Introdução a Teoria de Bases de Gröbner

Profa Dra: Diane Castonguay

INF-UFG

Setembro de 2007

Sumário

Motivação

O problema da pertinência em Subespaços

O problema de pertinência em $K[x]$.

O problema de pertinência em $K[x_1, \ldots, x_n]$

O problema de pertinência em $K<x_1, \ldots, x_n>$

Referência Principal

Este mini curso foi elaborado a partir da dissertação de mestrado de Alexey Antônio Villas Bôas.[Villas Bôas, 2005]

Motivação

Problema da pertinência para ideal de polinômios.

Dado um polinômio, decida se ele pertence ou não a um ideal do anel de polinômios.

Parece facil?

Motivação

Problema da pertinência para ideal de polinômios.
Dado um polinômio, decida se ele pertence ou não a um ideal do anel de polinômios.
Parece facil?

Motivação

Problema da pertinência para ideal de polinômios.
Dado um polinômio, decida se ele pertence ou não a um ideal do anel de polinômios.
Parece facil?

Exemplo

- Consideremos o anel dos polinômios em três variaveis comutativas $K[x_1, x_2, x_3]$ e o ideal gerado por

$$\{f_1 := x^2 - y^3 z, f_2 := x^2 - z^2, f_3 := y^2 z - y\}$$

Será que $f := xy - xz^3$ pertence a este ideal?

- Consideremos o anel dos polinômios em uma variavel $K[x]$ e o ideal gerado por

$$\{f_1 := x^3 - 3x + 2, f_2 := x^4 - 1, f_3 := x^6 - 1\}$$

Será que $f := x^3 + 4x^2 + 3x - 7$ pertence a este ideal?

Exemplo

- Consideremos o anel dos polinômios em três variaveis comutativas $K[x_1, x_2, x_3]$ e o ideal gerado por

$$\{f_1 := x^2 - y^3 z, f_2 := x^2 - z^2, f_3 := y^2 z - y\}$$

Será que $f := xy - xz^3$ pertence a este ideal?

- Consideremos o anel dos polinômios em uma variavel $K[x]$ e o ideal gerado por

$$\{f_1 := x^3 - 3x + 2, f_2 := x^4 - 1, f_3 := x^6 - 1\}$$

Será que $f := x^3 + 4x^2 + 3x - 7$ pertence a este ideal?

Problemas

- **Problema da pertinência para ideal de polinômios**
  Dado $f \in K[x_1, \ldots, x_n]$ e um conjunto gerador para um ideal I de $K[x_1, \ldots, x_n]$, decida se f pertence a I.

- **Problema da igualdade em quocientes do anel de polinômios**
  Dado $f, g \in K[x_1, \ldots, x_n]$ e um conjunto gerador para um ideal I de $K[x_1, \ldots, x_n]$, decida se $f + I = g + I$.

Problemas

- **Problema da pertinência para ideal de polinômios**
  Dado $f \in K[x_1, \ldots, x_n]$ e um conjunto gerador para um ideal I de $K[x_1, \ldots, x_n]$, decida se f pertence a I.

- **Problema da igualdade em quocientes do anel de polinômios**
  Dado $f, g \in K[x_1, \ldots, x_n]$ e um conjunto gerador para um ideal I de $K[x_1, \ldots, x_n]$, decida se $f + I = g + I$.

Para resolver estes problemas, precisamos das bases de Gröbner.

Estas ideias foram introducidas por Buchberger na sua tese de doutorado em 1965 [Buchberger, 1965] e desde então desempenham um papel muito importante na área de Álgebra Computacional.

Além do mas, muitos sistemas de computação algébrica incluem pacotes para lidar com Bases de Gröbner (comutativa). Entre eles, podemos citar: Axiom, Maple, Mathematica, CoCoA e Reduce.

Para resolver estes problemas, precisamos das bases de Gröbner.

Estas ideias foram introducidas por Buchberger na sua tese de doutorado em 1965 [Buchberger, 1965] e desde então desempenham um papel muito importante na área de Álgebra Computacional.

Além do mas, muitos sistemas de computação algébrica incluem pacotes para lidar com Bases de Gröbner (comutativa). Entre eles, podemos citar: Axiom, Maple, Mathematica, CoCoA e Reduce.

Para resolver estes problemas, precisamos das bases de Gröbner.

Estas ideias foram introducidas por Buchberger na sua tese de doutorado em 1965 [Buchberger, 1965] e desde então desempenham um papel muito importante na área de Álgebra Computacional.

Além do mas, muitos sistemas de computação algébrica incluem pacotes para lidar com Bases de Gröbner (comutativa). Entre eles, podemos citar: Axiom, Maple, Mathematica, CoCoA e Reduce.

Introduciremos dois algoritmos que são as chaves da teoria (no caso comutativo).

- **Algoritmo da Divisao**
  Este algoritmo decide da pertinência de um elemento num ideal, dados o elemento e uma Base de Gröbner para o ideal em questão.

- **Algoritmo de Buchberger**
  Constrói uma Base de Gröbner para um ideal, a partir de um conjunto finito de geradores.

Introduciremos dois algoritmos que são as chaves da teoria (no caso comutativo).

- **Algoritmo da Divisao**
  Este algoritmo decide da pertinência de um elemento num ideal, dados o elemento e uma Base de Gröbner para o ideal em questão.

- **Algoritmo de Buchberger**
  Constrói uma Base de Gröbner para um ideal, a partir de um conjunto finito de geradores.

Introduciremos dois algoritmos que são as chaves da teoria (no caso comutativo).

- **Algoritmo da Divisao**
  Este algoritmo decide da pertinência de um elemento num ideal, dados o elemento e uma Base de Gröbner para o ideal em questão.

- **Algoritmo de Buchberger**
  Constrói uma Base de Gröbner para um ideal, a partir de um conjunto finito de geradores.

Sumário

Motivação

O problema da pertinência em Subespaços
Algoritmo - Redução Incompleta de Gauss

O problema de pertinência em $K[x]$.

O problema de pertinência em $K[x_1, \ldots, x_n]$

O problema de pertinência em $K<x_1, \ldots, x_n>$

O problema da pertinência em Subespaços

Consideremos um corpo K, $V = K^n$ e fixamos uma base ordenada canônica de V.

Problema da pertinência.
Dado v um vetor de V e $B = \{b_1, \ldots, b_m\}$ uma base ordenada de um subespaço W de V, Decida se v pertence a W.
Consideremos estes elementos como vetores (coordenadas na base canônica de V.)

O problema da pertinência em Subespaços

Consideremos um corpo K, $V = K^n$ e fixamos uma base ordenada canônica de V.

Problema da pertinência.
Dado v um vetor de V e $B = \{b_1, \ldots, b_m\}$ uma base ordenada de um subespaço W de V, Decida se v pertence a W.
Consideremos estes elementos como vetores (coordenadas na base canônica de V.)

O problema da pertinência em Subespaços

Consideremos um corpo K, $V = K^n$ e fixamos uma base ordenada canônica de V.

Problema da pertinência.
Dado v um vetor de V e $B = \{b_1, \ldots, b_m\}$ uma base ordenada de um subespaço W de V, Decida se v pertence a W.
Consideremos estes elementos como vetores (coordenadas na base canônica de V.)

O problema da pertinência em Subespaços

Consideremos um corpo K, $V = K^n$ e fixamos uma base ordenada canônica de V.

Problema da pertinência.
Dado v um vetor de V e $B = \{b_1, \ldots, b_m\}$ uma base ordenada de um subespaço W de V, Decida se v pertence a W.
Consideremos estes elementos como vetores (coordenadas na base canônica de V.)

- **Primeira abordagem**:
  Resolver o sistema linear de equações $\alpha_1 b_1 + \ldots + \alpha_m b_m = v$

- **Segunda abordagem**:
  Constrói uma matriz M com $m+1$ linha, onde as m primeiras linhas correspondem aos elementos de B e a ultima linha ao elemento v.
  Aplique o algoritmo de Gauss-Jordan a M.
  Temos que v pertence a W se e somente se a matriz resultante da aplicação de Gauss-Jordan a matriz M tiver uma linha nula.

- **Primeira abordagem**:
  Resolver o sistema linear de equações $\alpha_1 b_1 + \ldots + \alpha_m b_m = v$

- **Segunda abordagem**:
  Constrói uma matriz M com $m+1$ linha, onde as m primeiras linhas correspondem aos elementos de B e a ultima linha ao elemento v.
  Aplique o algoritmo de Gauss-Jordan a M.
  Temos que v pertence a W se e somente se a matriz resultante da aplicação de Gauss-Jordan a matriz M tiver uma linha nula.

- **Primeira abordagem**:
  Resolver o sistema linear de equações $\alpha_1 b_1 + \ldots + \alpha_m b_m = v$

- **Segunda abordagem**:
  Constrói uma matriz M com $m+1$ linha, onde as m primeiras linhas correspondem aos elementos de B e a ultima linha ao elemento v.
  Aplique o algoritmo de Gauss-Jordan a M.
  Temos que v pertence a W se e somente se a matriz resultante da aplicação de Gauss-Jordan a matriz M tiver uma linha nula.

- **Primeira abordagem**:
  Resolver o sistema linear de equações $\alpha_1 b_1 + \ldots + \alpha_m b_m = v$

- **Segunda abordagem**:
  Constrói uma matriz M com $m+1$ linha, onde as m primeiras linhas correspondem aos elementos de B e a ultima linha ao elemento v.
  Aplique o algoritmo de Gauss-Jordan a M.
  Temos que v pertence a W se e somente se a matriz resultante da aplicação de Gauss-Jordan a matriz M tiver uma linha nula.

Terceira Abordagem

Consideramos uma base especial para W.

- Chamamos de **coordenada líder** de um vetor não nulo v (denotada por $\hat{v}$) a menor coordenada não nula de v.
- Uma base G de um subespaço vetorial W é dita uma **Base de Gauss** se ela satisfizer as segunites propriedades:
  - Não existem dois vetores em G com a mesma coordenada líder.
  - Se um vetor não nulo u pertence a W, então existe um elemento g em G tal que $\hat{u} = \hat{g}$.
- Denotaremos por $cl(u)$ o valor da coordenada líder de u.

Terceira Abordagem

Consideramos uma base especial para W.

