Università degli studi di Trento

Dipartimento di Matematica

Laurea triennale in Matematica

Teorema della base di Hilbert e basi di Gröbner

Relatrice:
Alessandra Bernardi

Laureanda:
Maria Ricci

26 settembre 2016

Introduzione

In questa tesi presentiamo un problema classico in algebra computazionale: dato un anello di polinomi in n variabili R a valori in un campo K, e un ideale $I \in R$, determinare se un polinomio f appartiene o meno a I. Se $R = K[x_1, \ldots, x_n]$, la soluzione è immediata, una volta risolto un secondo problema, ovvero la divisione tra polinomi. Nel caso $n = 1$, infatti, grazie all'unicità del resto dell'algoritmo di divisione, quest'ultimo è sufficiente come soluzione al problema: ne presentiamo la versione classica nella prima sezione, dopo alcuni risultati preliminari. Per $n \geq 2$ le cose si complicano, dal momento che non è più assicurata l'unicità del resto nella divisione. Tuttavia il problema è stato completamente risolto, grazie alla teoria delle basi di Gröbner, sviluppata da Bruno Buchberger a partire dalla sua tesi di dottorato [1]. Nella seconda parte dunque generalizziamo l'algoritmo di divisione tra polinomi da una a n variabili e introduciamo le basi di Gröbner, le quali forniscono un metodo di divisione che garantisce l'unicità del resto e rispondono esaustivamente al problema. Infine presentiamo una versione elementare e una più avanzata di un algoritmo per calcolare una base di Gröbner. Dove non altrimenti specificato, la teoria e gli esempi sono tratti da [2].

Indice

1 Problema dell'appartenenza in $K[x]$

1.1 Teorema della base di Hilbert

Definizione 1.1. Un anello A si dice *notheriano* se soddisfa una delle seguenti condizioni equivalenti:

(i) l'insieme degli ideali di A soddisfa la condizione della catena ascendente (*A.C.C.*): ogni catena ascendente di ideali

$$I_1 \subset I_2 \subset \cdots \subset I_k \subset \ldots$$

si arresta, ovvero $I_k = I_{k+1} = \ldots$ per qualche k;

(ii) ogni insieme non vuoto di ideali ammette un elemento massimale;

(iii) ogni ideale di A è finitamente generato.

Una dimostrazione dell'equivalenza si può trovare in [4].

La noetherianità degli anelli di polinomi è fondamentale per la terminazione degli algoritmi.

Teorema 1.1 (Teorema della base di Hilbert)**.** *L'anello di polinomi in una variabile $A[x]$ di un anello noetheriano A è noetheriano.*

Dimostrazione (Sarges [3]). Assumiamo per assurdo che $A[x]$ non sia noetheriano, quindi esiste I ideale di $A[x]$ non finitamente generato. Sia $f_1 \neq 0$ un polinomio di grado minimo tra quelli in I, dunque $(f_1) \subseteq I$. Prendiamo poi un secondo polinomio $f_2 \neq 0$ in $I \setminus (f_1)$ di grado minimo e procediamo così per induzione: se abbiamo trovato $f_1, \ldots, f_k \in I$ non nulli, prendiamo $f_{k+1} \in I \setminus (f_1, \ldots, f_k)$ $\forall k \in \mathbb{N}^*$. Poiché I non è finitamente generato otteniamo una sequenza infinita di polinomi. Se a_i è il coefficiente direttore di f_i (si veda la Definizione 2.5 più avanti) e $\deg(f_i) = n_i$, abbiamo per costruzione $n_1 \leq n_2 \leq \ldots$ e otteniamo una catena ascendente di ideali in A:

$$(a_1) \subsetneq (a_1, a_2) \subsetneq \cdots$$

Mostriamo che questa catena non è stazionaria, giungendo all'assurdo. Se fosse stazionaria $\exists\, a_h$ tale che $(a_1, \ldots, a_h) = (a_1, \ldots, a_{h+1})$ e dunque $a_{h+1} = \sum_{i=1}^{h} a_i b_i$ per certi $b_i \in A$, ma allora $f_{h+1} - \sum_{i=0}^{h} f_i x^{n_{h+1}-n_i} b_i$ sarebbe un polinomio in $I \setminus (f_1, \ldots, f_h)$ di grado strettamente minore di f_{h+1}, il che contraddice le ipotesi su f_{h+1}. Ne segue che la catena non è stazionaria, ma questo è assurdo perché A è noetheriano. □

