Resultantes e Aplicações

Fernando Tura,
Centro de Tecnologia de Alegrete,UNIPAMPA-UFSM,
97542-600, Alegrete, RS
E-mail: ftura@smail.ufsm.br

Vilmar Trevisan
UFRGS - Instituto de Matemática
91509-900, Porto Alegre, RS
E-mail: trevisan@mat.ufrgs.br.

O presente trabalho aborda uma técnica para determinar as soluções de sistemas de equações polinomiais. Esta técnica conhecida como Resultantes, é puramente algébrica, e interliga tópicos da Matemática, como a Geometria Algébrica e a Álgebra Computacional.

Mais especificamente, apresentaremos o Resultante e suas aplicações. Para o cálculo do Resultante, usaremos a fórmula de Macaulay e de Poisson.

Terminamos apresentando uma prova de um caso particular do Teorema de Bezout, como aplicação da teoria de Resultantes. Este teorema é muito importante, pois fornece um número de soluções de um sistema de equações polinomiais.

O tópico de resolução de sistemas de equações polinomiais é o centro de várias áreas da Matemática, não somente pela forte teoria, mas também por suas aplicações. Nos últimos anos, graças a um desenvolvimento explosivo de algoritmos, tem sido possível a resolução de muitos problemas que eram até então considerados como intratáveis.

Como exemplo de avanços, a fatoração de polinômios, um subproblema desse tópico de equações polinomiais, alcançou um desenvolvimento incrível, expandindo muito as áreas de aplicações como robótica, estrutura biológica molecular, design computacional, modelagem geométrica, e certamente áreas de estatísticas, otimização, teoria de jogos, e rede biológica. O leitor interessado poderá consultar os artigos [3] e [4] e os trabalhos [1] e [2] para um desenvolvimento mais recente.

Iniciamos com a seguinte motivação. Sejam os polinômios $a_0 + a_1x$ e $b_0 + b_1x$ de graus 1, com os coeficientes pertencentes a um corpo K, procuramos um valor x de modo que satisfaça

$$a_0 + a_1x = 0$$

$$b_0 + b_1x = 0. \tag{1}$$

Então ambas equações satisfazem simultaneamente

$$\frac{a_0}{a_1} = \frac{b_0}{b_1},$$

que pode ser escrito como a_0b_1 - $a_1b_0 = 0$. Formalmente podemos observar isto como um sistema na forma matricial

$$\begin{bmatrix} a_0 & a_1 \\ b_0 & b_1 \end{bmatrix} \begin{bmatrix} x^0 \\ x^1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

Então uma solução não trivial de (1) implica que

$$a_0b_1 \text{ - } a_1b_0 = 0.$$

Mais geral, dados dois polinômios $f(x)$ e $g(x)$ de graus n e m, respectivamente, podemos obter um sistema de $n + m$ equações nas variáveis $(x^0, x^1, x^2, \ldots, x^{n+m-1})$. E novamente a condição para que estes dois polinômios possuam uma raiz comum, implica que o determinante obtido pelos coeficientes deste sistema, seja zero.

A técnica mencionada acima é conhecida como o Resultante de dois polinômios a uma variável. Ela será uma motivação para encontrarmos ferramentas que determinam uma raiz comum, no caso de n polinômios em n variáveis.

A definição do Resultante se baseia numa matriz conhecida como matriz Sylvester. Sejam f, g dois polinômios em $K[x]$

$$f = \sum_{i=0}^{n} f_i x^i, g = \sum_{i=0}^{m} g_i x^i,$$

de graus n, m respectivamente. Definimos o Resultante de $f(x)$ e $g(x)$, denotado por $Res_{n,m}(f, g)$ como determinante da matriz

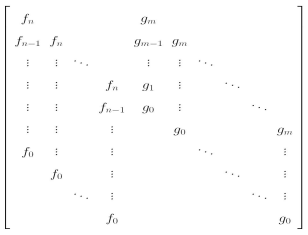

Figura 1: $Res_{n,m}(f, g)$

Considere, por exemplo, $f = x^4 - 3x^3 + 2x$ e $g = x^3 - 1$. Calculando o Resultante, segundo a definição acima, obtemos que o $Res_{4,3}(f, g) = 0$.