- Chamamos de **coordenada líder** de um vetor não nulo v (denotada por $\hat{v}$) a menor coordenada não nula de v.
- Uma base G de um subespaço vetorial W é dita uma **Base de Gauss** se ela satisfizer as segunites propriedades:
  - Não existem dois vetores em G com a mesma coordenada líder.
  - Se um vetor não nulo u pertence a W, então existe um elemento g em G tal que $\hat{u} = \hat{g}$.
- Denotaremos por $cl(u)$ o valor da coordenada líder de u.

Terceira Abordagem

Consideramos uma base especial para W.

- Chamamos de **coordenada líder** de um vetor não nulo v (denotada por $\hat{v}$) a menor coordenada não nula de v.
- Uma base G de um subespaço vetorial W é dita uma **Base de Gauss** se ela satisfizer as segunites propriedades:
  - Não existem dois vetores em G com a mesma coordenada líder.
  - Se um vetor não nulo u pertence a W, então existe um elemento g em G tal que $\hat{u} = \hat{g}$.
- Denotaremos por $cl(u)$ o valor da coordenada líder de u.

Terceira Abordagem

Consideramos uma base especial para W.

- Chamamos de **coordenada líder** de um vetor não nulo v (denotada por $\hat{v}$) a menor coordenada não nula de v.
- Uma base G de um subespaço vetorial W é dita uma **Base de Gauss** se ela satisfizer as segunites propriedades:
  - Não existem dois vetores em G com a mesma coordenada líder.
  - Se um vetor não nulo u pertence a W, então existe um elemento g em G tal que $\hat{u} = \hat{g}$.
- Denotaremos por $cl(u)$ o valor da coordenada líder de u.

Algoritmo - Redução Incompleta de Gauss (RedIncGAUSS)

Este algoritmo recebe como entrada uma Base de Gauss G de um subespaço W de V e um vetor v de V. O algoritmo devolve como saida um vetor h.

- RedIncGauss(G,v)
  1. $h \leftarrow v$
  2. **enquanto** existe $g \in G$ tal que $\hat{h} = \hat{g}$ **faça**
  3. $\quad h \leftarrow h - \frac{cl(h)}{cl(g)} g$
  4. **fim-enquanto**
  5. **devolva** h

Algoritmo - Redução Incompleta de Gauss (RedIncGAUSS)

Este algoritmo recebe como entrada uma Base de Gauss G de um subespaço W de V e um vetor v de V. O algoritmo devolve como saida um vetor h.

- RedIncGauss(G,v)
  1. $h \leftarrow v$
  2. **enquanto** existe $g \in G$ tal que $\hat{h} = \hat{g}$ **faça**
  3. $\quad h \leftarrow h - \frac{cl(h)}{cl(g)} g$
  4. **fim-enquanto**
  5. **devolva** h

Teorema

Seja G uma Base de Gauss do subespaço W de V e $v \in V$. O vetor v pertence a W se e somente se $h := RedIncGAUSS(G, v)$ for igual a zero.

Exemplo sobre a importância da base ser de Gauss
Consideremos a base $B := \{(1, 2, 1), (1, 0, 2), (0, 0, 1)\}$ e $v = (1, 0, 3)$

Teorema

Seja G uma Base de Gauss do subespaço W de V e $v \in V$. O vetor v pertence a W se e somente se $h := RedIncGAUSS(G, v)$ for igual a zero.

Exemplo sobre a importância da base ser de Gauss
Consideremos a base $B := \{(1, 2, 1), (1, 0, 2), (0, 0, 1)\}$ e $v = (1, 0, 3)$

Teorema

Seja G uma Base de Gauss do subespaço W de V e $v \in V$. O vetor v pertence a W se e somente se $h := RedIncGAUSS(G, v)$ for igual a zero.

Exemplo sobre a importância da base ser de Gauss
Consideremos a base $B := \{(1, 2, 1), (1, 0, 2), (0, 0, 1)\}$ e $v = (1, 0, 3)$

Sumário

Motivação

O problema da pertinência em Subespaços

O problema de pertinência em $K[x]$.

- Algoritmo da Divisão para polinômios em $K[x]$
- Algoritmo de Euclides

O problema de pertinência em $K[x_1, \ldots, x_n]$

O problema de pertinência em $K<x_1, \ldots, x_n>$

O problema de pertinência em $K[x]$.

Para $n = 1$, o algoritmo de Buchberger se reduz ao Algoritmo de Euclides.

- Fato: Todo ideal de $K[x]$ é principal.

Sejam I um ideal de $K[x]$ e p um polinômio. Sabemos que existe um polinômio h tal que $I =< h >$.
Para saber se p pertence a I, verificaremos se o resto da divisão por h é nulo.

- Dado um conjunto gerador $\{f_1, \ldots, f_n\}$ de I, precisamos encontrar um polinômio h tal que $I =< h >$. Para isto, podemos usar repetidamente o Algoritmo de Euclides para encontrar um máximo divisor comum dos dois polinômios que será o nosso gerador.

O problema de pertinência em $K[x]$.

Para $n = 1$, o algoritmo de Buchberger se reduz ao Algoritmo de Euclides.

- Fato: Todo ideal de $K[x]$ é principal.

Sejam I um ideal de $K[x]$ e p um polinômio. Sabemos que existe um polinômio h tal que $I =< h >$.
Para saber se p pertence a I, verificaremos se o resto da divisão por h é nulo.

- Dado um conjunto gerador $\{f_1, \ldots, f_n\}$ de I, precisamos encontrar um polinômio h tal que $I =< h >$. Para isto, podemos usar repetidamente o Algoritmo de Euclides para encontrar um máximo divisor comum dos dois polinômios que será o nosso gerador.

O problema de pertinência em $K[x]$.

Para $n = 1$, o algoritmo de Buchberger se reduz ao Algoritmo de Euclides.

- Fato: Todo ideal de $K[x]$ é principal.

Sejam I um ideal de $K[x]$ e p um polinômio. Sabemos que existe um polinômio h tal que $I =< h >$.

Para saber se p pertence a I, verificaremos se o resto da divisão por h é nulo.

- Dado um conjunto gerador $\{f_1, \ldots, f_n\}$ de I, precisamos encontrar um polinômio h tal que $I =< h >$. Para isto, podemos usar repetidamente o Algoritmo de Euclides para encontrar um máximo divisor comum dos dois polinômios que será o nosso gerador.

O problema de pertinência em $K[x]$.

Para $n = 1$, o algoritmo de Buchberger se reduz ao Algoritmo de Euclides.

- Fato: Todo ideal de $K[x]$ é principal.

Sejam I um ideal de $K[x]$ e p um polinômio. Sabemos que existe um polinômio h tal que $I =< h >$.
Para saber se p pertence a I, verificaremos se o resto da divisão por h é nulo.

- Dado um conjunto gerador $\{f_1, \ldots, f_n\}$ de I, precisamos encontrar um polinômio h tal que $I =< h >$. Para isto, podemos usar repetidamente o Algoritmo de Euclides para encontrar um máximo divisor comum dos dois polinômios que será o nosso gerador.

O problema de pertinência em $K[x]$.

Para $n = 1$, o algoritmo de Buchberger se reduz ao Algoritmo de Euclides.

- Fato: Todo ideal de $K[x]$ é principal.

Sejam I um ideal de $K[x]$ e p um polinômio. Sabemos que existe um polinômio h tal que $I =< h >$.
Para saber se p pertence a I, verificaremos se o resto da divisão por h é nulo.

- Dado um conjunto gerador $\{f_1, \ldots, f_n\}$ de I, precisamos encontrar um polinômio h tal que $I =< h >$. Para isto, podemos usar repetidamente o Algoritmo de Euclides para encontrar um máximo divisor comum dos dois polinômios que será o nosso gerador.

Algoritmo da Divisão para polinômios em $K[x]$ (DivisãoPoli)

O algoritmo recebe como entrada dois polinômios g e f e devolve o resto da divisão de f por g, ou seja, outro polinômio r que satisfaz $grau(r) < grau(g)$ e $f = ag + r$, para algum polinômio a.

- DivisãoPoli(f,g)
  1. $r \leftarrow f$
  2. **enquanto** $r \neq 0$ e $\hat{g}$ divide $\hat{r}$ **faça**
  3. $\quad r \leftarrow r - \frac{cl(r)\hat{r}}{cl(g)\hat{g}}g$
  4. **fim-enquanto**
  5. **devolva** r

Para um polinômio g, o termo líder é o monômio de maior grau de g.

Exemplos com maior e menor grau

- $f := x^5 - x^2$ e $g := x^2 - x$ e
- $f := x^5 - x^2$ e $g := x^2 - 1$

Algoritmo da Divisão para polinômios em $K[x]$ (DivisãoPoli)

O algoritmo recebe como entrada dois polinômios g e f e devolve o resto da divisão de f por g, ou seja, outro polinômio r que satisfaz $grau(r) < grau(g)$ e $f = ag + r$, para algum polinômio a.

- DivisãoPoli(f,g)
  1. $r \leftarrow f$
  2. **enquanto** $r \neq 0$ e $\hat{g}$ divide $\hat{r}$ **faça**
  3. $\quad r \leftarrow r - \frac{cl(r)\hat{r}}{cl(g)\hat{g}}g$
  4. **fim-enquanto**
  5. **devolva** r

Para um polinômio g, o termo líder é o monômio de maior grau de g.

Exemplos com maior e menor grau

- $f := x^5 - x^2$ e $g := x^2 - x$ e
- $f := x^5 - x^2$ e $g := x^2 - 1$

Algoritmo da Divisão para polinômios em $K[x]$ (DivisãoPoli)

O algoritmo recebe como entrada dois polinômios g e f e devolve o resto da divisão de f por g, ou seja, outro polinômio r que satisfaz $grau(r) < grau(g)$ e $f = ag + r$, para algum polinômio a.

- DivisãoPoli(f,g)
  1. $r \leftarrow f$
  2. **enquanto** $r \neq 0$ e $\hat{g}$ divide $\hat{r}$ **faça**
  3. $\quad r \leftarrow r - \frac{cl(r)\hat{r}}{cl(g)\hat{g}}g$
  4. **fim-enquanto**
  5. **devolva** r

Para um polinômio g, o termo líder é o monômio de maior grau de g.