Corollario 1.2. *Se A è un anello noetheriano, allora anche $A[x_1, \ldots, x_n]$ è un anello noetheriano.*

Dimostrazione. Sarà sufficiente procedere per induzione, ricordando che $A[x_1, \ldots, x_{n-1}][x_n] = A[x_1, \ldots, x_n]$: per il Teorema della base di Hilbert 1.1, A noetheriano implica $A[x_1]$ notheriano e quindi $A[x_1][x_2] = A[x_1, x_2]$ noetheriano eccetera. □

1.2 Teorema di scomposizione in fattori irriducibili in $K[x]$

Sia K un campo e $I \subseteq K[x]$ un suo ideale. L'anello $K[x]$ è noetheriano, poiché ogni campo è banalmente noetheriano. Con il prossimo teorema vedremo di più: ogni ideale di $K[x]$ è generato da un unico elemento. Un anello con questa proprietà viene detto *dominio a fattorizzazione unica*, o PID. Questo fatto, unito al Teorema della base di Hilbert 1.1, dimostra che $K[x]$ è un *dominio a fattorizzazione unica* (UFD), perciò se nella fattorizzazione di un polinomio f compare un certo elemento $g \in K[x]$ allora $f \in (g)$. Questa è la soluzione al Problema 1 per polinomi in una variabile.

Teorema 1.3. *Sia $f \in K[x]$ un polinomio di grado positivo e sia $c \in K$ il coefficiente direttore di f. Quindi esistono polinomi monici irriducibili distinti $p_1, \dots, p_r \in K[x]$ e interi positivi $m_1, \dots, m_r$ tali che $f = cp_1^{m_1} \cdots p_r^{m_r}$. Inoltre se esistono altri polinomi irriducibili distinti $q_1, \dots, q_s \in K[x]$ ed interi positivi $n_1, \dots, n_s$ tali che $f = cq_1^{n_1} \cdots q_s^{n_s}$, allora $r = s$ e si possono permutare i termini $q_1^{n_1} \cdots q_s^{n_s}$ in maniera tale che $p_1 = q_1, \dots, p_r = q_r$ e $m_1 = n_1, \dots, m_r = n_r$.*

Dimostrazione. • *K campo dunque $K[x]$ è un PID.*
Sia I un ideale di $K[x]$ e sia f un polinomio di grado minimo in I: chiaramente $(f) \subseteq I$. Viceversa, sia $g \in I \setminus (f)$, per cui $\deg(g) \geq \deg(f)$. Tramite l'algoritmo di divisione euclideo ($K[x]$ è *euclideo*, grazie alla funzione grado $deg : K[x] \to \mathbb{N}$, che manda un polinomio $f(x) \in K[x]$ nel suo grado $\deg(f) \in \mathbb{N}$) possiamo scrivere:

$$g = fq + r \text{ con } q, r \in K[x] \text{ e } \deg(r) < \deg(f)$$

osserviamo però che $r = g - fq$ e f, $g \in I$ che è un ideale, perciò $r \in I$ e $r = 0$ per minimalità di f, dunque $g = fq$ e $I = (f)$.

