Groupe de lecture

S-Polynômes

Clara Genes, Alice Morinière

ENS Rennes

19 Octobre 2022

Division par une base de Gröbner

Proposition

Soient $I \subseteq k[x_1, \ldots, x_n]$ un idéal et $G = \{g_1, \ldots, g_t\}$ une base de Gröbner pour I. Alors, si $f \in k[x_1, \ldots, x_n]$, il existe un unique $r \in k[x_1, \ldots, x_n]$ tel que :

1. *aucun monôme de r n'est divisible par les $LT(g_i), i = 1, \ldots, t$,*
2. *il existe $g \in I$ tel que $f = g + r$.*

Division par une base de Gröbner

Proposition

Soient $I \subseteq k[x_1, \ldots, x_n]$ un idéal et $G = \{g_1, \ldots, g_t\}$ une base de Gröbner pour I. Alors, si $f \in k[x_1, \ldots, x_n]$, il existe un unique $r \in k[x_1, \ldots, x_n]$ tel que :

1. *aucun monôme de r n'est divisible par les $LT(g_i), i = 1, \ldots, t$,*
2. *il existe $g \in I$ tel que $f = g + r$.*

Rappel : Soit $I = \langle x^\alpha | \alpha \in A \rangle$ un idéal monomial. Alors, un monôme x^β est dans I

si et seulement si il est divisible par un x^α pour $\alpha \in A$.

Division par une base de Gröbner

Proposition

Soient $I \subseteq k[x_1, \ldots, x_n]$ un idéal et $G = \{g_1, \ldots, g_t\}$ une base de Gröbner pour I. Alors, si $f \in k[x_1, \ldots, x_n]$, il existe un unique $r \in k[x_1, \ldots, x_n]$ tel que :

1. *aucun monôme de r n'est divisible par les $LT(g_i), i = 1, \ldots, t$,*
2. *il existe $g \in I$ tel que $f = g + r$.*

Remarque

La proposition précédente peut être affinée : il existe en fait un unique $r \in k[x_1, \ldots, x_n]$ tel que :

1. *Aucun monôme de r n'est divisible par l'un des éléments de $LT(I)$.*
2. *Il existe $g \in I$ tel que $f = g + r$.*

Division par une base de Gröbner

$$\forall f \in k[x_1, \ldots, x_n], \exists! r \in k[x_1, \ldots, x_n] \,|\, \exists g \in I \text{ t.q. } f = g + r$$

Corollaire

Soit $G = \{g_1, \ldots, g_t\}$ une base de Gröbner de l'idéal $I \subseteq k[x_1, \ldots, x_n]$ et soit $f \in k[x_1, \ldots, x_n]$. Alors $f \in I$ si et seulement si le reste de la division euclidienne de f par G est nul.

Attention :

La proposition donne l'unicité de r, mais rien n'indique que les "quotients" des divisions sont uniques !

Attention :

Exemple

On pose $f_1 = x + z$, $f_2 = y - z$, *et* $f = xy$.

$G = \{f_1, f_2\}$ *est une base de Gröbner pour lex. On a*

$$f = yf_1 - zf_2 - z^2,$$

et

$$f = xf_2 + zf_1 - z^2.$$

Attention :

Exemple

On pose $f_1 = x + z$, $f_2 = y - z$, *et* $f = xy$.

$G = \{f_1, f_2\}$ *est une base de Gröbner pour lex. On a*

$$f = yf_1 - zf_2 - z^2,$$

et

$$f = xf_2 + zf_1 - z^2.$$

Ainsi, on ne peut espérer que l'unicité du reste et non des quotients.

Utilité des S-polynômes

À quoi ça sert ?

Définition des *S-Polynômes*

Rappels : Si $f = 3x^3y^2 + 1$ *:* $\mathrm{LM}(f) = x^3y^2$, $\mathrm{LC}(f) = 3$, $\mathrm{LT}(f) = 3x^3y^2$, $\mathrm{multideg}(f) = (3, 2)$.