Exemplos com maior e menor grau

- $f := x^5 - x^2$ e $g := x^2 - x$ e
- $f := x^5 - x^2$ e $g := x^2 - 1$

Algoritmo da Divisão para polinômios em $K[x]$ (DivisãoPoli)

- DivisãoPoli(f,g)
  1. $r \leftarrow f$
  2. **enquanto** $r \neq 0$ e $\hat{g}$ divide $\hat{r}$ **faça**
  3. $\quad r \leftarrow r - \frac{cl(r)\hat{r}}{cl(g)\hat{g}} g$
  4. **fim-enquanto**
  5. **devolva** r

Para um polinômio g, o termo líder é o monômio de maior grau de g.
Exemplos com maior e menor grau

- $f := x^5 - x^2$ e $g := x^2 - x$ e
- $f := x^5 - x^2$ e $g := x^2 - 1$

Algoritmo da Divisão para polinômios em $K[x]$ (DivisãoPoli)

- DivisãoPoli(f,g)
  1. $r \leftarrow f$
  2. **enquanto** $r \neq 0$ e $\hat{g}$ divide $\hat{r}$ **faça**
  3. $\quad r \leftarrow r - \frac{cl(r)\hat{r}}{cl(g)\hat{g}} g$
  4. **fim-enquanto**
  5. **devolva** r

Para um polinômio g, o termo líder é o monômio de maior grau de g.
Exemplos com maior e menor grau

- $f := x^5 - x^2$ e $g := x^2 - x$ e
- $f := x^5 - x^2$ e $g := x^2 - 1$

Algoritmo de Euclides (Euclides)

O algoritmo recebe como entrada dois polinômios f e g de $K[x]$ e devolve um polinômio $h = mdc(f, g)$.

- Euclides(f,g)
  1. $h \leftarrow f$
  2. $s \leftarrow g$
  3. **enquanto** $s \neq 0$ **faça**
  4. $r \leftarrow$DivisãoPoli(h, s)
  5. $h \leftarrow s$
  6. $s \leftarrow r$
  7. **fim-enquanto**
  8. **devolva** h

Exemplo

$I =< f_1 := x^3 - 3x + 2, f_2 := x^4 - 1, f_3 := x^6 - 1 >$ e $p := x^3 + 4x^2 + 3x - 7$.

Algoritmo de Euclides (Euclides)

O algoritmo recebe como entrada dois polinômios f e g de $K[x]$ e devolve um polinômio $h = mdc(f, g)$.

- Euclides(f,g)
  1. $h \leftarrow f$
  2. $s \leftarrow g$
  3. **enquanto** $s \neq 0$ **faça**
  4. $\quad r \leftarrow$DivisãoPoli(h, s)
  5. $\quad h \leftarrow s$
  6. $\quad s \leftarrow r$
  7. **fim-enquanto**
  8. **devolva** h

Exemplo

$I =< f_1 := x^3 - 3x + 2, f_2 := x^4 - 1, f_3 := x^6 - 1 >$ e $p := x^3 + 4x^2 + 3x - 7$.

Algoritmo de Euclides (Euclides)

O algoritmo recebe como entrada dois polinômios f e g de $K[x]$ e devolve um polinômio $h = mdc(f, g)$.

- Euclides(f,g)
  1. $h \leftarrow f$
  2. $s \leftarrow g$
  3. **enquanto** $s \neq 0$ **faça**
  4. $\quad r \leftarrow$DivisãoPoli(h, s)
  5. $\quad h \leftarrow s$
  6. $\quad s \leftarrow r$
  7. **fim-enquanto**
  8. **devolva** h

Exemplo
$I =< f_1 := x^3 - 3x + 2, f_2 := x^4 - 1, f_3 := x^6 - 1 >$ e
$p := x^3 + 4x^2 + 3x - 7.$

Sumário

Motivação

O problema da pertinência em Subespaços

O problema de pertinência em $K[x]$.

O problema de pertinência em $K[x_1, \ldots, x_n]$
- Definições
- Algoritmo da Divisão
- Base de Gröbner
- Algoritmo de Buchberger

Ordem monomial

Uma **ordem monomial** em $K[x_1, \ldots, x_n]$ é uma relação $\leq$ nos monômios de $K[x_1, \ldots, x_n]$ satisfazendo:

- $\leq$ é uma boa ordem
- Para todos os monômios x^α, x^β, $x^\gamma \in K[x_1, \ldots, x_n]$, se $x^\alpha < x^\beta$ então $x^\alpha x^\gamma < x^\beta x^\gamma$

Notação: Assumiremos que $x_1 > x_2 > \ldots > x_n$.
Seja $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, denotaremos por $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$

Ordem monomial

Uma **ordem monomial** em $K[x_1, \ldots, x_n]$ é uma relação $\leq$ nos monômios de $K[x_1, \ldots, x_n]$ satisfazendo:

- $\leq$ é uma boa ordem
- Para todos os monômios x^α, x^β, $x^\gamma \in K[x_1, \ldots, x_n]$, se $x^\alpha < x^\beta$ então $x^\alpha x^\gamma < x^\beta x^\gamma$

Notação: Assumiremos que $x_1 > x_2 > \ldots > x_n$.
Seja $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, denotaremos por $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$

Ordem monomial

Uma **ordem monomial** em $K[x_1, \ldots, x_n]$ é uma relação $\leq$ nos monômios de $K[x_1, \ldots, x_n]$ satisfazendo:

- $\leq$ é uma boa ordem
- Para todos os monômios x^α, x^β, $x^\gamma \in K[x_1, \ldots, x_n]$, se $x^\alpha < x^\beta$ então $x^\alpha x^\gamma < x^\beta x^\gamma$

Notação: Assumiremos que $x_1 > x_2 > \ldots > x_n$.
Seja $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, denotaremos por $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$

Ordem monomial

Uma **ordem monomial** em $K[x_1, \ldots, x_n]$ é uma relação $\leq$ nos monômios de $K[x_1, \ldots, x_n]$ satisfazendo:

- $\leq$ é uma boa ordem
- Para todos os monômios x^α, x^β, $x^\gamma \in K[x_1, \ldots, x_n]$, se $x^\alpha < x^\beta$ então $x^\alpha x^\gamma < x^\beta x^\gamma$

Notação: Assumiremos que $x_1 > x_2 > \ldots > x_n$.
Seja $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, denotaremos por $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$

Ordem monomial

Uma **ordem monomial** em $K[x_1, \ldots, x_n]$ é uma relação $\leq$ nos monômios de $K[x_1, \ldots, x_n]$ satisfazendo:

- $\leq$ é uma boa ordem
- Para todos os monômios x^α, x^β, $x^\gamma \in K[x_1, \ldots, x_n]$, se $x^\alpha < x^\beta$ então $x^\alpha x^\gamma < x^\beta x^\gamma$

Notação: Assumiremos que $x_1 > x_2 > \ldots > x_n$.
Seja $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, denotaremos por $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$

Exemplos

- **Ordem lexicográfica** (abreviada por lex)
  Dizemos que $x^\alpha < x^\beta$ se existe $1 \leq j \leq n$ tal que $\alpha_j < \beta_j$ e $\alpha_i = \beta_i$, para todo $1 \leq i < j$.

- **Ordem de grau e lexicográfica** (abreviada por deglex)
  Dizemos que $x^\alpha < x^\beta$ se
  $\sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i$
  ou
  $\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i$ e x^α é menor que x^β na ordem lexicográfica.

Exemplos

- **Ordem lexicográfica** (abreviada por lex)
  Dizemos que $x^\alpha < x^\beta$ se existe $1 \leq j \leq n$ tal que $\alpha_j < \beta_j$ e $\alpha_i = \beta_i$, para todo $1 \leq i < j$.

- **Ordem de grau e lexicográfica** (abreviada por deglex)
  Dizemos que $x^\alpha < x^\beta$ se
  $\sum_{i=1}^{n} \alpha_i < \sum_{i=1}^{n} \beta_i$
  ou
  $\sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i$ e x^α é menor que x^β na ordem lexicográfica.

Monômio Líder

Seja $f = a_1x_1^{\alpha} + a_2x_2^{\alpha} + \ldots + a_tx_t^{\alpha}$ um polinômio não nulo de $K[x_1, \ldots, x_n]$, com $0 \neq a_i \in K$ e $\alpha_i \in \mathbb{N}^n$, para $1 \leq i \leq t$ e $\leq$ uma ordem monomial em $K[x_1, \ldots, x_n]$. Tome x^{α_j} o máximo dentre todos os x^{α_i}, na ordem $\leq$.

- Chamamos x^{α_j} o **monômio líder** de f (na ordem dada), e denotaremos por $\hat{f}$.
- Ainda, chamamos a_j de **coeficiente líder** de f e denotaremos por cl(f).
- Por fim, se S é um subconjunto de $K[x_1, \ldots, x_n]$, denotaremos por $\hat{S}$ o conjunto $\{\hat{f} \mid f \in S\}$.

Monômio Líder

Seja $f = a_1 x_1^{\alpha} + a_2 x_2^{\alpha} + \ldots + a_t x_t^{\alpha}$ um polinômio não nulo de $K[x_1, \ldots, x_n]$, com $0 \neq a_i \in K$ e $\alpha_i \in \mathbb{N}^n$, para $1 \leq i \leq t$ e $\leq$ uma ordem monomial em $K[x_1, \ldots, x_n]$. Tome x^{α_j} o máximo dentre todos os x^{α_i}, na ordem $\leq$.

- Chamamos x^{α_j} o **monômio líder** de f (na ordem dada), e denotaremos por $\hat{f}$.
- Ainda, chamamos a_j de **coeficiente líder** de f e denotaremos por cl(f).
- Por fim, se S é um subconjunto de $K[x_1, \ldots, x_n]$, denotaremos por $\hat{S}$ o conjunto $\{\hat{f} \mid f \in S\}$.

Monômio Líder

Seja $f = a_1x_1^{\alpha} + a_2x_2^{\alpha} + \ldots + a_tx_t^{\alpha}$ um polinômio não nulo de $K[x_1, \ldots, x_n]$, com $0 \neq a_i \in K$ e $\alpha_i \in \mathbb{N}^n$, para $1 \leq i \leq t$ e $\leq$ uma ordem monomial em $K[x_1, \ldots, x_n]$. Tome x^{α_j} o máximo dentre todos os x^{α_i}, na ordem $\leq$.

- Chamamos x^{α_j} o **monômio líder** de f (na ordem dada), e denotaremos por $\hat{f}$.
- Ainda, chamamos a_j de **coeficiente líder** de f e denotaremos por cl(f).
- Por fim, se S é um subconjunto de $K[x_1, \ldots, x_n]$, denotaremos por $\hat{S}$ o conjunto $\{\hat{f} \mid f \in S\}$.

