Cálculo da base de Gröbner e o problema de pertinência

André Luis & Patrícia Borges

Instituto de Ciências Exatas e Naturais do Pontal/ UFU

andre.tomaz@ufu.br & patriciabs@ufu.br

RESUMO

A teoria das bases de Gröbner é uma ferramenta fundamental na álgebra polinomial, respondendo a muitas questões importantes da álgebra comutativa, como por exemplo o problema da pertinência a um ideal. Este trabalho tem como objetivo calcular a base de Gröbner de um ideal I do anel de polinômios em várias variáveis $K[x_1,\ldots,x_n]$. Posteriormente utilizaremos a base assim construída para verificar se um dado polinômio g pertence ou não ao ideal I. Para tanto, utilizaremos dois algoritmos, um para dividir polinômios em várias variáveis e outro para calcular a base de Gröbner.

ALGORITMO DE DIVISÃO EM MAIS DE UMA VARIÁVEL.

Dados polinômios f e $g_1,\ldots,g_s$ de $K[x_1,\ldots,x_n]$, ordenados sob uma ordem monomial $>$, o algoritmo tem como saída polinômios $q_1,\ldots,q_s$ e r tais que $f = q_1g_1+\cdots+q_sg_s+r$ e $r=0$, ou nenhum monômio de r é divisível pelos termos iniciais $in(g_1),\ldots,in(g_s)$.

Etapa 1: Inicializa $F=f, Q_1=\cdots=Q_s=0$ e $R=0$.

Etapa 2: Enquanto $F\neq 0$, verifique se existe algum inteiro i entre 1 e s para o qual $in(g_i)$ divide $in(f)$. Se existir escolha j como sendo o menor deles e faça

$$Q_j = Q_j + \frac{in(F)}{in(g_j)};\ \ F = F - \frac{in(F)}{in(g_j)}g_j \ e\ R=R,$$

deixando as demais variáveis inalteradas, se tal i não existir, faça

$$F = F - in(f) \text{ e } R = R + in(f),$$

deixando as demais variáveis inalteradas.

Etapa 3: Imprima o resto é R e os quocientes são $Q_1,\ldots,Q_s$.

BASE DE GRÖBNER

Dizemos que um subconjunto finito $G\subset I$ é uma base de Gröbner para I se $in(I)$ for gerado por $in(g)$ para cada $g\in G$. Define-se o S-polinômio de g_1 e g_2 como

$$S(g_1,g_2) = \frac{in(g_2)}{\delta}g_1 - \frac{in(g_1)}{\delta}g_2$$

onde

$$\delta = mdc(in(g_1), in(g_2)).$$

ALGORITMO DE BUCHBERGER.

Seja $K[x_1,\ldots,x_n]$ um anel de polinômios munido de uma ordem monomial $>$. Dado um subconjunto finito $S\subset K[x_1,\ldots,x_n]$, o algoritmo tem como saída uma base de Gröbner do ideal gerado pelos polinômios de S no anel $K[x_1,\ldots,x_n]$.

Etapa 1: Inicializa $G=S$ e $P=\{(g,g'): g,g'\in G \text{ e } g\neq g'\}$.

Etapa 2: Enquanto $P\neq\emptyset$, repita:

- escolha $(g,g')\in P$;
- remova (g,g') de P;
- calcule o resto r da divisão do S-polinômio $S(g,g')$ por G;
- se $r\neq 0$, então:
  - ◇ acrescente r a G;
  - ◇ acrescente a P os pares da forma (h,r) para cada $h\in G$;

Etapa 3: Pare e imprima os elementos de G.

Seja G um subconjunto e f um elemento de $K[x_1,\ldots,x_n]$, então $R_G(f)$ denotará o resto da divisão de f por G.

Usando a notação de multíndices, a ordem grlex pode ser definida da seguinte maneira:

$$x^\alpha >_{grlex} x^\beta \text{ se } \begin{cases} |\alpha| > |\beta| \\ ou \\ |\alpha| = |\beta| \text{ e coeficiente não-nulo mais à direita} \\ \text{de } \alpha-\beta \text{ é negativo.}\end{cases}$$

Agora executaremos o algoritmo de Buchberger para calcular a base de Gröbner para o ideal $\langle x^2y-1, xy^2-x\rangle$ com a ordem grlex.

