Appunti per Geometria e Algebra Computazionale
3. S-coppie e algoritmo di Buchberger

Corso di Laurea in Matematica, Università di Firenze, 2019/20

Giorgio Ottaviani

20 marzo 2020

S-coppie

Definizione

Siano $f, g \in K[x_1, \ldots, x_n]$ *e sia* $x^\gamma = m.c.m.(\mathrm{LT}(f), \mathrm{LT}(g))$.
Definiamo la S-coppia:

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

Notiamo che in $S(f,g)$ i termini di multigrado γ si cancellano mentre tutti gli altri termini hanno multigrado $< \gamma$. Pertanto

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

Esempio $S(x^2+y^2, xy) = y(x^2+y^2) - x(xy) = y^3$

S-coppie danno ostruzioni affinché un insieme di generatori sia base di Gröbner

Una "ostruzione" a che $\{f_1, \ldots, f_h\}$ sia una base di Gröbner è

$$LT\left(S(f_i, f_j)\right) \notin \left(LT(f_1), \ldots, LT(f_h)\right)$$

Vedremo che questa è in sostanza l'unica ostruzione.

Ogni cancellazione tra LT viene da una S-coppia, I

Lemma

Supponiamo di avere una cancellazione tra i LT di un insieme di polinomi g_i. Cioè supponiamo di avere una combinazione $\sum_{i=1}^{t} c_i x^{\alpha_i} g_i$ *con* $c_i \in K$, $\alpha_i + \mathrm{MULTIDEG}\ g_i = \delta$ *(se* $c_i \neq 0$*) e* $\mathrm{MULTIDEG}\ (\sum c_i x^{\alpha_i} g_i) < \delta$. *Allora, posto* $x^{\gamma_{jk}} := m.c.m.(\mathrm{LT}(g_j), \mathrm{LT}(g_k))$ *esistono* c_{jk} *tali che*

$$\sum_{i=1}^{t} c_i x^{\alpha_i} g_i = \sum_{j,k=1}^{t} c_{jk} x^{\delta-\gamma_{jk}} S(g_j, g_k)$$

In particolare ogni termine del secondo membro ha multigrado $< \delta$

Dimostrazione Poniamo $LT(g_i) := d_i x^{\beta_i}$, quindi

$$\alpha_i + \beta_i = \delta \tag{0.1}$$

$$\sum_{t} c_i d_i = 0 \tag{0.2}$$

Ogni cancellazione tra LT viene da una S-coppia, II

Adesso $x^{\delta-\gamma_{jk}} S(g_j, g_k) = x^{\delta-\gamma_{jk}} \left(\frac{x^{\gamma_{jk}} g_j}{d_j x^{\beta_j}} - \frac{x^{\gamma_{jk}} g_k}{d_k x^{\beta_k}} \right)$ = (per **??**) = $\frac{x^{\alpha_j} g_j}{d_j} - \frac{x^{\alpha_k} g_k}{d_k}$

Quindi $\sum_{i=1}^{t} c_i x^{\alpha_i} g_i = \sum_{i=1}^{t} c_i d_i \left(\frac{x^{\alpha_i} g_i}{d_i} \right)$ = (ponendo $g_{t+1} = 0$)

$= \sum_{i=1}^{t} c_i d_i \left(\sum_{j=i}^{t} \left(\frac{x^{\alpha_j} g_j}{d_j} - \frac{x^{\alpha_{j+1}} g_{j+1}}{d_{j+1}} \right) \right)$ = (scambiando le sommatorie)

$= \sum_{j=1}^{t} \sum_{i=1}^{j} c_i d_i \left(\frac{x^{\alpha_j} g_j}{d_j} - \frac{x^{\alpha_{j+1}} g_{j+1}}{d_{j+1}} \right)$ = (usando **??**)

$\sum_{j=1}^{t-1} \sum_{i=1}^{j} c_i d_i x^{\delta-\gamma_{j,j+1}} S(g_j, g_{j+1})$

come volevasi dimostrare

Il criterio di Buchberger

Teorema

(Criterio di Buchberger, 1965) Sia I un ideale di $K[x_1, \ldots, x_n]$ generato da $(g_1, \ldots, g_t)$. Sia fissato un ordine monomiale.

$$(g_1, \ldots, g_t) \text{ è una base di Gröbner per } I \iff \begin{array}{c} \text{il resto della divisione} \\ \text{di } S(g_i, g_j) \text{ per } (g_1, \ldots g_t) \\ \text{è zero } \forall i \neq j \end{array}$$

La divisione di $S(g_i, g_j)$ per $(g_1, \ldots g_t)$ può essere effettuata prendendo $g_1, \ldots, g_t$ in un ordine qualunque; segue in particolare che se il resto è zero in un ordine rimane zero in tutti gli altri ordini.