Observe que $f = x(x-1)(x^2 - 2x - 2)$ e $g = (x-1)(x^2+x+1)$, têm um fator em comum $x - 1$, ou seja, f e g têm uma raiz em comum.

O fato do Resultante ser nulo, implicar em que f e g possuem uma raiz em comum, é o nosso primeiro resultado.

Teorema 1: Sejam $f = \sum_{i=0}^{n} f_i x^i, g = \sum_{i=0}^{m} g_i x^i$ dois polinômios em $K[x]$ tais que $f_n, g_m \neq 0$ de graus ≥ 1. Então as seguintes afirmações são equivalentes:

i) $Res_{n,m}(f, g) = 0$;

ii) Existem polinômios não nulos $A, B \in K[x]$, de graus menores que n e m respectivamente, tais que $A(x)g(x) = B(x)f(x)$;

iii) f e g têm um fator comum não constante em $K[x]$;

Esse teorema nos leva, a questionar, se podemos obter um resultado para o caso geral, ou seja, dados n polinômios $f_1 \ldots, f_n$ de n variáveis $x_1, \ldots, x_n$. Queremos determinar uma condição para que

$$f_1(x_1, \ldots, x_n) = \ldots = f_n(x_1, \ldots, x_n) = 0 \quad (2)$$

tenha uma solução não trivial.

Para obtermos uma condição necessária e suficiente para (2), precisamos fazer uma extensão do Resultante a várias variáveis, o que não é trivial. Para isto temos que trabalhar com polinômios homogêneos e usar algumas ferramentas da Geometria Algébrica, como espaços projetivos e dimensões desses espaços.

A condição para (2) é dada pelo seguinte resultado:

Teorema 2: Existe um único polinômio $Res_{d_1,\ldots,d_n}(F_1, \ldots, F_n)$ tal que, se $F_1, \ldots, F_n \in K[x_1, \ldots, x_n]$ são os polinômios homogêneos de $f_1, \ldots, f_n$, respectivamente de graus $d_1, \ldots, d_n$, então a equação (2) tem uma solução não trivial em $K[x_1, \ldots, x_n]$ se e somente se o $Res_{d_1,\ldots,d_n}(F_1, ..., F_n) = 0$.

A referência [5], mostra com detalhes, essa extensão do Resultante a várias variáveis e a demonstração dos teoremas 1 e 2.

Dada a condição para que um sistema de equações polinomiais admita uma solução não trivial, de acordo com o Teorema 2, o próximo problema é como calcular esse polinômio.

Vamos apresentar duas técnicas para calcular o Resultante de n polinômios homogêneos de n variáveis. A primeira é conhecida como a fórmula de Macaulay, cujo o $Res_{d_1,\ldots,d_n}(F_1, \ldots, F_n)$ é dado pelo quociente de dois determinantes. Essa fórmula na prática tem complexidade alta , em alguns casos pode não ser viável.

Assim o próximo resultado nos permite calcular o Resultante a várias variáveis.

Teorema 3: Sejam $F_1, ..., F_n$ polinômios homogêneos, então o Resultante é dado por

$$Res_{d_1,\ldots,d_n}(F_1, \ldots, F_n) = \frac{D_n}{D'_n}$$

desde que $D'_n \neq 0$. Aqui D_n e D'_n representam os determinantes obtidos sobre os coeficientes dos polinômios F_i.

A referência [5], mostra a prova desse resultado.

Por exemplo considere os polinômios $F_1 = a_1x_0^2 - a_2x_1^2, F_2 = b_1x_0^2 - b_2x_1^2 + b_3x_0x_1, F_3 = x_0 - x_1 - x_2 = 0$, onde os $a_i, b_i \in K$.

Assim pelo Teorema 3, temos que $Res_{2,2,1}(F_1, F_2, F_3) = b_2^2a_1^2 - 2a_1b_2a_2b_3 - 2a_1b_2a_2b_1 - a_1a_2b_3^2 + a_2^2b_3^2 + 2a_2^2b_3b_1 + a_2^2b_1^2$.