- *$K[x]$ è un UFD.*
Ogni PID è un UFD: mostriamo che $K[x]$ è principalmente noetheriano (ogni ideale principale soddisfa l'*A.C.C.*) e ogni elemento irriducibile è primo. La prima affermazione è banalmente vera: ogni PID è noetheriano e dunque principalmente noetheriano. Sia ora $p \in K[x]$ irriducibile. Supponiamo che $p|ab$ ma $p \nmid a$ per certi $a, b \in K[x]$ non nulli e non invertibili. L'ideale (p) è massimale: se $\exists\, J \subseteq K[x]$ tale che $(p) \subseteq J$ allora $J = (d)$ per un qualche $d \in K[x]$ e $(p) \subseteq (d)$ ossia $d|p$. Quindi o d è associato a p da cui $(p) = J$ oppure d è invertibile e $(d) = K[x]$. Poiché $p \nmid a$ allora $a \notin (p)$ da cui segue che $(p, a) = K[x]$, dunque $\exists\, u, v \in K[x]$ tali che $pu + av = 1$ per cui si può scrivere $pub + avb = b$. Abbiamo trovato che $p|b$.

- Osserviamo infine che se c è il coefficiente direttore di f, allora

$$f = cx^n + \sum_{i=0}^{n-1} c_i x^i \in K[x],\ c \in K \tag{1}$$

e c è invertibile. Possiamo allora scrivere

$$f = c\left(x^n + \sum_{i=0}^{n-1} \frac{c_i}{c^{-1}} x^i\right) =: cg \tag{2}$$

dove g è un polinomio monico in $K[x]$, che possiede una fattorizzazione unica in polinomi monici irriducibili: $g = p_1^{m_1} \cdots p_r^{m_r}$, dunque $f = cp_1^{m_1} \cdots p_r^{m_r}$ è la fattorizzazione (unica) di f.

□

Teorema 1.4. *Il polinomio $(x-a) \in K[x]$, $a \in K$, divide $f \in K[x]$ se e solo se $f(a) = 0$.*

Dimostrazione. Naturalmente $(x-a)$ divide f, da cui esiste $g \in K[x]$ tale che $f = (x-a)g$. Ne segue che $f(a) = g(a)(a-a) = 0$.
Viceversa, se $f(a) = 0$ e $f = (x-a)q + r$ per opportuni $q, r \in K[x]$ allora
$0 = f(a) = 0 + r(a)$, ma $\deg(r) < \deg((x-a)) = 0$ perciò $\deg(r) = 0$ e $r \in K$, ovvero $r = 0$. □

Corollario 1.5. *Per controllare se un polinomio $f \in K[x]$ appartiene ad un dato ideale $I = (p)$ è sufficiente controllare se $p|f$. Per fare questo si può usare il seguente algoritmo di divisione in una variabile.*

Algoritmo 1

Input: g, f
Output: q, r

1: **while** $r \neq 0$ **and** $LT(g)$ divide $LT(r)$ **do**
2: $\quad q := q + \frac{LT(r)}{LT(g)}$
3: $\quad r := r - \frac{LT(r)}{LT(g)} g$
4: **end while**

Esempio 1.2. Proviamo a vedere se $f = 2x^3+3x^2-5x-4 \in I \subset K[x]$ con $I = (x^2-x-1)$. Tramite l'Algoritmo 1 otteniamo:

$$\begin{array}{r|l} & 2x+5 \\ \hline x^2-x-1 & 2x^3+3x^2-5x-4 \\ & -2x^3+2x^2+2x \\ \hline & 5x^2-3x-4 \\ & -5x^2+5x+5 \\ \hline & 2x+1 \end{array}$$

Il resto della divisione è non nullo, perciò $f = 2x^3 + 3x^2 - 5x - 4 \notin I$.

2 Problema dell'appartenenza in $K[x_1, \ldots, x_n]$

Problema 1 (Ideal membership problem)**.** Sia I un ideale in un anello di polinomi $K[x_1, \ldots, x_n]$, dove K è un campo, e sia f un polinomio. Come stabilire se f appartiene ad I?