Dimostrazione del criterio di Buchberger,I

Dimostrazione

$\Rightarrow$ è ovvia da $S(g_i, g_j) \in I$ e dalle proprietà viste delle basi di Groebner.
$\Leftarrow$ Sia $f \in I$, voglio provare che $LT(f) \in < LT(g_1), \ldots, LT(g_t) >$. Per ipotesi abbiamo $f = \sum h_i g_i$ con MULTIDEG $(f) \leq max\,(\text{MULTIDEG}(h_i g_i))$. Sia δ il minimo tra tutte le espressioni $f = \sum h_i g_i$ di $max\,(\text{MULTIDEG}(h_i g_i))$, tale minimo esiste per la proprietà di buon ordinamento. Se MULTIDEG $f = \delta$ abbiamo concluso. Sia per assurdo MULTIDEG $f < \delta$ e poniamo $m(i) :=$ MULTIDEG $(g_i h_i)$.

Dimostrazione del criterio di Buchberger,II

Abbiamo:

$f = \sum h_i g_i =$ (dove il massimo MULTIDEG a secondo membro è δ)

$= \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i =$
$= \sum_{m(i)=\delta} LT(h_i) g_i + \sum_{m(i)=\delta} (h_i - LT(h_i))\, g_i + \sum_{m(i)<\delta} h_i g_i$
I monomi nella seconda e terza somma hanno MULTIDEG $< \delta$. Quindi nella prima somma abbiamo cancellazioni tra i LT dei g_i e possiamo applicare il lemma precedente. Pertanto possiamo riscrivere la prima somma come combinazione dei $S(g_j, g_k)$. A loro volta questi ultimi polinomi possono essere scritti nella forma $S(g_j, g_k) = \sum a_{ijk} g_i$ per l'algoritmo di divisione (l'ipotesi è resto zero!). Siccome $\mathrm{MULTIDEG}\ (a_{ijk} g_i) \leq \mathrm{MULTIDEG}\ S(g_j, g_k)$ (per l'algoritmo di divisione), risostituendo nell' espressione iniziale abbiamo $f = \sum h'_i g_i$ con tutti i multigradi a secondo membro $< \delta$. Pertanto δ non è il minimo. Questa contraddizione conclude il ragionamento.

Il criterio di Buchberger all'opera

Esempio

Proviamo che $\left(x - z^4, y - z^{10}\right)$ *è una base di Gröbner secondo Lex utilizzando il criterio di Buchberger. Abbiamo la sola S-coppia* $S(x - z^4, y - z^{10}) = \frac{xy}{x}(x - z^4) - \frac{xy}{y}(y - z^{10}) =$ $yx - yz^4 - xy + xz^{10} = xz^{10} - yz^4$. *La divisione porta a:*

$$
\begin{array}{lllll}
xz^{10} - yz^4 & |x - z^4 & |y - z^{10} & |RESTO \\
 & |\text{———} & |\text{———} & \\
xz^{10} - z^{14} & |z^{10} & |z^4 & \\
\text{———} & & & \\
-yz^4 + z^{14} & \longrightarrow & & 0 \\
yz^4 - z^{14} & & & \\
\text{———} & & & \\
0 & \longrightarrow & & 0
\end{array}
$$

Il resto è zero e quindi la condizione del criterio di Buchberger è verificata.

Commenti sulla dimostrazione del criterio di Buchberger

Osservazione critica.

Nel corso della dimostrazione dell'implicazione $\Leftarrow$ del criterio di Buchberger abbiamo scritto $S(g_j, g_k) = \sum a_{ijk} g_i$ usando l'algoritmo di divisione. Perché non si é fatto uso direttamente della definizione di $S(g_j, g_k)$ che lo esprime come combinazione di g_j e g_k? Il punto é che la disuguaglianza

$$\text{MULTIDEG } (a_{ijk} g_i) \leq \text{MULTIDEG } S(g_j, g_k)$$

non sarebbe stata soddisfatta!