Passo 1. Neste passo apenas inicializaremos as variáveis do algoritmo:

$$G=\{x^2y-1, xy^2-x\}\ e\ P=\{(x^2y-1, xy^2-x)\}$$

Passo 2. Calculando o primeiro S-polinômio, temos:

$$S(x^2y-1, xy^2-x) = y(x^2y-1)-(x)xy^2-x = x^2-y$$

O termo inicial deste S-polinômio tem grau menor que os graus dos elementos de G, de modo que

$$R_G(S(x^2y-1, xy^2-x)) = x^2-y$$

Ao final deste passo teremos que

$$G=\{x^2y-1, xy^2-x, x^2-y\}\ e\ P=\{(x^2y-1, x^2-y), (xy^2-x, x^2-y)\}$$

Passo 3. Calculando o S-polinômio do par (x^2y-1, x^2-y), obtemos:

$$S(x^2y-1, x^2-y) = (x^2y-1)-(y)(x^2-y) = y^2-1$$

O termo inicial deste S-polinômio tem grau menor que os graus dos elementos de G, de modo que

$$R_G(S(x^2y-1, x^2-y)) = y^2-1$$

Ao final deste passo teremos que

$$G=\{x^2y-1, xy^2-x, x^2-y, y^2-1\}$$

$$P=\{(x^2y-1, y^2-1), (xy^2-x, y^2-1), (x^2-y, y^2-1)\}$$

Passo 4. Calculando o S-polinômio do par (x^2y-1, y^2-1), obtemos:

$$S(x^2y-1, y^2-1) = y(x^2y-1)-x^2(x^2-y) = x^2-y$$

Dividindo x^2-y por $G=\{x^2y-1, xy^2-x, x^2-y, y^2-1\}$, obtemos o resto 0. Ao final deste passo teremos que

$$G=\{x^2y-1, xy^2-x, x^2-y, y^2-1\}$$

$$P=\{(xy^2-x, y^2-1), (x^2-y, y^2-1)\}$$

Passo 5. Calculando o S-polinômio do par (xy^2-x, y^2-1), obtemos:

$$S(xy^2-x, y^2-1) = xy^2-x-x(y^2-1) = xy^2-x-xy^2+x = 0$$

Dividindo 0 por $G=\{x^2y-1, xy^2-x, x^2-y, y^2-1\}$, obtemos o resto 0. Ao final deste passo teremos que

$$G=\{x^2y-1, xy^2-x, x^2-y, y^2-1\}\ e\ P=\{(x^2-y, y^2-1)\}$$

Passo 6. Calculando o S-polinômio do par (xy^2-x, y^2-1), obtemos:

$$S(x^2-y, y^2-1) = x^2-y-(y^2-1) = x^2-y^2-y+1$$

Dividindo x^2-y^2-y+1 por $G=\{x^2y-1, xy^2-x, x^2-y, y^2-1\}$, obtemos o resto 0. Ao final deste passo teremos que

$$G=\{x^2y-1, xy^2-x, x^2-y, y^2-1\}\ e\ P=\emptyset$$

Passo 7. Como $P=\emptyset$ então a base de Gröbner é

$$G=\{x^2y-1, xy^2-x, x^2-y, y^2-1\}.$$

O PROBLEMA DE PERTINÊNCIA

Seja I um ideal de $K[x_1,\ldots,x_n]$ e G uma base de Gröbner para I. Então, $f\in I$ se e somente se $R_G(f)=0$.

Por este critério fica fácil decidir se um polinômio g pertence ou não ao ideal I, basta dividir o polinômio pela base de Gröbner de I e depois avaliar se o resto anula ou não. Iremos agora utilizar este critério para decidir se o polinômio $x^3y^2+x^2y-y^3+1$ pertence ao ideal $\langle x^2y-1, xy^2-x\rangle$ de $K[x,y]$ cuja base de Gröbner foi calculada acima e é $G=\{x^2y-1, xy^2-x, x^2-y, y^2-1\}$. Utilizaremos o algoritmo da divisão de polinômios em várias variáveis com a orgem grlex.

$$\begin{array}{c|l}
x^3y^2+x^2y-y^3+1 & x^2y-1 \\
x^2y+xy-y^3+1 & xy^2-x \\
xy-y^3+2 & x^2-y \\
-y^3+2 & y^2-1 \\ \cline{2-2}
-y+2 & Q_1 = xy+1 \\
2 & Q_2 = 0 \\
0 & Q_3 = 0 \\
 & Q_4 = -y \\
 & R = xy-y+2
\end{array}$$

Como o resto R da divisão do polinômio $f=x^3y^2+x^2y-y^3+1$ pela base de Gröbner $G=\{x^2y-1, xy^2-x, x^2-y, y^2-1\}$ é diferente de zero então o polinômio f não pertence ao ideal de $K[x,y]$ gerado por x^2y-1 e xy^2-x.

CONCLUSÃO

Ao executar o algoritmo de Buchberger fomos capazes de perceber que dependendo da ordem monomial escolhida a quantidade de passos executados para se calcular a base de Gröbner pode aumentar e muito. Além disso, notamos que a ordem monomial grlex é a que converge mais rápido para a base procurada. Apesar da quantidade de passos do algoritmo sua utilização sempre nos retorna um conjunto finito que gera um ideal e também pode ser utilizado para resolver o problema de pertinência.

REFERÊNCIAS

S. C. Coutinho. *Polinômios e computação Algébrica*. IMPA, 1st edition, 2012.