2) & B_0(\alpha_1,\alpha_2,\alpha_3) \\ B_1(\alpha_1) & B_1(\alpha_1,\alpha_2) & B_1(\alpha_1,\alpha_2,\alpha_3) \\ B_2(\alpha_1) & B_2(\alpha_1,\alpha_2) & B_2(\alpha_1,\alpha_2,\alpha_3) \end{bmatrix}$

where $B_k = x^k B$

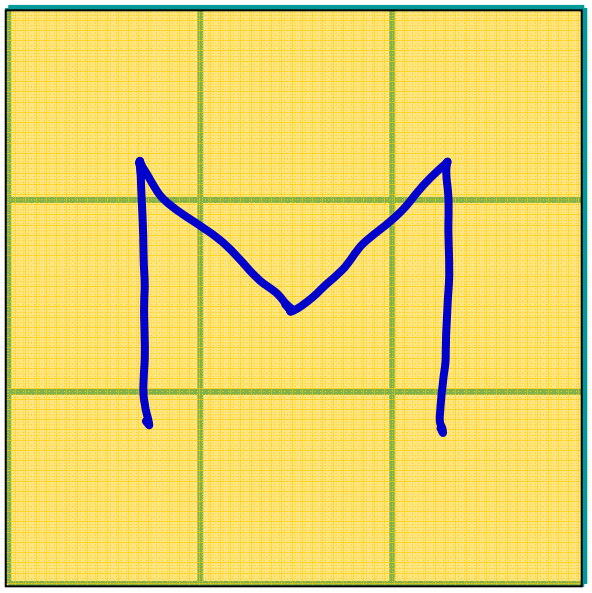
Then $S_2 =$



Theorem 3

Let $M_j = \begin{bmatrix} \alpha_1 - \beta_j & 1 & \\ & \alpha_2 - \beta_j & 1 \\ & & \alpha_3 - \beta_j \end{bmatrix}$

$M = M_1 M_2 M_3$

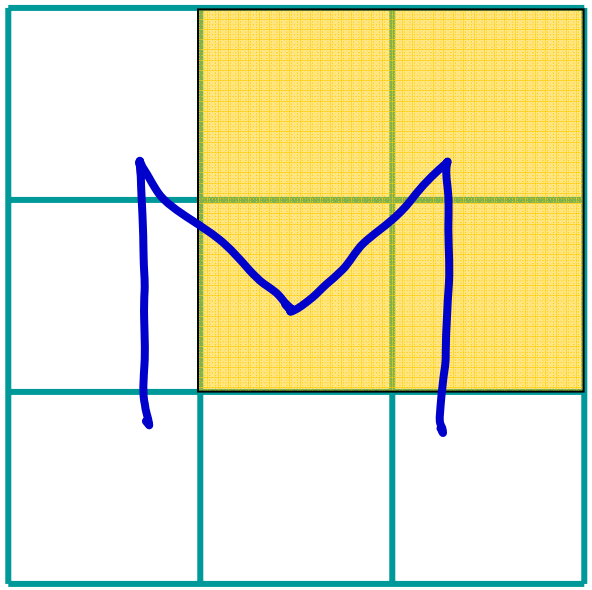
Then $S_0 =$ 

Theorem 3

Let $M_j = \begin{bmatrix} \alpha_1 - \beta_j & 1 & \\ & \alpha_2 - \beta_j & 1 \\ & & \alpha_3 - \beta_j \end{bmatrix}$

$M = M_1 M_2 M_3$

Then $S_1 =$

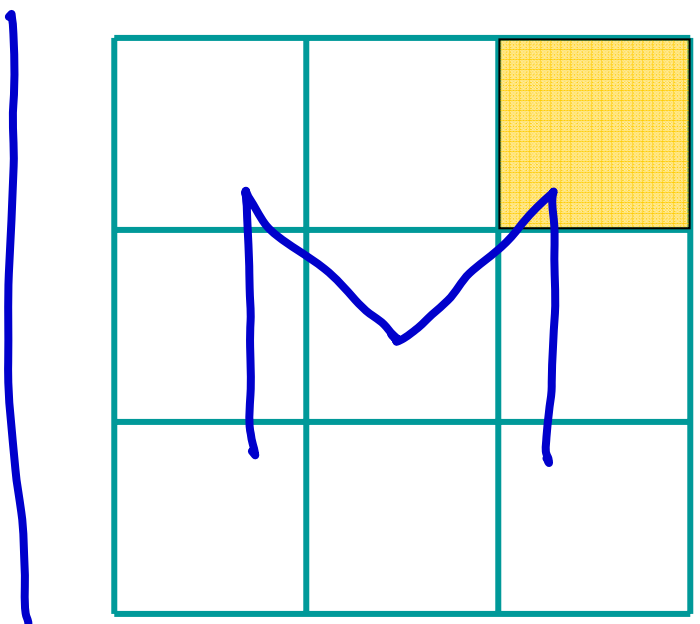


Theorem 3

Let $M_j = \begin{bmatrix} \alpha_1 - \beta_j & 1 & \\ & \alpha_2 - \beta_j & 1 \\ & & \alpha_3 - \beta_j \end{bmatrix}$