A outra técnica para calcular o Resultante a várias variáveis, é conhecida como a fórmula de Poisson. A fórmula de Poisson necessita de

ferramentas mais geométricas do que a fórmula de Macaulay.

O próximo resultado, nos fornece a fórmula da Poisson para o Resultante em uma variável, o caso geral pode ser encontrado em [5].

Teorema 4: Sejam $f = \sum_{i=0}^{n} f_i x^i, g = \sum_{i=0}^{m} g_i x^i$ dois polinômios de graus n, m respectivamente em $k[x]$. Então o Resultante é dado por $Res_{n,m}(f,g) = f_n^m det(m_g : A_f \longrightarrow A_f)$, onde $A_f = K[x]/ < f >$ é a álgebra quociente e m_g é a transformação linear.

Por exemplo, considere $f(x) = x^3 + x - 1$ e $g(x) = 2x^2 + 3x + 7$. Pelo resultado anterior, $Res_{3,2}(f,g) = f_n^m det(m_g : A_f \longrightarrow A_f)$, ou seja, $Res_{3,2}(f,g) = (1)^2 det(m_g : A_f \longrightarrow A_f)$. Sabendo que $A_f = K[x]/ < f >= \{c_0 + c_1 x + c_2 x^2 : c_i \in K\}$. Para determinar o $det(m_{f_n} : A_f \longrightarrow A_f)$ basta tomar o resto da divisão de $(c_0 + c_1 x + c_2 x^2) \times (2x^2 + 3x + 7)$ por $x^3 + x - 1$. O resto da divisão é dado por $7c_0 + 2c_1 + 3c_2 + (3c_0 + 5c_1 - c_2)x + (2c_0 + 3c_1 + 5c_2)x^2$. Logo a transformação que associa $(c_0, c_1, c_2) \longrightarrow (7c_0 + 2c_1 + 3c_2, 3c_0 + 5c_1 - c_2, 2c_0 + 3c_1 + 5c_2)$ é dada pelo $det \begin{bmatrix} 7 & 2 & 3 \\ 3 & 5 & -1 \\ 2 & 3 & 5 \end{bmatrix} = 159$.

Então $Res_{3,2}(f,g) = (1)^2 det(m_g : A_f \longrightarrow A_f) = 159$.

Pelo Teorema 1, podemos afirmar que os polinômios $f(x) = x^3 + x - 1$ e $g(x) = 2x^2 + 3x + 7$ não têm raiz em comum, pois o $Res_{3,2}(f,g) = 159 \neq 0$.

Apresentado o Resultante, vamos para as aplicações. Como primeira aplicação simples de Resultantes, vamos verificar como um sistema de duas equações com duas variáveis pode ser resolvido, ou pelo menos reduzido a uma variável.

Considere $f(x,y) = g(x,y) = 0$, com $f, g \in K[x,y]$. Podemos ocultar a variável y como coeficientes e pensar em $f, g \in K[y][x]$. Denotando n, m os respectivos graus de f, g na variável x. Então, o resultante $Res_{n,m}(f,g)$ na variável x, denotado por $Res(f,g)_x$ vai ser um polinômio em y, que se anulará em todo y_0 se existir um x_0 tal que $f(x_0, y_0) = g(x_0, y_0) = 0$.

A afirmação acima é dada pelo seguinte resultado, e a prova pode ser encontrado em [5].

Teorema 5: Sejam $f(x,y) = \sum_{i=1}^{n} f_i(y) x^i$, $g(x,y) = \sum_{i=1}^{m} g_i(y) x^i$ polinômios em $K[x,y]$, tal que $f_i, g_i \in K[y]$, com f_n e g_m não nulos. Seja y_0 uma raiz do Resultante $Res(f,g)_x \in K[y]$. Se ocorrer de $f_n(y_0) \neq 0$ ou $g_m(y_0) \neq 0$, existe um $x_0 \in K$ de modo que $f(x_0, y_0) = g(x_0, y_0) = 0$.