Conseguenza del criterio di Buchberger

La dimostrazione del Criterio di Buchberger fornisce immediatamente il seguente rafforzamento del Criterio di Buchberger.

Corollario

Sia I un ideale di $K[x_1, \ldots, x_n]$ generato da $(g_1, \ldots, g_t)$. Sia fissato un ordine monomiale.

$$\begin{array}{c}(g_1, \ldots, g_t) \\ \textit{è una base di Gröbner per } I\end{array} \iff \begin{array}{l}\textit{esistono polinomi } a_{ijk} \textit{ t.c.} \\ S(g_j, g_k) = \sum_i a_{ijk} g_i \\ \mathrm{LT}\,(a_{ijk} g_i) \leq \mathrm{LT}\; S(g_j, g_k) \\ \forall i, j, k,\ i \neq j\end{array}$$

Esercizi sul criterio di Buchberger

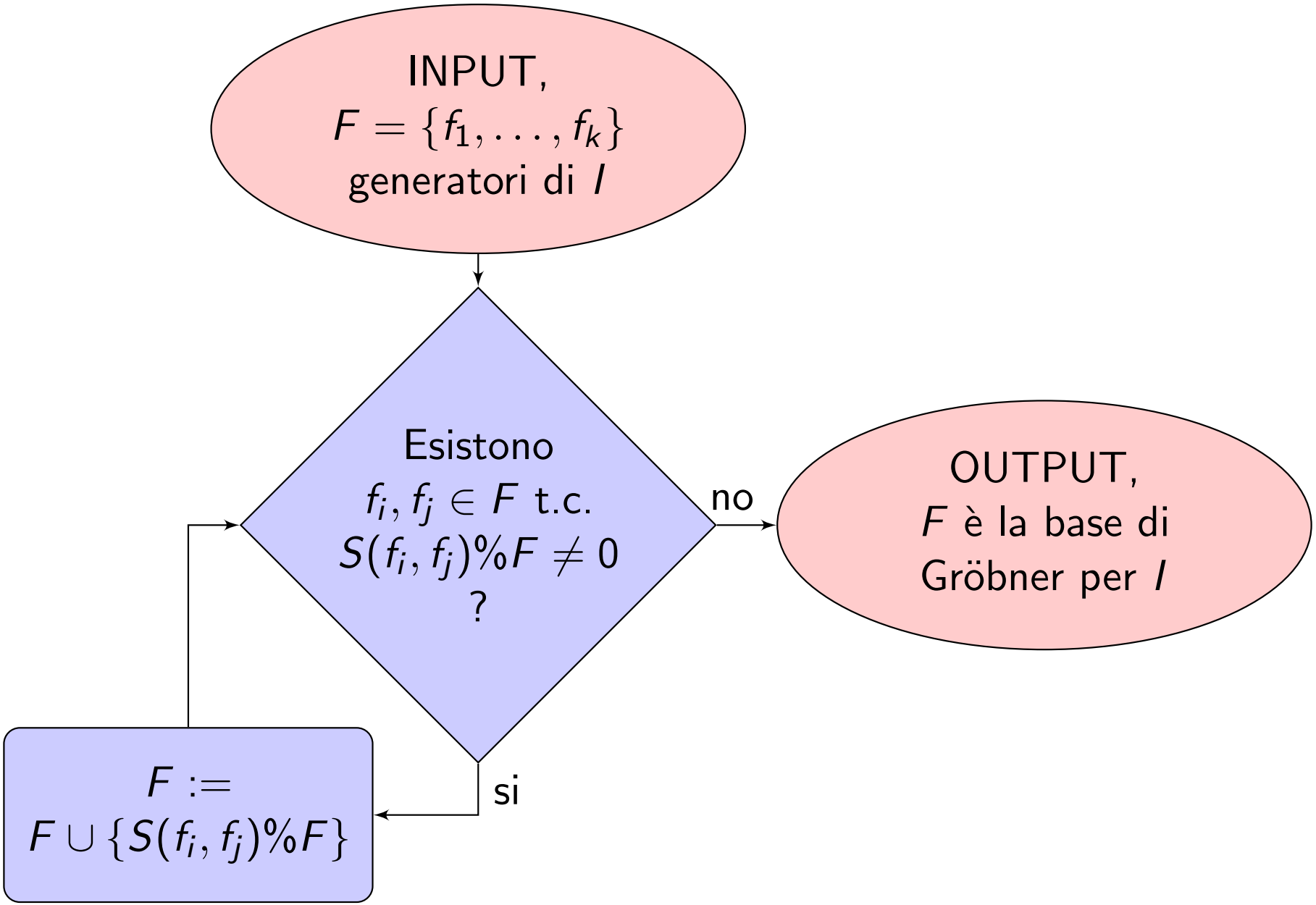
Esercizio

1. *Provare che* $G = \{x + z, y - z\}$ *è una base di Gröbner rispetto a Lex.*
2. *Dividere* xy *per* $x + z$, $y - z$ *(rispetto a Lex, si veda l'eserc. 1). Poi dividere* xy *per* $y - z$, $x + z$. *Nei due casi il resto è lo stesso, ma i quozienti sono differenti. Quindi questo esercizio mostra che non si riesce ad avere l'unicità dei quozienti, in contrasto col caso dei polinomi in una sola variabile. Concludere che la forma normale di* xy *rispetto a* $I = (x + z, y - z)$ *è* $-z^2$.
3. *Si calcoli* $S(f, g)$ *rispetto a Lex nei seguenti casi:*
   1. $f = 4x^2z - 7y^2, g = xyz^2 + 3xz^4$
   2. $f = x^4y - z^2, g = 3xz^2 - y$
   3. $f = x^7y^2z + 2ixyz, g = 2x^7y^2z + 4$
   4. $f = xy + z^3, g = z^2 - 3z$
4. $S(f, g)$ *dipende dall'ordine monomiale scelto?*

L'algoritmo di Buchberger

Il criterio di Buchberger suggerisce un algoritmo per costruire una base di Gröbner. Si considera $F = \{f_1, \ldots, f_k\}$ insieme di generatori di I. Indichiamo provvisoriamente con $f\%\ F$ il resto della divisione di f per gli elementi di F nell'ordine in cui sono