$M = M_1 M_2 M_3$

Then

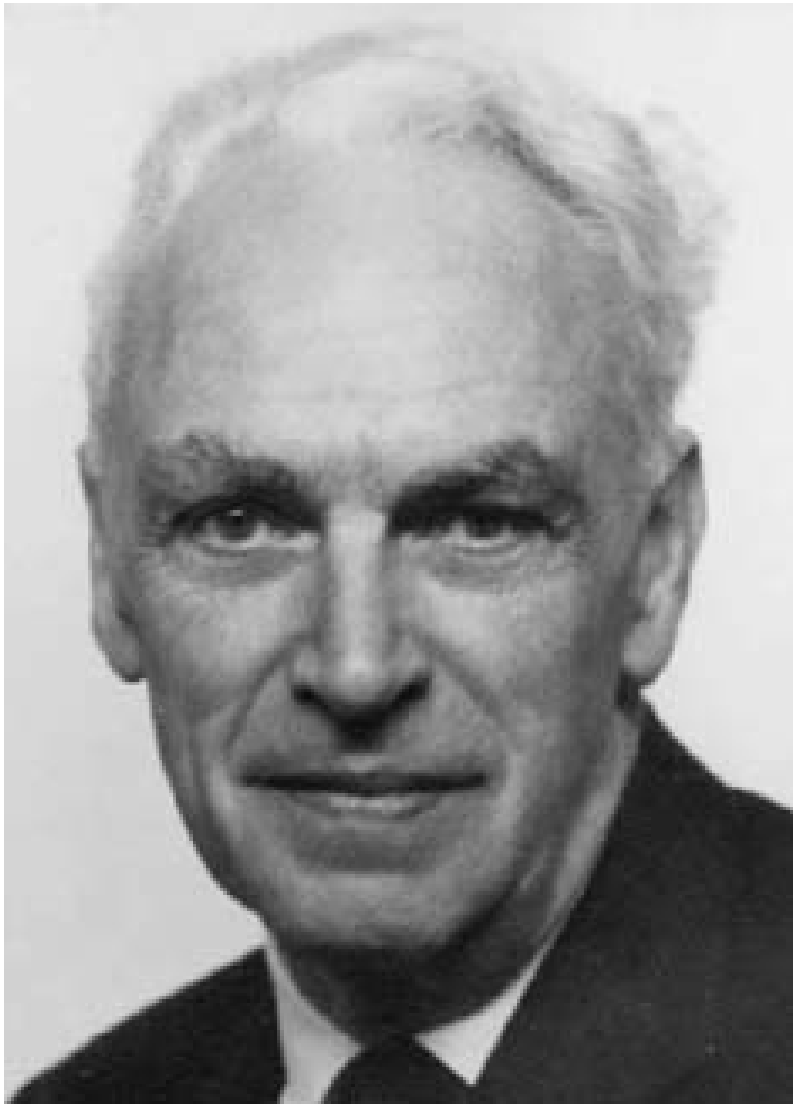
$S_2 =$ 

Several Others ....

Generalization

- Commutative $\longrightarrow$ Ore
- Univariate $\longrightarrow$ Multivariate

Ore (1899-1968)



Ore Polynomial Ring (1933)

$F[x]$ with $\sigma, \delta : F \to F$

such that for $a, b \in F$

- $x\,a = \sigma(a)\,x + \delta(a)$
- $\delta(ab) = \sigma(a)\,\delta(b) + \delta(a)\,b$

	σ	δ
Commutative	1	0
Linear differential	1	differential
Linear difference	shift	difference

Ore Subresultants

Ziming Li (1996)

- $x \cdot A \longrightarrow x \cdot A$

  $x \cdot A$: commutative; $x \cdot A$: non-commutative

- Use Sylvester matrix

Derived many interesting results

Theorem 4 (Hong)

$$S_0 = \frac{\begin{vmatrix} B_0(\alpha_1) & B_0(\alpha_2) & B_0(\alpha_3) \\ B_1(\alpha_1) & B_1(\alpha_2) & B_1(\alpha_3) \\ B_2(\alpha_1) & B_2(\alpha_2) & B_2(\alpha_3) \end{vmatrix}}{\begin{vmatrix} x^0(\alpha_1) & x^0(\alpha_2) & x^0(\alpha_3) \\ x^1(\alpha_1) & x^1(\alpha_2) & x^1(\alpha_3) \\ x^2(\alpha_1) & x^2(\alpha_2) & x^2(\alpha_3) \end{vmatrix}}$$

where $B_k = x^k B$

"Wronskian"