Por exemplo, considere $f(x,y) = x^2 + y^2 - 10$, $g(x,y) = x^2 + 2y^2 + xy - 16$. Reescrevemos $f(x,y) = x^2 + 0x + (y^2 - 10)$, $g(x,y) = x^2 + yx + (2y^2 - 16)$. Então o Resultante de f, g é igual $Res_{2,2}(f,g)_x = det \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & y & 1 \\ y^2 - 10 & 0 & 2y^2 - 16 & y \\ 0 & y^2 - 10 & 0 & 2y^2 - 16 \end{bmatrix}$

$Res_{2,2}(f,g)_x = -22y^2 + 2y^4 + 36 = 2(y + 3)(y - 3)(y^2 - 2)$. Este polinômio em y, tem exatamente quatro raízes $y_0 = -3, 3, \sqrt{2}, -\sqrt{2}$. Retomamos o sistema inicial:

$$f(x,y) = x^2 + y^2 - 10 = 0$$

$$g(x,y) = x^2 + 2y^2 + xy - 16 = 0$$

e fazendo $f(x,y) - g(x,y) = 0$, obtemos: $y^2 - 10 - 2y^2 - xy + 16 = 0 \longrightarrow -y^2 - xy + 6 = 0 \longrightarrow x = 6 - y^2 y$. Então substituindo as raízes $y_0 = -3, 3, \sqrt{2}, -\sqrt{2}$, temos $x_0 = 1, -1, 2\sqrt{2}, -2\sqrt{2}$.

A generalização do Teorema 5, pode ser vista em [5]. Para esse caso, considere o seguinte exemplo.

Sejam

$$F_1 = x_1^2 + x_2^2 - 10x_0^2 = 0$$

$$F_2 = x_1^2 + x_1 x_2 + 2x_2^2 - 16x_0^2 = 0.$$

Veremos a seguir, pelo Teorema de Bezout, que será a próxima aplicação dos Resultantes, que o sistema acima tem 4 soluções, ou seja, grau$(F_1)\times$ grau(F_2).

Para o caso geral, introduzimos uma nova equação $F_0 = u_0 x_0 + u_1 x_1 + u_2 x_2 = 0$, para calcularmos o Resultante. Assim calculando o $Res_{1,2,2}(F_0, F_1, F_2) = (2u_0^4 + 16u_1^4 + 36u_2^4 - 80u_1^3 u_2 + 120 u_1 u_2^3 - 18u_0^2 u_1^2 - 22u_0^2 u_2^2 + 52u_1^2 u_2^2 - 4u_0^2 u_1 u_2)$.

Fatorando este polinômio, usando o Maple podemos reescrever o Resultante como: $Res_{1,2,2}(F_0, F_1, F_2) = (u_0 + u_1 - 3u_2)(u_0 - u_1 + 3u_2)(u_0^2 - 8u_1^2 - 2u_2^2 - 8u_1 u_2) = (u_0 + u_1 - 3u_2)(u_0 - u_1 + 3u_2)(u_0 + 2\sqrt{2}u_1 + \sqrt{2}u_2)(u_0 - 2\sqrt{2}u_1 - \sqrt{2}u_2)$.

Os coeficientes dos fatores lineares do $Res_{1,2,2}(F_0, F_1, F_2)$ são dados por 4 pontos: $(1, 1, -3)(1, -1, 3)(1, 2\sqrt{2}, \sqrt{2})(1, -2\sqrt{2}, -\sqrt{2})$. Estes 4 pontos são as soluções de $F_1 = F_2 = 0$.

Podemos verificar que o problema de determinar as soluções de um sistema de equações polinomiais via Resultantes, é transferido para o problema de fatoração de polinômios, que é por si só uma tarefa complicada, principalmente no caso de muitas variáveis.

Nosso próximo passo, é fazer mais uma aplicação dos Resultantes. Vamos usar a teoria dos Resultantes, para provar um caso particular do Teorema de Bezout para curvas no plano xy, bastante conhecido da Geometria Algébrica.