Définition

Soient $f, g \in k[x_1, \ldots, x_n]$ *des polynômes non nuls.*

1. *Si* $\mathrm{multideg}(f) = \alpha$ *et* $\mathrm{multideg}(g) = \beta$, *on pose* $\gamma = (\gamma_1, \ldots, \gamma_n)$ *avec* $\gamma_i = \max(\alpha_i, \beta_i)$ *pour tout* i.
   On appelle x^γ *le* ***plus petit commun multiple*** *de* $LM(f)$ *et* $LM(g)$. *Autrement dit,*

$$x^\gamma = \mathrm{ppcm}\left\{LM(f), LM(g)\right\}.$$

Définition des *S-Polynômes*

Rappels : Si $f = 3x^3y^2 + 1$ *:* $\mathrm{LM}(f) = x^3y^2$, $\mathrm{LC}(f) = 3$, $\mathrm{LT}(f) = 3x^3y^2$, $\mathrm{multideg}(f) = (3, 2)$.

Définition

Soient $f, g \in k[x_1, \ldots, x_n]$ *des polynômes non nuls.*

1. *Si* $\mathrm{multideg}(f) = \alpha$ *et* $\mathrm{multideg}(g) = \beta$, *on pose* $\gamma = (\gamma_1, \ldots, \gamma_n)$ *avec* $\gamma_i = \max(\alpha_i, \beta_i)$ *pour tout* i.
   On appelle x^γ *le* ***plus petit commun multiple*** *de* $LM(f)$ *et* $LM(g)$. *Autrement dit,*

$$x^\gamma = \mathrm{ppcm}\left\{LM(f), LM(g)\right\}.$$

2. *Le* ***S-polynôme*** *de* f *et* g, *noté* $S(f, g)$ *est donné par*

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

Exemples de S-polynôme

Exemple

On pose $f = x^4y - xy^2$ *et* $g = 4x^3y^3 + x^2y$, *et l'on considère l'ordre lex. Alors* $\gamma = (4, 3)$, *et donc*

$$S(f, g) = \frac{x^4y^3}{x^4y} \times f - \frac{x^4y^3}{4x^3y^3} \times g$$

Exemples de S-polynôme

Exemple

On pose $f = x^4y - xy^2$ *et* $g = 4x^3y^3 + x^2y$, *et l'on considère l'ordre lex. Alors* $\gamma = (4, 3)$, *et donc*

$$\begin{aligned} S(f,g) &= \frac{x^4y^3}{x^4y} \times f - \frac{x^4y^3}{4x^3y^3} \times g \\ &= y^2 \times f - \frac{1}{4}x \times g \end{aligned}$$

Exemples de S-polynôme

Exemple

On pose $f = x^4y - xy^2$ *et* $g = 4x^3y^3 + x^2y$, *et l'on considère l'ordre lex. Alors* $\gamma = (4, 3)$, *et donc*

$$\begin{aligned} S(f,g) &= \frac{x^4y^3}{x^4y} \times f - \frac{x^4y^3}{4x^3y^3} \times g \\ &= y^2 \times f - \frac{1}{4}x \times g \\ &= -xy^4 - \frac{1}{4}x^3y. \end{aligned}$$

Propriétés des S-polynômes

Rappels : Si $f = 3x^3y^2 + 1$ *:* $\mathrm{LM}(f) = x^3y^2$, $\mathrm{LC}(f) = 3$, $\mathrm{LT}(f) = 3x^3y^2$, $\mathrm{multideg}(f) = (3, 2)$.

$S(f, g) = \frac{x^\gamma}{\mathrm{LT}(f)} \cdot f - \frac{x^\gamma}{\mathrm{LT}(g)} \cdot g$

Proposition

Étant donné deux polynômes f *et* g*,*

$$S(f, g) = S\left(\frac{f}{LC(f)}, \frac{g}{LC(g)}\right)$$

Propriétés des S-polynômes

Rappels : Si $f = 3x^3y^2 + 1$: $\mathrm{LM}(f) = x^3y^2$, $\mathrm{LC}(f) = 3$, $\mathrm{LT}(f) = 3x^3y^2$, $\mathrm{multideg}(f) = (3, 2)$.

$$S(f,g) = \frac{x^\gamma}{\mathrm{LT}(f)} \cdot f - \frac{x^\gamma}{\mathrm{LT}(g)} \cdot g$$

Proposition

Étant donné deux polynômes f *et* g,

$$S(f,g) = S\left(\frac{f}{LC(f)}, \frac{g}{LC(g)}\right)$$

Proposition

Étant donné deux polynômes f *et* g, *et* $x^\gamma = \mathrm{ppcm}(LM(f), LM(g))$, *alors*

$$\mathrm{multideg}(S(f,g)) < \gamma.$$

Propriétés des S-polynômes

Rappels : Si $f = 3x^3y^2 + 1$ *:* $\mathrm{LM}(f) = x^3y^2$, $\mathrm{LC}(f) = 3$, $\mathrm{LT}(f) = 3x^3y^2$, $\mathrm{multideg}(f) = (3, 2)$.

