APRIMORANDO A EFICIÊNCIA DO ALGORITMO DE BUCHBERGER PARA BASES DE GRÖBNER

1.Eder Alejandro Rodriguez Lopez & 2.Elkin Oveimar Quintero Vanegas

1.Pós graduação em Matematica - PPG-UFAM (ICE) – Bolsista CAPES

2.Professor Doutor na Universidade Federal do Amazonas - UFAM(ICE)

1.edarodriguezl@correo.udistrital.edu.co

2.eoquinterov@ufam.edu.br

Instituto de Matemática Pura e Aplicada

Introdução

No contexto da álgebra clássica, suponha primeiro que nos são dados polinômios univariados $f, g_1, ..., g_m \in K[x]$ com K um corpo, ¿f está no ideal gerado por g_i? Isto é $f \in I = \langle g_1, ..., g_m \rangle$. Deixe $gcd(g_i) = g$ então faça uma divisão de f por g. Existem $q, r \in K[x]$, com o grau r menor que o grau de g tal que $f = qg + r \implies f \in I \iff r = 0$, obtém-se um polinômio que satisfaz $f = qg$, ou seja, q é o quociente de divisão, A teoria da base de Gröbner generaliza essas ideias para polinômios multivariados. Mas esta divisão tem duas dificuldades. Uma ordenação dos termos é necessária para substituir a ordenação natural dos termos univariados, termos por expoentes ascendentes. A outra dificuldade, não haverá um único gerador do ideal dado em geral, isto é $f = q_1g_1 + \cdots + q_ng_n + r$. Sim $f \in I = \langle g_1, ..., g_m \rangle \implies r = 0$?. Isso não é verdade em geral. O teorema chave (algoritmo de Buchberger) que faz a teoria das bases de Gröbner funcionar afirma que é possível generalizar o algoritmo euclidiano para um ”pré-processamento”do conjunto dado $\{g_1, ..., g_m\}$ de tal forma que obtém-se outro conjunto que ainda gera o mesmo ideal e tem a propriedade desejada de produzir zero ”resto”para cada ”divisão”com um membro do ideal como ”dividendo”. Bases ideais com esta propriedade são chamadas de bases de Gröbner. [3].

Resultados

Definição 1. *Monômio:* $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$. *Polinômio:* $f = \sum a_\alpha x^\alpha$ *com* $a_\alpha \in K$,

Definição 2 (ordem de um Monômio)**.** *Denotamos por* $T(x_1, ..., x_n)$ *ou simplesmente por* T*, o conjunto de todos os Monômios no* $K[\bar{x}] = K[x_1, ..., x_n]$*. [3]. A ordem de um Monômio é uma ordem linear (ordem total) em* T *que satisfaz as seguintes condições.*

a. $1 \leq t$ *para todos os* $t \in T$,

b. $t_1 \leq t_2$ *implica* $t_1 \cdot s \leq t_2 \cdot s$, $s, t_1, t_2 \in T$.

Exemplo 1. $x^\alpha = x_1^{d_1} \cdots x_n^{d_n} \leq x_1^{e_1} \cdots x_n^{e_n} = x^\beta$ *se as seguintes condições forem satisfeitas:* $\alpha = (d_1, ..., d_n) = (e_1, ..., e_n) = \beta$*, ou existe* $1 \leq i \leq n$ *com* $d_j = e_j$ *para* $1 \leq j \leq i - 1$ *e* $d_i < e_i$*. Esse ordenamento de monômios é chamado de ordem lexicográfica ou ordem léxica em* T*. [3]*

Teorema 1 (Algoritmo de divisão generalizada)**.** *Algoritmo em* $K[\bar{x}]$ *fixar qualquer ordem monomial* $\leq$ *em* $K[\bar{x}]$ *e deixe* $F = (f_1, ..., f_s)$ *uma tupla ordenada de polinômios em* $K[\bar{x}]$*. Então todo* $f \in K[\bar{x}]$ *pode ser escrito como*

$$f = a_1f_1 + ... + a_sf_s + r, \text{ com } a_i, r \in K[\bar{x}],$$

$r = 0$ *ou* r *é uma combinação linear de monômios, nenhum dos quais é divisível por* $LT(f_1), ..., LT(f_s)$ *onde* $LT(f_i)$ *é o termo principal de* f_i*. Chamaremos* r *um resto de* f *a divisão por* F*. a notação* $r = \bar{f}^F$ *será usada para um resto na divisão por* F*. [1]*

Definição 3 (**Base de Gröbner**)**.** *Defina uma ordem monomial. Um subconjunto finito* $G = \{g_1, ..., g_t\}$ *de um* I *ideal é uma base de Gröbner se*

$$\langle LT(I) \rangle = \langle LT(g_1), ..., LT(g_t) \rangle.$$

Denotamos por $LT(I)$ *o conjunto de termos principais dos elementos de* I*. [1]*

