Результант

Выполнила Боброва Наталья

Литература

- Е.А.Калинина, А.Ю.Утешев "Теория исключения", 2002 год
- Vmath.ru (Интерактивная информационно-консультационная среда, a.k.a записная книжка Утешева)
- В.В.Прасолов "Многочлены", 2001 год

Определение результанта

Пусть даны два полином $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$ и $g(x) = b_0x^m + b_1x^{m-1} + \ldots + b_m$

Из их коэффициентов составлена матрица:

$$M = \begin{pmatrix} a_0 & a_1 & a_2 & \ldots & \ldots & a_n & 0 & \ldots & 0 & 0 \\ 0 & a_0 & a_1 & \ldots & \ldots & a_{n-1} & a_n & \ldots & 0 & 0 \\ \vdots & & \ddots & & & & & & \ddots & \\ 0 & 0 & \ldots & a_0 & \ldots & \ldots & & \ldots & a_{n-1} & a_n \\ 0 & 0 & \ldots & & b_0 & b_1 & \ldots & \ldots & b_{m-1} & b_m \\ 0 & 0 & \ldots & b_0 & b_1 & \ldots & & \ldots & b_m & 0 \\ \vdots & & \iddots & \ldots & & & & & & \vdots \\ 0 & b_0 & \ldots & \ldots & b_m & 0 & \ldots & & \ldots & 0 \\ b_0 & \ldots & \ldots & b_m & 0 & \ldots & & & & 0 \end{pmatrix} \begin{array}{l} \left.\begin{array}{c} \\ \\ \\ \\ \end{array}\right\} m \\ \left.\begin{array}{c} \\ \\ \\ \\ \\ \end{array}\right\} n \end{array}$$

ОПРЕДЕЛЕНИЕ:

Выражение $\mathcal{R}(f,g) \stackrel{\text{def}}{=} (-1)^{n(n-1)/2} \det M$

называется *результантом* полиномов f и g
в форме Сильвестра.

Замечание: чаще в литературе матрицу, определителем которой является результант (матрицу Сильвестра), определяют в несколько другом виде. Однако через приведённый выше вид удобнее определять *субрезультант*.

Теоремы

ТЕОРЕМА: Для того, чтобы f и g имели общий корень необходимо и достаточно, чтобы R(f, g) = 0.

СЛЕДСТВИЕ: (представление результанта через корни полиномов)

Пусть λ_j — корни полинома μ_k — корни полинома g. Тогда:

$$\mathcal{R}(f,g) = a_0^m b_0^n \prod_{k=1}^{m} \prod_{j=1}^{n} (\lambda_j - \mu_k) = a_0^m \prod_{j=1}^{n} g(\lambda_j) = (-1)^{mn} b_0^n \prod_{k=1}^{m} f(\mu_k)$$

ЗАМЕЧАНИЕ: Частный случай при g = const: R(f,const) = $(\text{const})^n$

Свойства

Свойство 1: $R(f, gh) = R(f, g)R(f, h)$

Свойство 2: $R(g, f) = (-1)^{nm} R(f, g)$

Свойство 3: Если $f = gq + r$, то $R(f, g) = b_0^{(\deg f - \deg r)} R(r, g)$

Свойства

Свойство 4: Есл $n \geq m \geq 1, \; A \neq 0, \; C \neq 0$ и

$\deg(Af(x) + Bg(x)) = \deg(Cf(x) + Dg(x)) = n,$ то

$$\mathcal{R}(Af(x) + Bg(x), Cf(x) + Dg(x)) = (AD - BC)^n \mathcal{R}(f(x), g(x))$$

Свойство 5: Пус $f^*(x) \stackrel{\text{def}}{=} x^n f(1/x) = a_n x^n + \ldots + a_0,$

$g^*(x) \stackrel{\text{def}}{=} x^m g(1/x) = b_m x^m + \ldots + b_0, \;\; a_0, a_n, b_0, b_m$ не равны 0