Monômio Líder

Seja $f = a_1x_1^{\alpha} + a_2x_2^{\alpha} + \ldots + a_tx_t^{\alpha}$ um polinômio não nulo de $K[x_1, \ldots, x_n]$, com $0 \neq a_i \in K$ e $\alpha_i \in \mathbb{N}^n$, para $1 \leq i \leq t$ e $\leq$ uma ordem monomial em $K[x_1, \ldots, x_n]$. Tome x^{α_j} o máximo dentre todos os x^{α_i}, na ordem $\leq$.

- Chamamos x^{α_j} o **monômio líder** de f (na ordem dada), e denotaremos por $\hat{f}$.
- Ainda, chamamos a_j de **coeficiente líder** de f e denotaremos por cl(f).
- Por fim, se S é um subconjunto de $K[x_1, \ldots, x_n]$, denotaremos por $\hat{S}$ o conjunto $\{\hat{f} \mid f \in S\}$.

Algoritmo da Divisão em $K[x_1, \ldots, x_n]$ (DivisãoComut)

O algoritmo recebe como entrada um polinômio $f \in K[x_1, \ldots, x_n]$, e um conjunto finito $S = \{f_1, f_2, \ldots, f_s\} \subset K[x_1, \ldots, x_n]$ e devolve como saída outro polinômio f.

- DivisãoComut(S, f)

1. $f' \leftarrow 0$
2. **enquanto** $f \neq 0$ **faça**
3. **enquanto** $f_i \in S$ tal que $\hat{f}_i$ divide $\hat{f}$ **faça**
4. $f \leftarrow f - \frac{cl(f)\hat{f}}{cl(f_i)\hat{f}_i} f_i$
5. **fim-enquanto**
6. **se** $f \neq 0$
7. **então** $f' \leftarrow f' + cl(f)\hat{f}$
8. $f \leftarrow f - cl(f)\hat{f}$
9. **fim-se**
10. **fim-enquanto**
11. **devolva** f'

Algoritmo da Divisão em $K[x_1, \ldots, x_n]$ (DivisãoComut)

- DivisãoComut(S, f)
  1. $f' \leftarrow 0$
  2. **enquanto** $f \neq 0$ **faça**
  3. **enquanto** $f_i \in S$ tal que $\hat{f}_i$ divide $\hat{f}$ **faça**
  4. $f \leftarrow f - \frac{cl(f)\hat{f}}{cl(f_i)\hat{f}_i} f_i$
  5. **fim-enquanto**
  6. **se** $f \neq 0$
  7. **então** $f' \leftarrow f' + cl(f)\hat{f}$
  8. $f \leftarrow f - cl(f)\hat{f}$
  9. **fim-se**
  10. **fim-enquanto**
  11. **devolva** f'

Exemplo

Considere $K[x, y, z]$ com a ordem lexicográfica ($x > y > z$).
$S = \{f_1 := x^2 - y^3z, f_2 := x^2 - z^2, f_3 := y^2z - y\}$ e $f := x^2 - y^2$.
$S = \{f_1 := x^2 - y^3z, f_2 := x^2 - z^2, f_3 := y^2z - y\}$ e
$f := xy - xz^3$.

Exemplo

Considere $K[x, y, z]$ com a ordem lexicográfica $(x > y > z)$.
$S = \{f_1 := x^2 - y^3 z, f_2 := x^2 - z^2, f_3 := y^2 z - y\}$ e $f := x^2 - y^2$.
$S = \{f_1 := x^2 - y^3 z, f_2 := x^2 - z^2, f_3 := y^2 z - y\}$ e
$f := xy - xz^3$.

Exemplo

Considere $K[x, y, z]$ com a ordem lexicográfica $(x > y > z)$.
$S = \{f_1 := x^2 - y^3 z, f_2 := x^2 - z^2, f_3 := y^2 z - y\}$ e $f := x^2 - y^2$.
$S = \{f_1 := x^2 - y^3 z, f_2 := x^2 - z^2, f_3 := y^2 z - y\}$ e
$f := xy - xz^3$.

Teorema da Base de Hilbert

Todo ideal I de $K[x_1, \ldots, x_n]$ é finitamente gerado,
ou seja $I =< g_1, \ldots, g_t >$, para alguns $g_1, \ldots, g_t \in I$.

Teorema da Base de Hilbert

Todo ideal I de $K[x_1, \ldots, x_n]$ é finitamente gerado, ou seja $I =< g_1, \ldots, g_t >$, para alguns $g_1, \ldots, g_t \in I$.

Base de Gröbner

Um subconjunto G de um ideal I de $K[x_1, \ldots, x_n]$ é uma base de Gröbner para I (na ordem monomial fixada) se $< \hat{G} >=< \hat{I} >$, ou equivalentemente se, para todo polinômio não nulo $f \in I$, existe um polinômio $g \in G$ tal que $\hat{g}$ divide $\hat{f}$.

Exemplo

Consideremos $K[x, y]$ com a ordem de grau e lexicográfica $(x > y)$.
Tomemos $F = \{f_1 := x^3 - 2xy, f_2 := x^2y - 2y^2 + x\}$ e I o ideal gerado por F.

- O conjunto F não é uma base de Gröbner para I. De fato, $f_1y - f_2x = -x^2 \in I$, mas $x^2 \notin < \hat{f}_1, \hat{f}_2 >$.
- O conjunto $\{x^2, 2xy, 2y^2 - x\}$ é uma base de Gröbner para I.
- O conjunto $\{f_1, f_2, x^2, 2xy, 2y^2 - x\}$ é uma base de Gröbner que contém F.

Exemplo

Consideremos $K[x, y]$ com a ordem de grau e lexicográfica $(x > y)$. Tomemos $F = \{f_1 := x^3 - 2xy, f_2 := x^2y - 2y^2 + x\}$ e I o ideal gerado por F.

- O conjunto F não é uma base de Gröbner para I. De fato, $f_1y - f_2x = -x^2 \in I$, mas $x^2 \notin < \hat{f}_1, \hat{f}_2 >$.
- O conjunto $\{x^2, 2xy, 2y^2 - x\}$ é uma base de Gröbner para I.
- O conjunto $\{f_1, f_2, x^2, 2xy, 2y^2 - x\}$ é uma base de Gröbner que contém F.

Exemplo

Consideremos $K[x, y]$ com a ordem de grau e lexicográfica $(x > y)$. Tomemos $F = \{f_1 := x^3 - 2xy, f_2 := x^2y - 2y^2 + x\}$ e I o ideal gerado por F.

- O conjunto F não é uma base de Gröbner para I. De fato, $f_1y - f_2x = -x^2 \in I$, mas $x^2 \notin < \hat{f}_1, \hat{f}_2 >$.
- O conjunto $\{x^2, 2xy, 2y^2 - x\}$ é uma base de Gröbner para I.
- O conjunto $\{f_1, f_2, x^2, 2xy, 2y^2 - x\}$ é uma base de Gröbner que contém F.

Exemplo

Consideremos $K[x, y]$ com a ordem de grau e lexicográfica $(x > y)$. Tomemos $F = \{f_1 := x^3 - 2xy, f_2 := x^2y - 2y^2 + x\}$ e I o ideal gerado por F.

- O conjunto F não é uma base de Gröbner para I. De fato, $f_1y - f_2x = -x^2 \in I$, mas $x^2 \notin < \hat{f}_1, \hat{f}_2 >$.
- O conjunto $\{x^2, 2xy, 2y^2 - x\}$ é uma base de Gröbner para I.
- O conjunto $\{f_1, f_2, x^2, 2xy, 2y^2 - x\}$ é uma base de Gröbner que contém F.

Exemplo

Consideremos $K[x, y]$ com a ordem de grau e lexicográfica $(x > y)$. Tomemos $F = \{f_1 := x^3 - 2xy, f_2 := x^2y - 2y^2 + x\}$ e I o ideal gerado por F.

- O conjunto F não é uma base de Gröbner para I. De fato, $f_1y - f_2x = -x^2 \in I$, mas $x^2 \notin < \hat{f}_1, \hat{f}_2 >$.
- O conjunto $\{x^2, 2xy, 2y^2 - x\}$ é uma base de Gröbner para I.
- O conjunto $\{f_1, f_2, x^2, 2xy, 2y^2 - x\}$ é uma base de Gröbner que contém F.

Teorema

Seja G uma base de Gröbner do ideal I em $K[x_1, \ldots, x_n]$ e seja f um polinômio de $K[x_1, \ldots, x_n]$.
Então $f' = \text{DivisãoComut}(G, f)$ é igual a zero se, e somente se, f pertence a I.

Exemplo:
Consideremos $K[x, y]$ com a ordem de grau-lexicográfica $(x > y)$ e $G = \{x^2, 2xy, 2y^2 - x\}$ uma base de Gröbner.
Seja $f := x^2y - 2y^2 + x$. O polinômio f pertence a $<G>$?

Teorema

Seja G uma base de Gröbner do ideal I em $K[x_1, \ldots, x_n]$ e seja f um polinômio de $K[x_1, \ldots, x_n]$.
Então $f' =$ DivisãoComut(G, f) é igual a zero se, e somente se, f pertence a I.

Exemplo:
Consideremos $K[x, y]$ com a ordem de grau-lexicográfica $(x > y)$ e $G = \{x^2, 2xy, 2y^2 - x\}$ uma base de Gröbner.
Seja $f := x^2y - 2y^2 + x$. O polinômio f pertence a $<G>$?

Teorema

Seja G uma base de Gröbner do ideal I em $K[x_1, \ldots, x_n]$ e seja f um polinômio de $K[x_1, \ldots, x_n]$.
Então $f' = \text{DivisãoComut}(G, f)$ é igual a zero se, e somente se, f pertence a I.

Exemplo:
Consideremos $K[x, y]$ com a ordem de grau-lexicográfica $(x > y)$ e $G = \{x^2, 2xy, 2y^2 - x\}$ uma base de Gröbner.
Seja $f := x^2y - 2y^2 + x$. O polinômio f pertence a $<G>$?

Teorema

Seja G uma base de Gröbner do ideal I em $K[x_1, \ldots, x_n]$ e seja f um polinômio de $K[x_1, \ldots, x_n]$.
Então $f' = \text{DivisãoComut}(G, f)$ é igual a zero se, e somente se, f pertence a I.

Exemplo:
Consideremos $K[x, y]$ com a ordem de grau-lexicográfica $(x > y)$ e $G = \{x^2, 2xy, 2y^2 - x\}$ uma base de Gröbner.
Seja $f := x^2y - 2y^2 + x$. O polinômio f pertence a $<G>$?