Proposition

Étant donné deux polynômes f *et* g*, le S-polynôme* $S(f, g)$ *dépend de l'ordre monomial.*

Propriétés des S-polynômes

Rappels : Si $f = 3x^3y^2 + 1$ *:* $\mathrm{LM}(f) = x^3y^2$, $\mathrm{LC}(f) = 3$, $\mathrm{LT}(f) = 3x^3y^2$, $\mathrm{multideg}(f) = (3, 2)$.

Proposition

Étant donné deux polynômes f *et* g*, le S-polynôme* $S(f, g)$ *dépend de l'ordre monomial.*

Exemple

On considère $f = x^4y^2 - x^2y^5 + x$ *et* $g = 3x^4y + y^2$*, on a alors*

1. *Pour l'ordre lexicographique*

Propriétés des S-polynômes

Rappels : Si $f = 3x^3y^2 + 1$: $\mathrm{LM}(f) = x^3y^2$, $\mathrm{LC}(f) = 3$, $\mathrm{LT}(f) = 3x^3y^2$, $\mathrm{multideg}(f) = (3, 2)$.

Proposition

Étant donné deux polynômes f *et* g, *le S-polynôme* $S(f, g)$ *dépend de l'ordre monomial.*

Exemple

On considère $f = x^4y^2 - x^2y^5 + x$ *et* $g = 3x^4y + y^2$, *on a alors*

1. *Pour l'ordre lexicographique*

$$S(f, g) = -x^2y^5 + x - \frac{1}{3}y^3,$$

2. *Pour l'ordre lexicographique gradué*

Propriétés des S-polynômes

Rappels : Si $f = 3x^3y^2 + 1$ *:* $\mathrm{LM}(f) = x^3y^2$, $\mathrm{LC}(f) = 3$, $\mathrm{LT}(f) = 3x^3y^2$, $\mathrm{multideg}(f) = (3, 2)$.

Proposition

Étant donné deux polynômes f *et* g*, le S-polynôme* $S(f, g)$ *dépend de l'ordre monomial.*

Exemple

On considère $f = x^4y^2 - x^2y^5 + x$ *et* $g = 3x^4y + y^2$*, on a alors*

1. *Pour l'ordre lexicographique*

$$S(f, g) = -x^2y^5 + x - \frac{1}{3}y^3,$$

2. *Pour l'ordre lexicographique gradué*

$$S(f, g) = -x^6y^2 - x^3 - \frac{1}{3}y^6$$

Propriétés des S-polynômes

Lemme

On suppose qu'on a une somme

$$\sum_{i=1}^{s} p_i, \ \text{où} \ \text{multideg}(p_i) = \delta \in \mathbb{N}^n .$$

Si

$$\text{multideg}\left(\sum_{i=1}^{s} p_i\right) < \delta,$$

alors cette somme est une combinaison linéaire des S-polynômes $S(p_j, p_l)$ pour $1 \leqslant j, l \leqslant s$ avec coefficients dans k. De plus, chaque $S(p_j, p_l)$ a un multidegré strictement plus petit que δ.

Propriétés des S-polynômes

Rappels : Si $f = 3x^3y^2 + 1$ *:* $\mathrm{LM}(f) = x^3y^2$, $\mathrm{LC}(f) = 3$, $\mathrm{LT}(f) = 3x^3y^2$, $\mathrm{multideg}(f) = (3, 2)$.

Proposition

Soient f *et* g *deux polynômes non nuls, et* x^α, x^β *deux monômes. Alors*

$$S(x^\alpha f, x^\beta g) = x^\gamma S(f, g),$$

où

$$x^\gamma = \frac{\mathrm{ppcm}\{x^\alpha \,\mathrm{LM}(f), x^\beta \,\mathrm{LM}(g)\}}{\mathrm{ppcm}\{\mathrm{LM}(f), \mathrm{LM}(g)\}}.$$

Propriétés des S-polynômes

Corollaire

Soient c_i, c_j des coefficiens dans k, $x^{\alpha(i)}, x^{\alpha(j)}$ deux monômes, et g_i, g_j deux polynômes non nuls. Supposons que $c_i x^{\alpha(i)} g_i$ et $c_j x^{\alpha(j)} g_j$ ont pour multidegré δ. Alors

$$S(c_i x^{\alpha(i)} g_i, c_j x^{\alpha(j)} g_j) = x^{\delta - \gamma_{ij}} S(g_i, g_j),$$

avec $\gamma_{ij} = \text{ppcm}(LM(g_i), LM(g_j))$.