Тогда $\mathcal{R}(f^*, g^*) = (-1)^{mn} \mathcal{R}(f, g)$

Результант и НОД

Алгоритм Евклида:

$$
\begin{array}{lcll}
f(x) & = & g(x)q_1(x) + r_1(x)\,, & 0 \le \deg r_1(x) < \deg g(x)\,, \\
g(x) & = & r_1(x)q_2(x) + r_2(x)\,, & 0 \le \deg r_2(x) < \deg r_1(x), \\
r_1(x) & = & r_2(x)q_3(x) + r_3(x)\,, & 0 \le \deg r_3(x) < \deg r_2(x), \\
\ldots & & \ldots & \\
r_{j-2}(x) & = & r_{j-1}(x)q_j(x) + r_j(x)\,, & 0 \le \deg r_j(x) < \deg r_{j-1}(x), \\
\ldots & & \ldots & \\
r_{k-2}(x) & = & r_{k-1}(x)q_k(x) + r_k(x)\,, & 0 \le \deg r_k(x) < \deg r_{k-1}(x), \\
r_{k-1}(x) & = & r_k(x)q_{k+1}(x). &
\end{array}
$$

Результант и НОД

Линейное представление НОД $f(x)v(x) + g(x)u(x) \equiv \text{НОД}\,(f, g)$

ТЕОРЕМА: существуют полиномы v(x) и u(x) со степенями deg u ≤ (deg f) - 1, deg v ≤ (deg g) - 1, удовлетворяющие тождеству R(f,g) ≡ f(x)v(x) + g(x)u(x). Если же f и g взаимно просты, то полиномы v, u определены единственным образом.

Субрезультант

ОПРЕДЕЛЕНИЕ: Определитель матрицы M1, полученной из матрицы M вычёркиванием первых и последних строк и столбцов, называется *первым субрезультантом* полиномов f и g.

$$\mathcal{R}^{(1)}(f,g) = \begin{vmatrix} a_0 & a_1 & \dots & \dots & a_{n-1} & a_n & \dots & 0 \\ \vdots & \ddots & & & & & \ddots & \\ 0 & \dots & a_0 & \dots & \dots & & \dots & a_{n-1} \\ 0 & \dots & & b_0 & b_1 & \dots & \dots & b_{m-1} \\ 0 & \dots & b_0 & b_1 & \dots & & \dots & b_m \\ \vdots & & \dots & & & & & \vdots \\ b_0 & \dots & \dots & & b_m & \dots & & 0 \end{vmatrix} \begin{matrix} \left.\begin{matrix} \\ \\ \\ \end{matrix}\right\} m-1 \\ \left.\begin{matrix} \\ \\ \\ \\ \end{matrix}\right\} n-1 \end{matrix}$$

Субрезультант

ТЕОРЕМА 1: Для того, чтобы f и g имели ровно один общий корень, необходимо и достаточно, чтобы $R(f, g) = 0$, $R^{(1)}(f, g) \neq 0$.

ТЕОРЕМА 2: Пусть $R(f, g) = 0$ и $x = c$ — общий корень f и g. Обозначим $f_1 = f/(x - c)$, $g_1 = g/(x - c)$. Тогда $R^{(1)}(f, g) = R(f_1, g_1)$.

СЛЕДСТВИЕ 1: При выполнении условия теоремы 1 единственный общий корень рационально выражается через коэффициенты полиномов f(x) и g(x):

$$c = -\frac{\det M_1^{(1)}}{\mathcal{R}^{(1)}(f, g)}$$

Субрезультант

ОПРЕДЕЛЕНИЕ: Определитель матрицы M_2, получаемой из матрицы M вычеркиванием двух первых и двух последних столбцов, двух первых и двух последних строк, называется *вторым субрезультантом* полиномов f и g и обозначается $R^{(2)}(f, g)$.