S-polinômio

Sejam f, g polinômios de $K[x_1, \ldots, x_n]$.
O **S-polinômio** de f e g é.

$$S(f,g) := \frac{x^\gamma}{cl(f)\hat{f}} f - \frac{x^\gamma}{cl(g)\hat{g}} g$$

onde x^γ é o mínimo comum multíplo de $\hat{f}$ e $\hat{g}$,
ou seja, se $\hat{f} = x^\alpha$ e $\hat{g} = x^\beta$, com $\alpha = (\alpha_1, \ldots, \alpha_n\}$ e
$\beta = (\beta_1, \ldots, \beta_n\}$, então $\gamma = (\gamma_1, \ldots, \gamma_n\}$, com $\gamma_i = max(\alpha_i, \beta_i)$.

S-polinômio

Sejam f, g polinômios de $K[x_1, \ldots, x_n]$.
O **S-polinômio** de f e g é.

$$S(f,g) := \frac{x^\gamma}{cl(f)\hat{f}} f - \frac{x^\gamma}{cl(g)\hat{g}} g$$

onde x^γ é o mínimo comum multíplo de $\hat{f}$ e $\hat{g}$,
ou seja, se $\hat{f} = x^\alpha$ e $\hat{g} = x^\beta$, com $\alpha = (\alpha_1, \ldots, \alpha_n\}$ e
$\beta = (\beta_1, \ldots, \beta_n\}$, então $\gamma = (\gamma_1, \ldots, \gamma_n\}$, com $\gamma_i = max(\alpha_i, \beta_i)$.

S-polinômio

Sejam f, g polinômios de $K[x_1, \ldots, x_n]$.
O **S-polinômio** de f e g é.

$$S(f,g) := \frac{x^\gamma}{cl(f)\hat{f}} f - \frac{x^\gamma}{cl(g)\hat{g}} g$$

onde x^γ é o mínimo comum multíplo de $\hat{f}$ e $\hat{g}$,
ou seja, se $\hat{f} = x^\alpha$ e $\hat{g} = x^\beta$, com $\alpha = (\alpha_1, \ldots, \alpha_n\}$ e
$\beta = (\beta_1, \ldots, \beta_n\}$, então $\gamma = (\gamma_1, \ldots, \gamma_n\}$, com $\gamma_i = max(\alpha_i, \beta_i)$.

S-polinômio

Sejam f, g polinômios de $K[x_1, \ldots, x_n]$.
O **S-polinômio** de f e g é.

$$S(f,g) := \frac{x^\gamma}{cl(f)\hat{f}} f - \frac{x^\gamma}{cl(g)\hat{g}} g$$

onde x^γ é o mínimo comum multíplo de $\hat{f}$ e $\hat{g}$,
ou seja, se $\hat{f} = x^\alpha$ e $\hat{g} = x^\beta$, com $\alpha = (\alpha_1, \ldots, \alpha_n\}$ e $\beta = (\beta_1, \ldots, \beta_n\}$, então $\gamma = (\gamma_1, \ldots, \gamma_n\}$, com $\gamma_i = max(\alpha_i, \beta_i)$.

S-polinômio

Sejam f, g polinômios de $K[x_1, \ldots, x_n]$.
O **S-polinômio** de f e g é.

$$S(f,g) := \frac{x^\gamma}{cl(f)\hat{f}} f - \frac{x^\gamma}{cl(g)\hat{g}} g$$

onde x^γ é o mínimo comum multíplo de $\hat{f}$ e $\hat{g}$,
ou seja, se $\hat{f} = x^\alpha$ e $\hat{g} = x^\beta$, com $\alpha = (\alpha_1, \ldots, \alpha_n\}$ e
$\beta = (\beta_1, \ldots, \beta_n\}$, então $\gamma = (\gamma_1, \ldots, \gamma_n\}$, com $\gamma_i = max(\alpha_i, \beta_i)$.

Teorema

Seja I um ideal de $K[x_1, \ldots, x_n]$.
Um conjunto gerador $G = \{g_1, \ldots, g_t\}$ é uma base de Gröbner se e somente se para todos pares (i, j), com $i \neq j$, $S(g_i, g_j)$ se reduz para zero sobre G (para alguma ordem em que os elementos de G são considerados pelo Algoritmo da Divisão).

Teorema

Seja I um ideal de $K[x_1, \ldots, x_n]$.
Um conjunto gerador $G = \{g_1, \ldots, g_t\}$ é uma base de Gröbner se e somente se para todos pares (i, j), com $i \neq j$, $S(g_i, g_j)$ se reduz para zero sobre G (para alguma ordem em que os elementos de G são considerados pelo Algoritmo da Divisão).

Algoritmo de Buchberger (BUCHBERGER)

O algoritmo recebe como entrada um conjunto finito $F = \{f_1, f_2, \ldots, f_t\}$ de geradores de um ideal I de $K[x_1, \ldots, x_n]$ e devolve um conjunto $G \supseteq F$ que é uma Base de Gröbner de I.

BUCHBERGER(F)

1. $G \leftarrow F$
2. **repita**
3. $\quad G' \leftarrow G$
4. $\quad$ **para cada** par $f_i, f_j \in G$ **faça**
5. $\quad\quad r \leftarrow \text{DivisãoComut}(G, S(f_i, f_j))$
6. $\quad\quad$ **se** $r \neq 0$
7. $\quad\quad\quad$ **então** $G \leftarrow G \cup \{r\}$
8. $\quad\quad$ **fim-se**
9. $\quad$ **fim-para**
10. **até** $G = G'$

Algoritmo de Buchberger (BUCHBERGER)

BUCHBERGER(F)

1. $G \leftarrow F$
2. **repita**
3. $\quad G' \leftarrow G$
4. $\quad$ **para cada** par $f_i, f_j \in G$ **faça**
5. $\quad\quad r \leftarrow \text{DivisãoComut}(G, S(f_i, f_j))$
6. $\quad\quad$ **se** $r \neq 0$
7. $\quad\quad\quad$ **então** $G \leftarrow G \cup \{r\}$
8. $\quad\quad$ **fim-se**
9. $\quad$ **fim-para**
10. **até** $G = G'$
11. **devolva** G

Exemplo

Seja $K[x, y]$ com a ordem de grau-lexicográfica $(x > y)$.
Consideremos $F = \{f_1 := x^3 - 2xy, f_2 := x^2y - 2y^2 + x\}$ e I o ideal gerado por F.

Exemplo

Seja $K[x, y]$ com a ordem de grau-lexicográfica $(x > y)$.
Consideremos $F = \{f_1 := x^3 - 2xy, f_2 := x^2y - 2y^2 + x\}$ e I o ideal gerado por F.

Teorema

Seja $F = \{f_1, f_2, \ldots, f_t\}$ um conjunto gerador de um ideal I não nulo de de $K[x_1, \ldots, x_n]$.

Se F for fornecido como entrada para o Algoritmo de Buchberger, esse terminará em um número finito de passos e devolverá uma Base de Gröbner finita para I.

Teorema

Seja $F = \{f_1, f_2, \ldots, f_t\}$ um conjunto gerador de um ideal I não nulo de de $K[x_1, \ldots, x_n]$.
Se F for fornecido como entrada para o Algoritmo de Buchberger, esse terminará em um número finito de passos e devolverá uma Base de Gröbner finita para I.

Sumário

Motivação

O problema da pertinência em Subespaços

O problema de pertinência em $K[x]$.

O problema de pertinência em $K[x_1, \ldots, x_n]$

O problema de pertinência em $K<x_1, \ldots, x_n>$

- Definições
- Algoritmo da Divisão
- Base de Gröbner

As idéias envolvidas na Teoria de Bases de Gröbner não comutativas foram inicialmente estudadas de forma independente por Bokut [Bokut, 1976] e por Bergman [Bergman, 1978].

Entretanto, quem primeiro considerou essa teoria de um ponto de vista mais computacional foi Mora [Mora, 1986, Mora, 1994], introduzindo uma generalização do Algoritmo de Buchberger para o caso não comutativo (em particular para a álgebra livre), conhecido como Procidemento de Mora.

Existem uma série de pacotes computacionais que implementam os algoritmos e procedimentos da Teoria de Bases de Gröbner não comutativas. Entre eles, destacamos Opal, NCGB (Mathematica), Bergman (Standard Lisp) e GNBP (GAP4).

As idéias envolvidas na Teoria de Bases de Gröbner não comutativas foram inicialmente estudadas de forma independente por Bokut [Bokut, 1976] e por Bergman [Bergman, 1978].

Entretanto, quem primeiro considerou essa teoria de um ponto de vista mais computacional foi Mora [Mora, 1986, Mora, 1994], introduzindo uma generalização do Algoritmo de Buchberger para o caso não comutativo (em particular para a álgebra livre), conhecido como Procidemento de Mora.

Existem uma série de pacotes computacionais que implementam os algoritmos e procedimentos da Teoria de Bases de Gröbner não comutativas. Entre eles, destacamos Opal, NCGB (Mathematica), Bergman (Standard Lisp) e GNBP (GAP4).

As idéias envolvidas na Teoria de Bases de Gröbner não comutativas foram inicialmente estudadas de forma independente por Bokut [Bokut, 1976] e por Bergman [Bergman, 1978].

Entretanto, quem primeiro considerou essa teoria de um ponto de vista mais computacional foi Mora [Mora, 1986, Mora, 1994], introduzindo uma generalização do Algoritmo de Buchberger para o caso não comutativo (em particular para a álgebra livre), conhecido como Procidemento de Mora.

Existem uma série de pacotes computacionais que implementam os algoritmos e procedimentos da Teoria de Bases de Gröbner não comutativas. Entre eles, destacamos Opal, NCGB (Mathematica), Bergman (Standard Lisp) e GNBP (GAP4).

Os problemas do caso não comutativo

No caso comutativo há sempre a garantia de existência de uma Base de Gröbner finita.

Par o caso não comutativo, existem exemplos de ideais finitamente gerados que não possuem nenhuma Base de Gröbner finita, independente da ordem dada nos termos. Com isso o Procedimento de Mora pode nunca finalizar sua computação.

Por outro lado, existe a garantia de que se o ideal admitir alguma Base de Gröbner finita (para a ordem dada) então o procedimento de Mora terminará e devolverá uma Base de Gröbner finita.

O problema de calcular uma Base de Gröbner não é computável.