scritti. Aggiungiamo ad F stesso tutti gli elementi $[S(f_i, f_j)\%\ F]$ e ripetiamo questa operazione col nuovo insieme F (più grande !). Continuando in questo modo si ottiene corrispondentemente una catena ascendente di ideali monomiali data ad ogni passo da $< LT(F) >$. Per Noetherianità la catena diventa stazionaria e questo vuol dire esattamente che dopo un certo numero di passi $[S(f_i, f_j)\%\ F] = 0 \quad \forall \quad i, j$ e quindi per il criterio di Buchberger quando l'algoritmo ha termine F è una base di Gröbner.

Diagramma di flusso dell'algoritmo di Buchberger.



Dimostrazione dell'algoritmo di Buchberger

Dimostrazione La notazione $S(f_i, f_j)\%F$ indica il resto della divisione della S-coppia $S(f_i, f_j)$ per tutti gli elementi di F. Il fatto che l'output è una base di Gröbner è garantito dal criterio di Buchberger, che è verificato esattamente quando la risposta al test di esistenza di (f_i, f_j) è NO. Il ciclo non può essere percorso infinite volte, perché ad ogni passo l'ideale monomiale $< LT(F) >$ contiene strettamente l'ideale monomiale del passo precedente. Non si può ottenere una catena ascendente infinita di ideali, perché $K[x_1, \ldots, x_n]$ è noetheriano.

Osservazione importante sull'algoritmo di Buchberger

L'algoritmo permette di avere delle espressioni esplicite $g_i = \sum_{j=1}^{k} a_{ij} f_j$, di ciascun elemento della base di Gröbner in funzione dei generatori. Infatti, ogni elemento che viene aggiunto ad F, ad ogni passo, si può esprimere come combinazione degli elementi già presenti in F. Per esempio, se $F = \{f_1, \ldots, f_p\}$, abbiamo dall'algoritmo di divisione $[S(f_i, f_j)\%F] = S(f_i, f_j) - \sum_{i=1}^{p} q_i f_i$ e anche $S(f_i, f_j)$ è combinazione di elementi di F.