Definição 4 (S-polinômio)**.** *Seja* $f, g \in K[\bar{x}]$ *diferente de zero. definir uma ordem monomial e deixe* $LT(f) = cx^\alpha$ *y* $LT(g) = dx^\beta$*, onde* $c, d \in K$*. Seja* x^γ *o mínimo múltiplo comum de* x^α *e* x^β *. O* S*-polinômio de* f *e* g*, denotado* $S(f, g)$*, é o polinômio [1]*

$$S(f, g) = \frac{x^\gamma}{LT(f)}f + \frac{x^\gamma}{LT(g)}g.$$

Teorema 2 (Critério de Buchberger)**.** *Um conjunto finito* $G = \{g_1, ..., g_t\} \subset I$ *é uma base de Gröbner de* I *se e somente se* $\overline{S(g_i, g_j)}^G = 0$ *para todos os pares* $i \neq j$*. [2]*

A complexidade combinatória do algoritmo Buchberger pode ser reduzida testando certos S-polinômios que não precisam ser considerados. Uma abordagem computacional faz uso de

Lema 1 (PRIMEIRO CRITÉRIO DE BUCHBERGER)**.** *Seja* $f, g \in K[\bar{X}]$ *com termos principais disjuntos. Então* $S(f, g) \xrightarrow[\{f,g\}]{*} 0$*, onde* $s, t \in T$ *disjuntos se* s *e* t *não tiverem variável em comum; em outras palavras* $gcd(s, t) = 1$*. [3]*

Definição 5 (t-representação)**.** *Seja* F *um subconjunto finito de* $K[\bar{x}]$*,* $0 \neq f \in K[\bar{x}]$ *e* $t \in T$*. suponha* $f = \sum_{i=1}^k m_if_i$*. Com monômios* $0 \neq m_i = a_it_i \in K[\bar{x}]$ *e* $f_i \in F$ *não necessariamente diferente em pares* $(1 \leq i \leq k)$ *é chamado* t*-representação de* f *em relação a* F *se* $max\{LT(m_if_i) \mid 1 \leq i \leq k\} \leq t$*. [3]*

Teorema 3 (SEGUNDO CRITÉRIO DE BUCHBERGER)**.** *Seja* F *um subconjunto finito de* $K[\bar{x}]$ *e* $g_1, p, g_2 \in K[\bar{x}]$ *tal que o seguinte seja válido: [3]*

1. $LT(p) \mid lcm(LT(g_1), LT(g_2))$*, y*

2. $S(g_i, p)$ *tem uma* t_i*-representação em relação a* F *com*

$$t_i < lcm(LT(g_i), LT(p)) \text{ para } i = 1, 2.$$

Entonces el S*-polinomio* $S(g_1, g_2)$ *tiene* t*-representación con respecto a* F *para algún* $t < lcm(HT(g_1), HT(g_2))$

Teorema 4 (**GRÖBNERNEW1**)**.** *Seja* F *um subconjunto finito de* $K[\bar{x}]$*, calcula uma base de Gröbner* G *em* $K[\bar{x}]$ *tal que* $\langle G \rangle = \langle F \rangle$*. O algoritmo elimina* S*-polinômios supérfluos de acordo com os critérios de Buchberger. [3]*

Specification: $G \leftarrow$ GRÖBNERNEW1(F)
Construction of a Gröbner basis G for Id(F)
Given: $F \equiv$ a finite subset of $K[\underline{X}]$
Find: $G \equiv$ a finite subset of $K[\underline{X}]$ such that G is a Gröbner basis in $K[\underline{X}]$ with Id(G) = Id(F)
begin
$G \leftarrow$ REDUCTION(F)
$B \leftarrow \{\{g_1, g_2\} \mid g_1, g_2 \in G$ with non-disjoint head terms, $g_1 \neq g_2\}$
create a matrix M with a Boolean entry $M(g_1, g_2)$ for each $\{g_1, g_2\}$, where $g_1, g_2 \in G$ with $g_1 \neq g_2$
for all $\{g_1, g_2\}$ with $g_1, g_2 \in G$ and $g_1 \neq g_2$ **do**
  if $\{g_1, g_2\} \in B$ **then** $M(g_1, g_2) \leftarrow$ **false**
  else $M(g_1, g_2) \leftarrow$ **true end**
end
while $B \neq \emptyset$ **do**
  select $\{g_1, g_2\}$ from B with lcm(HT(g_1), HT(g_2)) minimal among all pairs in B
  $B \leftarrow B \setminus \{\{g_1, g_2\}\}$
  $M(g_1, g_2) \leftarrow$ **true**
  if there does not exist $p \in G$ with:
    HT(p) | lcm(HT(g_1), HT(g_2)) and
    $M(g_1, p) = M(p, g_2) =$ **true then**
    $h \leftarrow$ spol(g_1, g_2)
    $h_0 \leftarrow$ some normal form of h modulo G
    if $h_0 \neq 0$ **then**
      for all $g \in G$ **do**
        enlarge M by an entry for $\{h_0, g\}$
        if HT(g), HT(h_0) disjoint **then**
          $M(g, h_0) \leftarrow$ **true**
        else
          $B \leftarrow B \cup \{\{g, h_0\}\}$
          $M(g, h_0) \leftarrow$ **false**
        end
      end
      $G \leftarrow G \cup \{h_0\}$
    end
  end
end
end
end GRÖBNERNEW1

Referências

[1] A. Cox David, “Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra [3rd ed]”, Springer Science, New York, 2007.

[2] A. Cox David, “Using Algebraic Geometry [2 ed.]”, Springer-Verlag, New York, 2005.

[3] B. Thomas, “Gröbner Bases - A Computational Approach to Commutative Algebra”, Springer Science, New York, 1993.