Os problemas do caso não comutativo

No caso comutativo há sempre a garantia de existência de uma Base de Gröbner finita.
Par o caso não comutativo, existem exemplos de ideais finitamente gerados que não possuem nenhuma Base de Gröbner finita, independente da ordem dada nos termos. Com isso o Procedimento de Mora pode nunca finalizar sua computação.

Por outro lado, existe a garantia de que se o ideal admitir alguma Base de Gröbner finita (para a ordem dada) então o procedimento de Mora terminará e devolverá uma Base de Gröbner finita.

O problema de calcular uma Base de Gröbner não é computável.

Os problemas do caso não comutativo

No caso comutativo há sempre a garantia de existência de uma Base de Gröbner finita.
Par o caso não comutativo, existem exemplos de ideais finitamente gerados que não possuem nenhuma Base de Gröbner finita, independente da ordem dada nos termos. Com isso o Procedimento de Mora pode nunca finalizar sua computação.

Por outro lado, existe a garantia de que se o ideal admitir alguma Base de Gröbner finita (para a ordem dada) então o procedimento de Mora terminará e devolverá uma Base de Gröbner finita.

O problema de calcular uma Base de Gröbner não é computável.

Os problemas do caso não comutativo

No caso comutativo há sempre a garantia de existência de uma Base de Gröbner finita.
Par o caso não comutativo, existem exemplos de ideais finitamente gerados que não possuem nenhuma Base de Gröbner finita, independente da ordem dada nos termos. Com isso o Procedimento de Mora pode nunca finalizar sua computação.

Por outro lado, existe a garantia de que se o ideal admitir alguma Base de Gröbner finita (para a ordem dada) então o procedimento de Mora terminará e devolverá uma Base de Gröbner finita.

O problema de calcular uma Base de Gröbner não é computável.

Os problemas do caso não comutativo

No caso comutativo há sempre a garantia de existência de uma Base de Gröbner finita.
Par o caso não comutativo, existem exemplos de ideais finitamente gerados que não possuem nenhuma Base de Gröbner finita, independente da ordem dada nos termos. Com isso o Procedimento de Mora pode nunca finalizar sua computação.

Por outro lado, existe a garantia de que se o ideal admitir alguma Base de Gröbner finita (para a ordem dada) então o procedimento de Mora terminará e devolverá uma Base de Gröbner finita.

O problema de calcular uma Base de Gröbner não é computável.

Ordem Admissível

Dado uma alfabeto $X = \{x_1, \ldots, x_n\}$. Consideramos, neste mini curso, o caso particular de $K<X>$ a álgebra livre sobre X. Denotamos por X^* o conjunto das palavras sobre X.

Dizemos que uma ordem $\leq$ em X^* é **admissível** se, as seguintes condições forem satisfeitas.

- A ordem $\leq$ é uma boa ordem em X^*.
- Sejam $p, q \in X^*$, se $p < q$ então $upr < uqr$, para todos $u, r \in X^*$.

Ordem Admissível

Dado uma alfabeto $X = \{x_1, \ldots, x_n\}$. Consideramos, neste mini curso, o caso particular de $K<X>$ a álgebra livre sobre X. Denotamos por X^* o conjunto das palavras sobre X.

Dizemos que uma ordem $\leq$ em X^* é **admissível** se, as seguintes condições forem satisfeitas.

- A ordem $\leq$ é uma boa ordem em X^*.
- Sejam $p, q \in X^*$, se $p < q$ então $upr < uqr$, para todos $u, r \in X^*$.

Ordem Admissível

Dado uma alfabeto $X = \{x_1, \ldots, x_n\}$. Consideramos, neste mini curso, o caso particular de $K<X>$ a álgebra livre sobre X. Denotamos por X^* o conjunto das palavras sobre X.

Dizemos que uma ordem $\leq$ em X^* é **admissível** se, as seguintes condições forem satisfeitas.

- A ordem $\leq$ é uma boa ordem em X^*.
- Sejam $p, q \in X^*$, se $p < q$ então $upr < uqr$, para todos $u, r \in X^*$.

Ordem Admissível

Dado uma alfabeto $X = \{x_1, \ldots, x_n\}$. Consideramos, neste mini curso, o caso particular de $K<X>$ a álgebra livre sobre X. Denotamos por X^* o conjunto das palavras sobre X.

Dizemos que uma ordem $\leq$ em X^* é **admissível** se, as seguintes condições forem satisfeitas.

- A ordem $\leq$ é uma boa ordem em X^*.
- Sejam $p, q \in X^*$, se $p < q$ então $upr < uqr$, para todos $u, r \in X^*$.

Ordem de grau e lexicográfica

- **Ordem lexicográfica** (abreviada por lex)
  Dizemos que $u \leq v$ se $v = uw$ para algum $w \in X^*$ ou se $u = wx_u u'$ e $v = wx_v v'$ para algumas letras $x_u, x_v \in X$ e algumas palavras $w, u', v' \in X^*$.

  A ordem lexicográfica **NÃO** é uma ordem admíssivel.

- **Ordem de grau e lexicográfica** (abreviada por deglex)
  Dizemos que $u < v$ se
  $\| u \| < \| v \|$
  ou
  $\| u \| = \| v \|$ e u é menor que v na ordem lexicográfica.

Ordem de grau e lexicográfica

- **Ordem lexicográfica** (abreviada por lex)
  Dizemos que $u \leq v$ se $v = uw$ para algum $w \in X^*$ ou se $u = wx_u u'$ e $v = wx_v v'$ para algumas letras $x_u, x_v \in X$ e algumas palavras $w, u', v' \in X^*$.

  A ordem lexicográfica **NÃO** é uma ordem admíssivel.

- **Ordem de grau e lexicográfica** (abreviada por deglex)
  Dizemos que $u < v$ se
  $\| u \| < \| v \|$
  ou
  $\| u \| = \| v \|$ e u é menor que v na ordem lexicográfica.

Ordem de grau e lexicográfica

- **Ordem lexicográfica** (abreviada por lex)
  Dizemos que $u \leq v$ se $v = uw$ para algum $w \in X^*$ ou se $u = wx_u u'$ e $v = wx_v v'$ para algumas letras $x_u, x_v \in X$ e algumas palavras $w, u', v' \in X^*$.

  A ordem lexicográfica **NÃO** é uma ordem admíssivel.

- **Ordem de grau e lexicográfica** (abreviada por deglex)
  Dizemos que $u < v$ se
  $\| u \| < \| v \|$
  ou
  $\| u \| = \| v \|$ e u é menor que v na ordem lexicográfica.

Ordem de grau e lexicográfica

- **Ordem de peso e lexicográfica** (abreviada por weight-lex) Dada uma aplicação peso $\phi : X \to \mathbb{N} - \{0\}$, definimos $\phi : X^* \to \mathbb{N}$ sua extensão natural. Dizemos que $u < v$ se $\phi(u) < \phi(v)$
  ou
  $\phi(u) = \phi(v)$ e u é menor que v na ordem lexicográfica.

  As ordens de grau e lexicográfica e de peso e lexicográfica são admíssiveis.

Ordem de grau e lexicográfica

- **Ordem de peso e lexicográfica** (abreviada por weight-lex) Dada uma aplicação peso $\phi : X \to \mathbb{N} - \{0\}$, definimos $\phi : X^* \to \mathbb{N}$ sua extensão natural. Dizemos que $u < v$ se $\phi(u) < \phi(v)$
  ou
  $\phi(u) = \phi(v)$ e u é menor que v na ordem lexicográfica.

  As ordens de grau e lexicográfica e de peso e lexicográfica são admíssiveis.

Termo Líder

Sejam $\leq$ uma ordem admissível em X^* e $f \in K<X>$.

- Definimos como **termo líder** de f o maior elemento do suporte de f (na ordem dada), e o denotamos por $\hat{f}$.
- Ainda, chamamos o coeficiente de $\hat{f}$ de **coeficiente líder** de f, denotado por cl(f).
- Por fim, se S é um subconjunto de $K<X>$, denotaremos por $\hat{S}$ o conjunto $\{\hat{f} \mid f \in S\}$.

Termo Líder

Sejam $\leq$ uma ordem admissível em X^* e $f \in K<X>$.

- Definimos como **termo líder** de f o maior elemento do suporte de f (na ordem dada), e o denotamos por $\hat{f}$.
- Ainda, chamamos o coeficiente de $\hat{f}$ de **coeficiente líder** de f, denotado por cl(f).
- Por fim, se S é um subconjunto de $K<X>$, denotaremos por $\hat{S}$ o conjunto $\{\hat{f} \mid f \in S\}$.

Termo Líder

Sejam $\leq$ uma ordem admissível em X^* e $f \in K<X>$.

- Definimos como **termo líder** de f o maior elemento do suporte de f (na ordem dada), e o denotamos por $\hat{f}$.
- Ainda, chamamos o coeficiente de $\hat{f}$ de **coeficiente líder** de f, denotado por cl(f).
- Por fim, se S é um subconjunto de $K<X>$, denotaremos por $\hat{S}$ o conjunto $\{\hat{f} \mid f \in S\}$.

Termo Líder

Sejam $\leq$ uma ordem admissível em X^* e $f \in K<X>$.

- Definimos como **termo líder** de f o maior elemento do suporte de f (na ordem dada), e o denotamos por $\hat{f}$.
- Ainda, chamamos o coeficiente de $\hat{f}$ de **coeficiente líder** de f, denotado por cl(f).
- Por fim, se S é um subconjunto de $K<X>$, denotaremos por $\hat{S}$ o conjunto $\{\hat{f} \mid f \in S\}$.

Algoritmo da Divisão em $K<X>$ (Divisão)

O algoritmo recebe como entrada um elemento $f \in K<X>$, e um conjunto finito $S = \{f_1, f_2, \ldots, f_s\} \subset K<X>$ e devolve como saída outro elemento h de $K<X>$ tal que $f = a + h$ onde $a \in <S>$ e nenhum elemento do suporte de h seja divisível pelo termo líder de um dos f_i. Além do mais, $\hat{h} \leq \hat{f}$.