ТЕОРЕМА 3: Для того чтобы f(x) и g(x) имели в точности два общих корня, необходимо и достаточно, чтобы выполнялись условия $R(f, g) = R^{(1)}(f, g)=0$, $R^{(2)}(f, g) \neq 0$.

СЛЕДСТВИЕ 2:При условии теоремы 3 оба корня должны удовлетворять квадратному уравнению $x^2R^{(2)}(f, g) + x \det M_2^{(1)} + \det M_2^{(2)} = 0$. Полином, стоящий в левой части уравнения, является НОД (f, g).

Субрезультант

ОПРЕДЕЛЕНИЕ: Определитель матрицы M_k, получаемой из матрицы M вычеркиванием k первых и k последних столбцов, k первых и k последних строк, называется k-м субрезультантом полиномов f и g и обозначается $R^{(k)}(f, g)$.

ТЕОРЕМА 5: А) Для существования d общих корней f(x) и g(x) (т.е. для того, чтобы deg(НОД (f, g)) = d), необходимо и достаточно, чтобы $R(f, g) = R^{(1)}(f, g) = \ldots = R^{(d-1)}(f, g) = 0$, $R^{(d)}(f, g) \neq 0$.

б) В этом случае НОД(f, g) можно представить в виде $x^d R^{(d)}(f,g) + x^{d-1} \det M_d^{(1)} + \ldots + \det M^{(d)}$

в) Полиномы v(x) и u(x), дающие линейное представление НОД(f, g), получаются из $R^{(d)}$ заменой в нем последнего столбца на $[x^{m-d-1}, x^{m-d-2}, \ldots, x, 1, 0, 0, \ldots, 0]$ и $[0, 0, \ldots, 0, 0, 1, x, \ldots, x^{n-d-1}]$ соответственно. Эти полиномы будут единственными при ограничениях на степени: $\deg v \leq m - d - 1$, $\deg u \leq n - d - 1$.

Полином двух переменных

ОПРЕДЕЛЕНИЕ: Если полином $f(x, y)$ содержит только мономы степени k: $f(x, y) = a_{k0}x^k + a_{k-1,1}x^{k-1}y + \dots + a_{1,k-1}xy^{k-1} + a_{0k}y^k$ то он называется однородным полиномом или формой степени k. Обозначение: $f_k(x, y)$.

ОПРЕДЕЛЕНИЕ: Точка $(x_0, y_0) \in C^2$ называется нулем полинома $f(x, y)$, если $f(x_0, y_0) = 0$.

ОПРЕДЕЛЕНИЕ: Нуль (x_0, y_0) полинома $f(x, y)$ будем называть вещественным, если $x_0 \in R$ и $y_0 \in R$; в противном случае пару (x_0, y_0) и сопряжённую к ней будем называть комплексно-сопряженными нулями.

Общая схема исключения

ОПРЕДЕЛЕНИЕ: Результант f(x, y) и g(x, y), рассматриваемых как полиномы по переменной y, называется элиминантой системы f(x,y) = 0, g(x,y) = 0 по x. Аналогично определяется и вторая элиминанта системы.

$$\mathcal{X}(x) \stackrel{\text{def}}{=} \mathcal{R}_y(f(x,y), g(x,y)) \qquad \mathcal{Y}(y) \stackrel{\text{def}}{=} \mathcal{R}_x(f(x,y), g(x,y))$$

ТЕОРЕМА 1: Пусть выполнено усло $a_{n0} \neq 0, a_{0n} \neq 0, b_{m0} \neq 0, b_{0m} \neq 0$
Если пара (a,b) является решением f(x,y) = 0, g(x,y) = 0, то необходимо, чтобы X(a) = 0, Y(b) = 0.

ТЕОРЕМА 2: Пусть выполнено усло $a_{n0} \neq 0, a_{0n} \neq 0, b_{m0} \neq 0, b_{0m} \neq 0$
Тогда для любого корня a элиминанты X существует хотя бы одно значение y = b такое, что пара (a,b) — решение f(x,y) = 0, g(x,y) = 0.

Спасибо за внимание!