De acordo com [5], a solução de um sistema de equações lineares, foi desenvolvida na China, cerca de 200 ac, e a aplicação do método de eliminar a variavél x de dois polinômios foi desenvolvido no século 12. Estas técnicas foram utilizadas na Europa por matemáticos somente no século 17, motivados pela geometria de curvas e equações algébricas. O estudo de curvas e seus pontos de intersecção cobriu naturalmente o estudo de polinômios e suas raízes comuns.

Em 1620 Descartes descobriu algo mais geral: um método de resolver qualquer equação de grau 3 ou 4 através de intersecções de curvas de grau 2, como uma parábola e um círculo. Na verdade não é fácil encontrar uma construção satisfatória para equações de elevado grau.

Na procura de uma construção geral, matemáticos têm casualmente assumido que uma curva de grau m intercepta uma curva de grau n em mn pontos. A primeira afirmação deste princípio, que tornou-se conhecido como o Teorema de Bezout, foi feito por Newton.

Primeiramente considere a intersecção de uma parábola com uma elipse. Sejam $y = x^2$ e $x^2 + 4(y - \lambda)^2 = 4$, onde λ é um parâmetro que podemos variar. Tomando $\lambda = 2$, obtemos a seguinte figura:

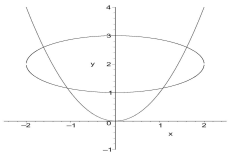

Figura 2: $\lambda = 2$.

Sobre o corpo dos reais, obtemos números diferentes na intersecção. Isto fica claro, se observarmos a figura, o parâmetro λ determina o deslocamento da elipse no eixo y. Assim tomando $\lambda \leq -2$, implica que as curvas têm intersecção vazia. Isto justifica que existem valores de λ para os quais as curvas não têm ponto em comum.

O que é mais interessante é trabalhar sobre o corpo dos complexos, no qual obtemos 4 pontos na intersecção, ou seja 4 = grau(parábola)× grau(elipse).

É importante lembrar que, que agora estamos trabalhando com curvas C e D, no plano, cujos polinômios que representam estas curvas são variedades no plano projetivo. Além disso, esses polinômios não têm um fator irredutível em comum. Pois se caso tivessem tal fator comum, implicaria que essas curvas teriam infinitos pontos em comum.

Agora precisamos de um resultado, que afirma que a intersecção de duas curvas C e D, sem fatores irredutíveis em comum, seja finita.

Teorema 6: Sejam C e D curvas no plano xy, sem fatores irredutíveis em comum. Se os graus das equações C e D são m e n respectivamente, então $C \cap D$ é finita e tem no máximo mn pontos.

A prova do Teorema acima pode ser vista em [5].

Agora que temos um critério para $C \cap D$ ser finito, o próximo passo é definir a multiplicidade de um ponto $p \in C \cap D$. Antes de definir a multiplicidade de um ponto de uma intersecção, retornamos ao exemplo da intersecção da parábola $y = x^2$ com uma elipse $x^2 + 4(y - \lambda)^2 = 4$.

Tomando $\lambda = 1$, observe a figura abaixo

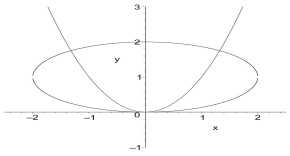

Figura 3: $\lambda = 1$.

Vemos facilmente que existe somente 3 pontos na intersecção. Isto é verdadeiro, mesmo que trabalhando sobre o corpo dos complexos. Mas isso não contraria o Teorema de Bezout? Na verdade não. Pois o ponto da origem (0, 0), que pertence a intersecção da parábola com a elipse, tem multiplicidade 2. E os outros 2

pontos da intersecção têm cada um multiplicidade 1. Assim se adicionarmos as multiplicidades dos pontos obtemos que o número total na intersecção é 4, que está de acordo com o Teorema de Bezout.

A importância deste exemplo, implica na seguinte definição. Dado $p = (u, v, w) \in C \cap D$, a multiplicidade $I_p(C, D)$ é definida como o expoente de $vx - uy$ da fatoração do $Res(f, g)_z$.