- Divisão(S, f)
  1. $g \leftarrow f$
  2. $h \leftarrow 0$
  3. **enquanto** $g \neq 0$ **faça**
  4. **enquanto** existem $f_i \in S$ e $w, w' \in X^*$ tais que $w\hat{f}_i w' = \hat{g}$ **faça**
  5. $g \leftarrow g - \frac{cl(g)}{cl(f_i)} w f_i w'$
  6. **fim-enquanto**
  7. **se** $g \neq 0$
  8. **então** $h' \leftarrow h' + cl(g)\hat{g}$

Algoritmo da Divisão em $K<X>$ (Divisão)

- Divisão(S, f)
  1. $g \leftarrow f$
  2. $h \leftarrow 0$
  3. **enquanto** $g \neq 0$ **faça**
  4. **enquanto** existem $f_i \in S$ e $w, w' \in X^*$ tais que $w\hat{f}_i w' = \hat{g}$ **faça**
  5. $g \leftarrow g - \frac{cl(g)}{cl(f_i)} w f_i w'$
  6. **fim-enquanto**
  7. **se** $g \neq 0$
  8. **então** $h' \leftarrow h' + cl(g)\hat{g}$
  9. $g \leftarrow g - cl(g)\hat{g}$
  10. **fim-se**
  11. **fim-enquanto**
  12. **devolva** h

Exemplo

Considere $K<a, b, c>$ com a ordem de grau e lexicográfica $(a > b > c)$.

$S = \{f_1 := ab - ac, f_2 := a^2 - ac, f_3 := ba\}$ e $f := caaba$.

Escolhendo f_1 primeiro, temos como saída $cacca$.

Escolhendo f_2 primeiro, temos como saída 0.

Escolhendo f_3 primeiro, temos como saída 0.

Exemplo

Considere $K<a, b, c>$ com a ordem de grau e lexicográfica $(a > b > c)$.
$S = \{f_1 := ab - ac, f_2 := a^2 - ac, f_3 := ba\}$ e $f := caaba$.
Escolhendo f_1 primeiro, temos como saída $cacca$.
Escolhendo f_2 primeiro, temos como saída 0.
Escolhendo f_3 primeiro, temos como saída 0.

Exemplo

Considere $K<a, b, c>$ com a ordem de grau e lexicográfica $(a > b > c)$.
$S = \{f_1 := ab - ac, f_2 := a^2 - ac, f_3 := ba\}$ e $f := caaba$.
Escolhendo f_1 primeiro, temos como saída $cacca$.
Escolhendo f_2 primeiro, temos como saída 0.
Escolhendo f_3 primeiro, temos como saída 0.

Exemplo

Considere $K<a, b, c>$ com a ordem de grau e lexicográfica $(a > b > c)$.
$S = \{f_1 := ab - ac, f_2 := a^2 - ac, f_3 := ba\}$ e $f := caaba$.
Escolhendo f_1 primeiro, temos como saída $cacca$.
Escolhendo f_2 primeiro, temos como saída 0.
Escolhendo f_3 primeiro, temos como saída 0.

Exemplo

Considere $K<a, b, c>$ com a ordem de grau e lexicográfica $(a > b > c)$.
$S = \{f_1 := ab - ac, f_2 := a^2 - ac, f_3 := ba\}$ e $f := caaba$.
Escolhendo f_1 primeiro, temos como saída $cacca$.
Escolhendo f_2 primeiro, temos como saída 0.
Escolhendo f_3 primeiro, temos como saída 0.

Base de Gröbner

Um subconjunto G de um ideal I de $K<X>$ é uma **base de Gröbner** para I (na ordem admissível fixada) se $< \hat{G} >=< \hat{I} >$, ou equivalentemente se, para todo elemento não nulo $f \in I$, existe um polinômio $g \in G$ tal que $\hat{g}$ divide $\hat{f}$.

Exemplo - Nem sempre é finito

Seja I o ideal gerado por $f := aba - b^2a$.

- Consideremos $K<a, b>$ com a ordem de grau e lexicográfica $(a > b)$.
  Uma base de Gröbner para I é

$$G := \{ab^{2i-1}a - b^{2i}a \mid i \geq 1\}$$

  De fato, não existe base de Gröbner finita para I.

- Consideremos $K<a, b>$ com a ordem de grau e lexicográfica $(b > a)$.
  Uma base de Gröbner para I é $\{f\}$.

Exemplo - Nem sempre é finito

Seja I o ideal gerado por $f := aba - b^2a$.

- Consideremos $K<a, b>$ com a ordem de grau e lexicográfica $(a > b)$.
  Uma base de Gröbner para I é

$$G := \{ab^{2i-1}a - b^{2i}a \mid i \geq 1\}$$

  De fato, não existe base de Gröbner finita para I.

- Consideremos $K<a, b>$ com a ordem de grau e lexicográfica $(b > a)$.
  Uma base de Gröbner para I é $\{f\}$.

Exemplo - Nem sempre é finito

Seja I o ideal gerado por $f := aba - b^2a$.

- Consideremos $K<a, b>$ com a ordem de grau e lexicográfica $(a > b)$.
  Uma base de Gröbner para I é

$$G := \{ab^{2i-1}a - b^{2i}a \mid i \geq 1\}$$

  De fato, não existe base de Gröbner finita para I.

- Consideremos $K<a, b>$ com a ordem de grau e lexicográfica $(b > a)$.
  Uma base de Gröbner para I é $\{f\}$.

Exemplo - Nem sempre é finito

Seja I o ideal gerado por $f := aba - b^2a$.

- Consideremos $K<a, b>$ com a ordem de grau e lexicográfica $(a > b)$.
  Uma base de Gröbner para I é

$$G := \{ab^{2i-1}a - b^{2i}a \mid i \geq 1\}$$

  De fato, não existe base de Gröbner finita para I.

- Consideremos $K<a, b>$ com a ordem de grau e lexicográfica $(b > a)$.
  Uma base de Gröbner para I é $\{f\}$.

Exemplo - Nem sempre é finito

Seja I o ideal gerado por $f := aba - b^2a$.

- Consideremos $K<a, b>$ com a ordem de grau e lexicográfica $(a > b)$.
  Uma base de Gröbner para I é

$$G := \{ab^{2i-1}a - b^{2i}a \mid i \geq 1\}$$

  De fato, não existe base de Gröbner finita para I.

- Consideremos $K<a, b>$ com a ordem de grau e lexicográfica $(b > a)$.
  Uma base de Gröbner para I é $\{f\}$.

Exemplo - Nem sempre é finito

Seja I o ideal gerado por $f := aba - b^2a$.

- Consideremos $K<a, b>$ com a ordem de grau e lexicográfica $(a > b)$.
  Uma base de Gröbner para I é

$$G := \{ab^{2i-1}a - b^{2i}a \mid i \geq 1\}$$

  De fato, não existe base de Gröbner finita para I.

- Consideremos $K<a, b>$ com a ordem de grau e lexicográfica $(b > a)$.
  Uma base de Gröbner para I é $\{f\}$.

Exemplo - Sempre infinito

Consideremos $K<a, x, y>$ e I o ideal gerado por $\{axya - xya, xy - yx\}$.

- O conjunto

$$G := \{ay^i x^i a - y^i x^i a, xy - yx \mid i \geq 1\}$$

é uma base de Gröbner para I para qualquer ordem admissível satisfazendo $xy > yx$.

De fato, não existe base de Gröbner finita para I, independente da ordem admissível escolhida.

Exemplo - Sempre infinito

Consideremos $K<a, x, y>$ e I o ideal gerado por $\{axya - xya, xy - yx\}$.

- O conjunto

$$G := \{ay^i x^i a - y^i x^i a, xy - yx \mid i \geq 1\}$$

é uma base de Gröbner para I para qualquer ordem admissível satisfazendo $xy > yx$.

De fato, não existe base de Gröbner finita para I, independente da ordem admissível escolhida.

Exemplo - Sempre infinito

Consideremos $K<a, x, y>$ e I o ideal gerado por $\{axya - xya, xy - yx\}$.

- O conjunto

$$G := \{ay^i x^i a - y^i x^i a, xy - yx \mid i \geq 1\}$$

é uma base de Gröbner para I para qualquer ordem admissível satisfazendo $xy > yx$.

De fato, não existe base de Gröbner finita para I, independente da ordem admissível escolhida.

Teorema

Seja G uma base de Gröbner do ideal I em $K<X>$ e seja $f \in K<X>$.

Então $f' =$ Divisão(G, f) é independente da escolha feita na linha 4.

Logo, f' é igual a zero se, e somente se, f pertence a I.

Teorema

Seja G uma base de Gröbner do ideal I em $K<X>$ e seja $f \in K<X>$.
Então $f' =$ Divisão(G, f) é independente da escolha feita na linha 4.
Logo, f' é igual a zero se, e somente se, f pertence a I.

Teorema

Seja G uma base de Gröbner do ideal I em $K<X>$ e seja $f \in K<X>$.
Então $f' =$ Divisão(G, f) é independente da escolha feita na linha 4.
Logo, f' é igual a zero se, e somente se, f pertence a I.

Relação de Sobreposição

Sejam f, g dois elementos de $K<X>$.

Uma **sobreposição** envolvendo f e g é uma quadrupla (f, g, u, v) satisfazendo:

- u e v são palavras não nula de X^*.
- $u\hat{f} = \hat{g}v$.
- O termo líder de f não divide v e o termo líder de g não divide u.

Dado uma sobreposição (f, g, u, v), diremos que uma **relação de sobreposição** envolvendo f e g é dada por

$$\mathcal{O}(f, g, u, v) = uf - \alpha gv$$

com $\alpha = cl(uf)/cl(gv)$.

Relação de Sobreposição

Sejam f, g dois elementos de $K<X>$.
Uma **sobreposição** envolvendo f e g é uma quadrupla (f, g, u, v) satisfazendo:

- u e v são palavras não nula de X^*.
- $u\hat{f} = \hat{g}v$.
- O termo líder de f não divide v e o termo líder de g não divide u.

Dado uma sobreposição (f, g, u, v), diremos que uma **relação de sobreposição** envolvendo f e g é dada por

$$\mathcal{O}(f, g, u, v) = uf - \alpha gv$$

com $\alpha = cl(uf)/cl(gv)$.

Relação de Sobreposição

Sejam f, g dois elementos de $K<X>$.
Uma **sobreposição** envolvendo f e g é uma quadrupla (f, g, u, v) satisfazendo:

- u e v são palavras não nula de X^*.
- $u\hat{f} = \hat{g}v$.
- O termo líder de f não divide v e o termo líder de g não divide u.

Dado uma sobreposição (f, g, u, v), diremos que uma **relação de sobreposição** envolvendo f e g é dada por

$$\mathcal{O}(f, g, u, v) = uf - \alpha gv$$

com $\alpha = cl(uf)/cl(gv)$.