L'anello $K[x_1, \ldots, x_n]$ è ancora noetheriano e a fattorizzazione unica, ma non è un PID, quindi non vale un analogo del Corollario 1.5. In questa sezione vediamo che esiste tuttavia un algoritmo di divisione in più variabili che ci permette di scrivere una fattorizzazione di f, con un eventuale resto, imponendo alcune condizioni sui termini direttori dei polinomi. Proseguiamo mostrando che è sempre possibile estrarre da I un opportuno sistema di generatori (una *base di Gröbner*) per cui il resto è unico, e questo sarà il criterio per stabilire se $f \in I$ o meno.

2.1 Ordini monomiali

Definizione 2.1. Un **ordine monomiale** su $K[x_1, \ldots, x_n]$ è una relazione " $>$ " su $\mathbb{Z}^n_{\geq 0}$ o, equivalentemente, ogni relazione sull'insieme dei monomi x^α, $\alpha \in \mathbb{Z}^n_{\geq 0}$, che soddisfa:

1. " $>$ " è un *ordine totale* su $\mathbb{Z}^n_{\geq 0}$: per ogni coppia di monomi x^α, x^β vale alternativamente $x^\alpha > x^\beta$, $x^\alpha < x^\beta$, $x^\alpha = x^\beta$;

2. se $\alpha > \beta$ e $\gamma \in \mathbb{Z}^n_{\geq 0}$, allora $\alpha + \gamma > \beta + \gamma$;

3. " $>$ " è un *buon ordinamento*: ogni sottoinsieme non vuoto di $\mathbb{Z}^n_{\geq 0}$ ammette minimo rispetto a " $>$ ".

Esempio 2.2 (Ordine lessicografico `LEX`)**.** Siano $\alpha = (\alpha_1, \ldots, \alpha_n)$ e $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{Z}^n_{\geq 0}$. Si dice che $\alpha >_{lex} \beta$ se nel vettore differenza $\alpha - \beta \in \mathbb{Z}^n_{\geq 0}$ la prima entrata non nulla da sinistra è positiva. Scriveremo $x^\alpha >_{lex} x^\beta$ se $\alpha >_{lex} \beta$.
Mostriamo che l'ordine lessicografico è un ordine monomiale.

Osserviamo che l'ordine lessicografico su $\mathbb{Z}^n_{\geq 0}$ si riduce all'ordine naturale in $\mathbb{Z}_{\geq 0}$ sul $k+1$-esimo termine di α e β se $\alpha_i - \beta_i = 0 \ \forall i \in 1, \ldots, k$.

1. Supponiamo che $\alpha_i - \beta_i$ sia la prima entrata da sinistra non nulla del vettore $(\alpha_1, \ldots, \alpha_n) - (\beta_1, \ldots, \beta_n)$: ora l'ordinamento è su $\mathbb{Z}_{\geq 0}$ dunque vale alternativamente $\alpha_i > \beta_i$, $\alpha_i < \beta_i$, $\alpha_i = \beta_i$; ne segue che $>_{lex}$ è un ordine totale.

2. Supponiamo $\alpha >_{lex} \beta$ e $\gamma \in \mathbb{Z}^n_{\geq 0}$. Si ha $((\alpha + \gamma) - (\beta + \gamma)) = ((\alpha_1 + \gamma_1) - (\beta_1 + \gamma_1), \ldots, (\alpha_n + \gamma_n) - (\beta_n + \gamma_n)) = (\alpha_1 - \beta_1, \ldots, \alpha_n - \beta_n) = \alpha - \beta$ perciò $\alpha >_{lex} \beta$ da cui $\alpha + \gamma >_{lex} \beta + \gamma$.

3. Sia $S := \{\alpha_j\}_{j \in \Lambda}$, $\Lambda \neq \emptyset$ un sottoinsieme non vuoto di $\mathbb{Z}^n_{\geq 0}$. Per il principio del minimo esiste un elemento minimale in S, e questo si trova ordinando in $\mathbb{Z}_{\geq 0}$ i k-esimi termini di $\{\alpha_j = (\alpha_{j1}, \ldots, \alpha_{jn})\}$ tra gli α_j che hanno un minimo nell'entrata $(k-1)$-esima $\forall k = 2, \ldots, n$.

