Lec20A Resultants + Factorization, Michael Monagan

March 25, 2021 1:58 PM

Assignment #5 is due on Monday — end of MACM 401.

Resultant Calculus

Let $A, B \in K[x]$, K a field e.g. $\mathbb{Q}$

Let $A = a_m x^m + \cdots + a_0 = a_m \prod_{i=1}^{m} (x - \alpha_i)$ where $\alpha_i \in \overline{K}$.

$B = b_n x^n + \cdots + b_0 = b_n \prod_{i=1}^{n} (x - \beta_i)$ where $\beta_i \in \overline{K}$.

$$\operatorname{res}(A,B) = \underline{a_m^n} \cdot b_n^m \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j) = (-1)^{m \cdot n} b_n^m a_m^n \prod_{j=1}^{n} \prod_{i=1}^{m} (\beta_j - \alpha_i)$$

① $\operatorname{res}(c \in K, B) = c^n \cdot b_n^0 = c^n$.

② $\operatorname{res}(B, A) = (-1)^{mn} \operatorname{res}(A,B)$.

$$\operatorname{res}(A,B) = a_m^n \prod_{i=1}^{m} \underbrace{\left(b_n \prod_{j=1}^{n} (\alpha_i - \beta_j) \right)}_{B(\alpha_i)} = (-1)^{mn} b_n^m \prod_{j=1}^{n} \underbrace{\left(a_m \prod_{i=1}^{m} (\beta_j - \alpha_i) \right)}_{A(\beta_j)}$$

③ $\operatorname{res}(A,B) = a_m^n \prod_{i=1}^{m} B(\alpha_i) = (-1)^{mn} b_n^m \prod_{j=1}^{n} A(\beta_j)$.

deg m deg n

④ $\operatorname{res}(A, BC) = a_m^{n+\ell} \prod_{i=1}^{m} (BC)(\alpha_i) = \underbrace{a_m^n \prod_{i=1}^{m} B(\alpha_i)}\cdot a_m^{\ell} \prod_{i=1}^{m} C(\alpha_i)$

deg ℓ

$\overset{③}{=} \operatorname{res}(A,B) \cdot \operatorname{res}(A,C)$.

⑤ $\operatorname{res}(A,B) = 0 \iff \deg(\gcd(A,B)) > 0$.

Suppose $\overset{A}{m} \geq \overset{B}{n} > 0$. Let $R = \operatorname{rem}(A \div B) \Rightarrow \boxed{A = BQ + R}$

CASE $R = 0 \Rightarrow \deg(\gcd(A,B)) > 0 \Rightarrow \operatorname{res}(A,B) = 0$.

CASE $R \neq 0$.

Let $\ell = \deg R$.

$$\operatorname{res}(A,B) = \operatorname{res}(BQ+R, B)$$

$$③ = (-1)^{mn} b_n^m \prod_{j=1}^{n} \underbrace{(BQ)(\beta_j)}_{=0} + R(\beta_j)$$

$$\Rightarrow. \quad \operatorname{res}(A,B) = \underline{(-1)^{mn}} b_n^m \prod_{j=1}^{n} R(\beta_j)$$

$$\operatorname{res}(R,B) \overset{③}{=} \underline{(-1)^{\ell n}} b_n^{\ell} \prod_{j=1}^{n} R(\beta_j)$$

$$\frac{\operatorname{res}(A,B)}{\operatorname{res}(R,B)} = (-1)^{mn-\ell n} \cdot b_n^{m-\ell}.$$

$$⑥ \quad \operatorname{res}(A,B) = (-1)^{n(m-\ell)} \cdot b_n^{m-\ell} \operatorname{res}(R,B).$$

$$\gcd(A,B) = \gcd(R,B)$$

We can compute the resultant using the E.A. in $O(n \cdot m)$ arithmetic operations which is better than using $\det(S)$ where S is Sylvester's matrix because that costs $O((n+m)^3)$ using Gaussian elimination.