Considere os seguintes polinômios em $C[x, y, z]$: $f = x^3 + y^3 - 2xyz$, $g = 2x^3 - 4x^2y + 3xy^2 + y^3 - 2y^2z$. Estes polinômios definem curvas cúbicas $C = V(f)$ e $D = V(g)$ em $P^2(C)$, ou seja, no plano projetivo.

Para verificar a intersecção destas curvas, primeiramente vamos calcular o resultante na variável z : $Res(f, g)_z = -2y(x - y)^3(2x + y)$. Assim para determinarmos os pontos de $C \cap D$, basta fazer $Res(f, g)_z = 0$, isto é equivalente $y = 0$, $x - y = 0$ ou $2x + y = 0$. Deste modo $C \cap D$ consiste em 3 pontos: $p = (0, 0, 1)$, $q = (1, 1, 1)$, $r = (4/7, -8/7, 1)$. Isto mostra em particular que C e D não têm componentes em comum.

Como $(0, 0, 1) \in C$, pois é um ponto de intersecção, fica difícil de determinar sua multiplicidade. Então devemos fazer uma mudança de coordenadas. Para isso considere:

$$(0, 1, 0) \notin C \cup D \cup L_{pq} \cup L_{pr} \cup L_{qr},$$

onde, L_{ij} é a reta que une os pontos i e j. Agora devemos encontrar uma transformação A, de modo que a mudança de coordenadas satisfaça $A(0, 1, 0) = (0, 0, 1)$. Isto não é difícil de fazer, seja $A(x, y, z) = (z, x, y)$.

Então $(0, 1, 0) \notin A(C) \cup A(D) \cup L_{A(p)A(q)} \cup L_{A(p)A(r)} \cup L_{A(q)A(r)}$. Para encontrar a equação que define $A(C)$, note que $(u, v, w) \in A(C) \Leftrightarrow A^{-1}(u, v, w) \in C \Leftrightarrow f(A^{-1}(u, v, w)) = 0$.

Deste modo, $A(C)$ é definida pela equação $f \circ A^{-1}(x, y, z) = f(y, z, x) = 0$, e de forma análoga, $A(D) = g(y, z, x) = 0$.

Assim o $Res(f(y, z, x), g(y, z, x))$ determina as multiplicidades para $A(p) = (1, 0, 0)$, $A(q) = (1, 1, 1)$ e $A(r) = (1, 4/7, -8/7)$. Dessa forma, o Resultante é $Res(f(y, z, x), g(y, z, x))_z = 8y^5(x - y)^3(4x - 7y)$.

Logo as multiplicidades dos pontos p, q, e r são $I_p(C, D) = 5$, $I_q(C, D) = 3$, $I_r(C, D) = 1$, que está de acordo com o Teorema da Bezout.

Teorema de Bezout: Sejam C e D curvas em $P^2(C)$ sem componentes em comum, e sejam m e n os graus de suas equações, respectivamente. Então

$$\sum_{p \in C \cap D} I_p(C, D) = mn,$$

onde $I_p(C, D)$ é a multiplicidade do ponto $p \in C \cap D$.

A prova desse resultado, pode ser encontrada em [5].

Referências

[1] Gao, S. Factoring multivariate polynomials via partial differential equations. Mathematics of Computation (72)- 2003, 801-822.

[2] Hoppen,C. Uma Generalização do Algoritmo de Gao para a fatoração de Polinômios. Dissertação de Mestrado-PPG Matemática Aplicada- UFRGS- http: www.biblioteca.ufrgs.br/bibliotecadigital/, 2004.

[3] KALTOFEN, E. Polinomial factorization 1982-1986, vol.125 of Lecture Notes in Pure and Applied Mathematics. Marcel Dekker, Inc, 1990 pp. 285-309.

[4] KALTOFEN, E. Polinomial factorization 1987-1991, vol.583 of Lecture Notes in Computer Science. Springer Verlag, 1992 pp. 294-313.

[5] Tura,F. Equações Polinomiais, Resultantes, e o Teorema de Bezout. Dissertação de Mestrado-PPG Matemática Aplicada- UFRGS- http: www.biblioteca.ufrgs.br/bibliotecadigital/, 2006.