Relação de Sobreposição

Sejam f, g dois elementos de $K<X>$.
Uma **sobreposição** envolvendo f e g é uma quadrupla (f, g, u, v) satisfazendo:

- u e v são palavras não nula de X^*.
- $u\hat{f} = \hat{g}v$.
- O termo líder de f não divide v e o termo líder de g não divide u.

Dado uma sobreposição (f, g, u, v), diremos que uma **relação de sobreposição** envolvendo f e g é dada por

$$\mathcal{O}(f, g, u, v) = uf - \alpha gv$$

com $\alpha = cl(uf)/cl(gv)$.

Relação de Sobreposição

Sejam f, g dois elementos de $K<X>$.
Uma **sobreposição** envolvendo f e g é uma quadrupla (f, g, u, v) satisfazendo:

- u e v são palavras não nula de X^*.
- $u\hat{f} = \hat{g}v$.
- O termo líder de f não divide v e o termo líder de g não divide u.

Dado uma sobreposição (f, g, u, v), diremos que uma **relação de sobreposição** envolvendo f e g é dada por

$$\mathcal{O}(f, g, u, v) = uf - \alpha gv$$

com $\alpha = cl(uf)/cl(gv)$.

Relação de Sobreposição

Sejam f, g dois elementos de $K<X>$.
Uma **sobreposição** envolvendo f e g é uma quadrupla (f, g, u, v) satisfazendo:

- u e v são palavras não nula de X^*.
- $u\hat{f} = \hat{g}v$.
- O termo líder de f não divide v e o termo líder de g não divide u.

Dado uma sobreposição (f, g, u, v), diremos que uma **relação de sobreposição** envolvendo f e g é dada por

$$\mathcal{O}(f, g, u, v) = uf - \alpha gv$$

com $\alpha = cl(uf)/cl(gv)$.

Relação de Divisão

Sejam f, g dois elementos de $K<X>$.
Dizemos que existe uma **relação de divisão**envolvendo f e G se $\hat{f} = u\hat{g}v$, para algumas palavras de X^*.
Neste caso, essa relação de divisão é dada por

$$\mathcal{D}(f, g, u, v) = f - \alpha ugv$$

com $\alpha = cl(f)/cl(ugv)$.

Relação de Divisão

Sejam f, g dois elementos de $K<X>$.
Dizemos que existe uma **relação de divisão**envolvendo f e G se $\hat{f} = u\hat{g}v$, para algumas palavras de X^*.
Neste caso, essa relação de divisão é dada por

$$\mathcal{D}(f, g, u, v) = f - \alpha ugv$$

com $\alpha = cl(f)/cl(ugv)$.

Relação de Divisão

Sejam f, g dois elementos de $K<X>$.
Dizemos que existe uma **relação de divisão**envolvendo f e G se $\hat{f} = u\hat{g}v$, para algumas palavras de X^*.
Neste caso, essa relação de divisão é dada por

$$\mathcal{D}(f, g, u, v) = f - \alpha ugv$$

com $\alpha = cl(f)/cl(ugv)$.

Proposição

Sejam f, g dois elementos de $K<X>$.
Existe apenas um número finito de relações de sobreposição e de divisão envolvendo f e g.

Proposição

Sejam f, g dois elementos de $K<X>$.
Existe apenas um número finito de relações de sobreposição e de divisão envolvendo f e g.

Procedimento de Mora (PMORA)

O algoritmo recebe como entrada um conjunto finito $F = \{f_1, f_2, \ldots, f_t\}$ de geradores de um ideal I de $K<X>$. Caso termine sua computação, ele devolve uma Base de Gröbner finita para I. Aindam se I possuir alguma Base de Gröbner finita (para a ordem admissível fixada), o procedimento termina.

1. $R \leftarrow \emptyset$; $G \leftarrow F$
2. **para cada** par $f, g \in G$ **faça**
3. $\quad R \leftarrow R \cup$ CalculaRelações(f, g)
4. **fim-para**
5. **enquanto** $R \neq \emptyset$ **faça**
6. $\quad r \leftarrow$ EscolheRelação(R)
7. $\quad h \leftarrow$ Divisão(G, r)
8. $\quad$ **se** $h \neq 0$
9. $\quad\quad$ **então** $G \leftarrow G \cup \{h\}$

Procedimento de Mora (PMORA)

1. $R \leftarrow \emptyset$; $G \leftarrow F$
2. **para cada** par $f, g \in G$ **faça**
3. $\quad R \leftarrow R \cup$ CalculaRelações(f, g)
4. **fim-para**
5. **enquanto** $R \neq \emptyset$ **faça**
6. $\quad r \leftarrow$ EscolheRelação(R)
7. $\quad h \leftarrow$ Divisão(G, r)
8. $\quad$ **se** $h \neq 0$
9. $\quad$ **então** $G \leftarrow G \cup \{h\}$
10. $\quad\quad$ **para cada** par $g \in G$ **faça**
11. $\quad\quad\quad R \leftarrow R \cup$ CalculaRelações(g, h)
12. $\quad$ **fim-para; fim-se;fim-enquanto**
13. **devolva** G

CalculaRelações(f, g)

Esta função recebe como entrada dois elementos de $K<X>$ e devolve um conjunto contendo todas as relações de sobreposição e de divisão não nulas envolvendo os elementos f e g.

Esta função pode ser emplementada sem muita dificuldade fazendo buscas por subpalavras envolvendo f e g. Ademais, sua saída será sempre um conjunto finito.

CalculaRelações(f, g)

Esta função recebe como entrada dois elementos de $K<X>$ e devolve um conjunto contendo todas as relações de sobreposição e de divisão não nulas envolvendo os elementos f e g.

Esta função pode ser emplementada sem muita dificuldade fazendo buscas por subpalavras envolvendo f e g. Ademais, sua saída será sempre um conjunto finito.

EscolheRelação(R)

Esta função recebe como entrada um conjunto composto por relações de sobreposição e de divisão e devolve um desses elementos (removendo-o do conjunto original R).

Ela deve possuir a seguinte propriedade: se um elemento s é inserido no conjunto R e sucessivas chamadas são feitas para a função EscolheRelação, s deve ser devolvido em um número finito de chamadas de EscolheRelação.

Em outras palavras, exigimos que toda relação de sobreposição e de divisão encontrada pelo procedimento seja considerada em tempo finito.

EscolheRelação(R)

Esta função recebe como entrada um conjunto composto por relações de sobreposição e de divisão e devolve um desses elementos (removendo-o do conjunto original R).

Ela deve possuir a seguinte propriedade: se um elemento s é inserido no conjunto R e sucessivas chamadas são feitas para a função EscolheRelação, s deve ser devolvido em um número finito de chamadas de EscolheRelação.

Em outras palavras, exigimos que toda relação de sobreposição e de divisão encontrada pelo procedimento seja considerada em tempo finito.

EscolheRelação(R)

Esta função recebe como entrada um conjunto composto por relações de sobreposição e de divisão e devolve um desses elementos (removendo-o do conjunto original R).

Ela deve possuir a seguinte propriedade: se um elemento s é inserido no conjunto R e sucessivas chamadas são feitas para a função EscolheRelação, s deve ser devolvido em um número finito de chamadas de EscolheRelação.

Em outras palavras, exigimos que toda relação de sobreposição e de divisão encontrada pelo procedimento seja considerada em tempo finito.

Exemplo

Seja $K<a,b,c,d,e,f>$ com a ordem de peso e lexicográfica $(a < b < c < d < e < f)$ com a seguinte aplicação peso:

$$\phi(a) = 3 \text{ e } \phi(b) = \phi(c) = \phi(d) = \phi(e) = \phi(f) = 1$$

Consideremos I o ideal gerado por $F = \{g_1, g_2, \ldots, g_7\}$ com:

$g_1 := ca - ac$ $g_2 := da - ad$ $g_3 := ba - b^2c$

$g_4 := be^2 - b^2c$ $g_5 := b^2cf - bc$ $g_6 := e^2f - bc^2$

$g_7 := bcd$

Exemplo

Seja $K<a,b,c,d,e,f>$ com a ordem de peso e lexicográfica $(a < b < c < d < e < f)$ com a seguinte aplicação peso:

$$\phi(a) = 3 \text{ e } \phi(b) = \phi(c) = \phi(d) = \phi(e) = \phi(f) = 1$$

Consideremos I o ideal gerado por $F = \{g_1, g_2, \ldots, g_7\}$ com:

$g_1 := ca - ac$ $\quad g_2 := da - ad$ $\quad g_3 := ba - b^2c$

$g_4 := be^2 - b^2c$ $\quad g_5 := b^2cf - bc$ $\quad g_6 := e^2f - bc^2$

$g_7 := bcd$

Teorema

Seja $F = \{f_1, f_2, \ldots, f_t\}$ um conjunto gerador de um ideal I não nulo de de $K<X>$.

Se F for fornecido como entrada para o Procedimento de Mora, esse terminará em um número finito de passos e devolverá uma Base de Gröbner finita para I se e somente se I possui uma Base de Gröbner finita.

Teorema

Seja $F = \{f_1, f_2, \ldots, f_t\}$ um conjunto gerador de um ideal I não nulo de de $K<X>$.
Se F for fornecido como entrada para o Procedimento de Mora, esse terminará em um número finito de passos e devolverá uma Base de Gröbner finita para I se e somente se I possui uma Base de Gröbner finita.

Bergman, G. M., *The diamond lemma for ring theory*, Adv. in Math. 29 (1978), no. 2, 178-218.

Bokut, L. A., *Imbeddings into simple associative algebras*, Algebra i Logika **15** (1976), no. 2, 117-142, 245.

Buchberger, B., *On finding a vector space basis of the residue class ring modulo a zero dimensional polynomial ideal*, Ph.D. thesis, Univ. of Innsbruck, Austria, 1965.

Mora, F., *Gröbner bases for non-commutative polynomial rings*, Algebraic algoritms and error-correcting codes: proceedings (Jacques Calmet, ed.), Lecture Notes in Computer Science, vol. 229, Springer-Verlag, 1986, 353-362.

 Mora, T., *An introduction to commutative and noncommutative Gröbner bases*, Theoretical Computer Science 134 (1994), 131-173.

 Villas Bôas, A. A., *Aspectos algébricos e computacionais da teoria de bases de Gröbner não comutativas*, Dissertação de Mestrado, Univ. de São Paulo, Brasil, 2005.