Theorem 4

$$S_1 = \frac{\begin{vmatrix} x^0(\alpha_1) & x^0(\alpha_2) & x^0(\alpha_3) \\ B_0(\alpha_1) & B_0(\alpha_2) & B_0(\alpha_3) \\ B_1(\alpha_1) & B_1(\alpha_2) & B_1(\alpha_3) \end{vmatrix}}{\begin{vmatrix} x^0(\alpha_1) & x^0(\alpha_2) & x^0(\alpha_3) \\ x^1(\alpha_1) & x^1(\alpha_2) & x^1(\alpha_3) \\ x^2(\alpha_1) & x^2(\alpha_2) & x^2(\alpha_3) \end{vmatrix}}$$

where $B_k = x^k B$

Theorem 4

$$S_2 = \frac{\begin{vmatrix} x^0(\alpha_1) & x^0(\alpha_2) & x^0(\alpha_3) \\ x^1(\alpha_1) & x^1(\alpha_2) & x^1(\alpha_3) \\ B_0(\alpha_1) & B_0(\alpha_2) & B_0(\alpha_3) \end{vmatrix}}{\begin{vmatrix} x^0(\alpha_1) & x^0(\alpha_2) & x^0(\alpha_3) \\ x^1(\alpha_1) & x^1(\alpha_2) & x^1(\alpha_3) \\ x^2(\alpha_1) & x^2(\alpha_2) & x^2(\alpha_3) \end{vmatrix}}$$

where $B_k = x^k B$

Multivariate Subresultants

$A_1, \ldots, A_n, B \in \mathbb{C}[x_1, \ldots, x_n]$

Gonzalez-Vega 1990

Chardin 1995

Multivariate Subresultants in Roots

$A_1, \ldots, A_n, B \in \mathbb{C}[x_1, \ldots, x_n]$

$\alpha_1, \ldots, \alpha_\ell$

D'Andrea, Krick, Szanto 2006

$\{w_i\}$ be a basis of $\mathbb{C}[x_1,\dots,x_n]/\langle A_1,\dots,A_n\rangle$

$$S_0 \sim \frac{\begin{vmatrix} B_0(\alpha_1) & B_0(\alpha_2) & B_0(\alpha_3) \\ B_1(\alpha_1) & B_1(\alpha_2) & B_1(\alpha_3) \\ B_2(\alpha_1) & B_2(\alpha_2) & B_2(\alpha_3) \end{vmatrix}}{\begin{vmatrix} w_0(\alpha_1) & w_0(\alpha_2) & w_0(\alpha_3) \\ w_1(\alpha_1) & w_1(\alpha_2) & w_1(\alpha_3) \\ w_2(\alpha_1) & w_2(\alpha_2) & w_2(\alpha_3) \end{vmatrix}}$$

where $B_k = w_k B$

$\{w_i\}$ be a basis of $\mathbb{C}[x_1,\dots,x_n]/\langle A_1,\dots,A_n\rangle$

$$S_1 \sim \frac{\begin{vmatrix} w_0(\alpha_1) & w_0(\alpha_2) & w_0(\alpha_3) \\ B_0(\alpha_1) & B_0(\alpha_2) & B_0(\alpha_3) \\ B_1(\alpha_1) & B_1(\alpha_2) & B_1(\alpha_3) \end{vmatrix}}{\begin{vmatrix} w_0(\alpha_1) & w_0(\alpha_2) & w_0(\alpha_3) \\ w_1(\alpha_1) & w_1(\alpha_2) & w_1(\alpha_3) \\ w_2(\alpha_1) & w_2(\alpha_2) & w_2(\alpha_3) \end{vmatrix}}$$

where $B_\kappa = w_\kappa B$

$\{w_i\}$ be a basis of $\mathbb{C}[x_1,\dots,x_n]/\langle A_1,\dots,A_n\rangle$

$$S_2 \sim \frac{\begin{vmatrix} w_0(\alpha_1) & w_0(\alpha_2) & w_0(\alpha_3) \\ w_1(\alpha_1) & w_1(\alpha_2) & w_1(\alpha_3) \\ B_0(\alpha_1) & B_0(\alpha_2) & B_0(\alpha_3) \end{vmatrix}}{\begin{vmatrix} w_0(\alpha_1) & w_0(\alpha_2) & w_0(\alpha_3) \\ w_1(\alpha_1) & w_1(\alpha_2) & w_1(\alpha_3) \\ w_2(\alpha_1) & w_2(\alpha_2) & w_2(\alpha_3) \end{vmatrix}}$$

where $B_k = w_k B$

Summary

Nice expressions of subresultants in terms of roots

Open Problems

- Multivariate Ore
- New root separation bounds?
- ...