Critère de Buchberger

Théorème

Soient I un idéal de $k[x_1, \ldots, x_n]$ et $G = \{g_1, \ldots, g_t\}$ une base de I.

G est une base de Gröbner de I ssi pour toute paire $i \neq j$ le reste de la division de $S(g_i, g_j)$ par G avec un certain ordre est nul.

Critère de Buchberger : preuve

Théorème

Soient I un idéal de $k[x_1, \ldots, x_n]$ et $G = \{g_1, \ldots, g_t\}$ une base de I.

G est une base de Gröbner de I ssi pour toute paire $i \neq j$ le reste de la division de $S(g_i, g_j)$ par G avec un certain ordre est nul.

Démonstration :

$\Rightarrow$

Corollaire

Soit $G = \{g_1, \ldots, g_t\}$ une base de Gröbner de l'idéal $I \subseteq k[x_1, \ldots, x_n]$ et soit $f \in k[x_1, \ldots, x_n]$. Alors $f \in I$ si et seulement si le reste de la division euclidienne de f par G est nul.

Critère de Buchberger : preuve

Théorème

Soient I un idéal de $k[x_1, \ldots, x_n]$ et $G = \{g_1, \ldots, g_t\}$ une base de I.

G est une base de Gröbner de I ssi pour toute paire $i \neq j$ le reste de la division de $S(g_i, g_j)$ par G avec un certain ordre est nul.

Démonstration :

$\Leftarrow$

Lemme

Soit $f, g \in k[x_1, \ldots, x_n]$ deux polynômes non nuls. Alors

1. $\text{multideg}(fg) = \text{multideg}(f) + \text{multideg}(g)$.
2. *si* $f + g \neq 0$, $\text{multideg}(f + g) \leq \max(\text{multideg}(f), \text{multideg}(g))$. *De plus, si* $\text{multideg}(f) \neq \text{multideg}(g)$, *alors l'égalité a lieu.*

Critère de Buchberger : preuve

Lemme

On suppose qu'on a une somme

$$\sum_{i=1}^{s} p_i, \ \text{où} \ \text{multideg}(p_i) = \delta \in \mathbb{N}^n .$$

Si

$$\text{multideg}\left(\sum_{i=1}^{s} p_i\right) < \delta$$

alors cette somme est une combinaison linéaire des S-polynômes $S(p_j, p_l)$ pour $1 \leqslant j, l \leqslant s$ avec coefficients dans k. De plus, chaque $S(p_j, p_l)$ a un multidegré strictement plus petit que δ.

Critère de Buchberger : preuve

Théorème

Soient I un idéal de $k[x_1, \ldots, x_n]$ et $G = \{g_1, \ldots, g_t\}$ une base de I.

G est une base de Gröbner de I ssi pour toute paire $i \neq j$ le reste de la division de $S(g_i, g_j)$ par G avec un certain ordre est nul.

Corollaire

Soient c_i, c_j des coefficiens dans k, $x^{\alpha(i)}, x^{\alpha(j)}$ deux monômes, et g_i, g_j deux polynômes non nuls. Supposons que $c_i x^{\alpha(i)} g_i$ et $c_j x^{\alpha(j)} g_j$ ont pour multidegré δ. Alors

$$S(c_i x^{\alpha(i)} g_i, c_j x^{\alpha(j)} g_j) = x^{\delta - \gamma_{ij}} S(g_i, g_j),$$

avec $\gamma_{ij} = \text{ppcm}(LM(g_i), LM(g_j))$.

Critère de Buchberger

Théorème

Soient I un idéal de $k[x_1, \ldots, x_n]$ et $G = \{g_1, \ldots, g_t\}$ une base de I.

G est une base de Gröbner de I ssi pour toute paire $i \neq j$ le reste de la division de $S(g_i, g_j)$ par G avec un certain ordre est nul.

Proposition

Étant donné deux polynômes f et g, et $x^\gamma = \text{ppcm}(LM(f), LM(g))$, alors

$$\text{multideg}(S(f, g)) < \gamma.$$