Esercizi sull'algoritmo di Buchberger

1. Si trovi una base di Gröbner per l'ideale $I = (x^2 + y^2, xy)$ rispetto a Lex utilizzando l'algoritmo di Buchberger.
2. Sia $A = (a_{ij})$ una matrice $n \times m$ a scala a coefficienti reali e sia $J \subset \mathbb{R}[x_1, \ldots, x_m]$ l'ideale generato dai polinomi $f_i = \sum_{j=1}^{m} a_{ij} x_j$ per $1 \leq i \leq n$. Provare che $LT(J)$ è generato dalle variabili dei pivot. Provare che i generatori di J formano una base di Gröbner rispetto all'ordine Lex dove $x_1 > x_2 > \ldots$. *Suggerimento: ogni monomio di $S(f_i, f_j)$ è divisibile per almeno una variabile di un pivot.*
3. Sia $A = (a_{ij})$ una matrice $n \times m$ a coefficienti reali e sia $J \subset \mathbb{R}[x_1, \ldots, x_m]$ l'ideale generato dai polinomi $\sum_{j=1}^{m} a_{ij} x_j$ per $1 \leq i \leq n$. Provare che $LT(J)$ è generato dalle variabili dei pivot di una riduzione a scala di A.
4. Sia $I = (f, g) \subset K[x]$ un ideale nell'anello dei polinomi nella variabile x. Provare che $LT(I)$ è generato da $LT(\mathrm{GCD}(f, g))$ e che l'algoritmo di Buchberger si riconduce essenzialmente all'algoritmo euclideo.

Algoritmo per il calcolo della forma normale rispetto a un ideale

Questo algoritmo è una sorta di *divisione "intelligente"* per polinomi in più variabili. Fissiamo un ordine monomiale. Dati $f, f_1, \ldots, f_h \in K[x_1, \ldots, x_n]$, denotiamo con I l'ideale generato da $(f_1, \ldots, f_h)$, si costruiscono $q_1, \ldots, q_h, r \in K[x_1, \ldots, x_n]$ tali che

$$f = \sum_{i=1}^{h} f_i q_i + r, \quad \text{dove}$$

- nessun termine di r appartiene a $LT(I)$.

In particolare, r è la forma normale di f rispetto a I, denotata con $f\%I$, e implementata in *Macaulay2* con questa stessa sintassi. Notiamo che l'equivalenza

$$f \in I \iff (f\%I = 0)$$

permette di risolvere in modo effettivo il *problema di appartenenza* di f ad I.

Passi dell'algoritmo

1. Si calcola una base di Gröbner $G = \{g_1, \ldots, g_s\}$ di I mediante l'algoritmo di Buchberger.
2. L'algoritmo permette anche di avere delle espressioni

$$g_i = \sum_{j=1}^{h} a_{ij} f_j \tag{0.3}$$

3. Si divide f per $\{g_1, \ldots, g_s\}$, ottenendo

$$f = \sum_{i=1}^{s} q'_i g_i + r \tag{0.4}$$

   dove nessun termine di r è divisibile per $LT(g_1), \ldots LT(g_s)$. Dato che G è una base di Gröbner, segue che nessun termine di r appartiene a $LT(I)$.
4. Si sostituiscono le espressioni (**??**) nella formula (**??**).

Implementazione in Macaulay2 della forma normale rispetto a un ideale.

Divisione "intelligente"

Questo algoritmo è implementato in *Macaulay2*, con il comando

```
(q,r)=quotientRemainder(matrix{{f}},matrix{{f_1,..., f_h}})
```

Nell'output, q è una matrice che contiene i quozienti $q_1, ...q_h$ e r è il resto.

Esercizi

1. Determinare se $f = xy^3 - z^2 + y^5 - z^3$ appartiene all'ideale $I = (-x^3 + y, x^2y - z)$.Suggerimento: utilizzando GRevLex la base di Gröbner di I é costituita da 3 elementi, mentre utilizzando Lex o GLex i calcoli sono piú complessi.
2. Determinare se $f = x^3z - 2y^2$ appartiene all'ideale $I = (xz - y, xy + 2z^2, y - z)$.