Esempio 2.3 (Ordine lessicografico graduato `GRLEX`)**.** Siano α, $\beta \in \mathbb{Z}^n_{\geq 0}$. Con $|\alpha|$ indichiamo $\sum_{i=1}^n \alpha_i$. Diciamo che $\alpha >_{grlex} \beta$ se $|\alpha| > |\beta|$, oppure se $|\alpha| = |\beta|$ e $\alpha >_{lex} \beta$.
Mostriamo che l'ordine lessicografico graduato è un ordine monomiale.

La funzione $\mathbb{Z}^n_{\geq 0} \ni \alpha \longrightarrow |\alpha| = \sum_{i=1}^n \alpha_i \in \mathbb{Z}_{\geq 0}$ è un omomorfismo di gruppi, dunque:

1. $|\alpha| > |\beta|$ in $\mathbb{Z}_{\geq 0}$ implica $\alpha >_{grlex} \beta$ in $\mathbb{Z}^n_{\geq 0}$ e da $|\alpha| < |\beta|$ segue $\beta >_{grlex} \alpha$; nel caso $|\alpha| = |\beta|$ `GRLEX` si riduce a `LEX`.

2. Poiché $|\alpha| + |\gamma| = \sum_{i=1}^n \alpha_i + \sum_{i=1}^n \gamma_i = \sum_{i=1}^n (\alpha_i + \gamma_i) = |\alpha + \gamma|$ e abbiamo già visto da $\alpha >_{lex} \beta$ segue $\alpha + \gamma >_{lex} \beta + \gamma$, se $\alpha >_{grlex} \beta$ allora $\alpha + \gamma >_{grlex} \beta + \gamma$.

3. Se $S := \{\alpha_j\}_{j \in \Lambda}$ è un sottoinsieme non vuoto di $\mathbb{Z}^n_{\geq 0}$, allora, a meno di riordino degli indici, abbiamo:
$$\alpha_1 \geq_{grlex} \alpha_2 \geq_{grlex} \cdots \geq_{grlex} \alpha_k \geq_{grlex} \cdots \tag{3}$$
e dunque in $\mathbb{Z}_{\geq 0}$:
$$|\alpha_1| \geq |\alpha_2| \geq \cdots \geq |\alpha_k| \geq \cdots \tag{4}$$
e questa catena ammette un minimo, cioè esiste un $n_0 \in \mathbb{N}$ per cui $|\alpha_n| = |\alpha_{n_0}| \forall n > n_0$; da n_0 in poi ricadiamo nell'ordine lessicografico, che è un buon ordinamento, dunque S ammette minimo.

Esempio 2.4 (Ordine lessicografico graduato inverso `DEGREVLEX`)**.** Siano α, $\beta \in \mathbb{Z}^n_{\geq 0}$. Diciamo che $\alpha >_{degrevlex} \beta$ se $|\alpha| > |\beta|$ o $|\alpha| = |\beta|$ e la prima entrata non nulla da destra in $\alpha - \beta$ è non negativa.
Mostriamo che l'ordine lessicografico graduato inverso è un ordine monomiale.

1. Se $|\alpha|$ è maggiore o minore di $|\beta|$ vale lo stesso discorso di `GRLEX`. Quando $|\alpha| = |\beta|$, l'ordine si riduce a quello in $\mathbb{Z}_{\geq 0}$: infatti, sia $\alpha_i - \beta_i$ la prima entrata non nulla da destra di $\alpha - \beta$; se $\alpha_i - \beta_i > 0$ allora $\alpha >_{degrevlex} \beta$, mentre se, al contrario, $\alpha_i - \beta_i < 0$ abbiamo $\beta >_{degrevlex} \alpha$; da ultimo, se il vettore differenza $\alpha - \beta$ è nullo, allora $\alpha =_{degrevlex} \beta$.

2. È sufficiente verificare il caso $\alpha >_{degrevlex} \beta$ e $|\alpha| = |\beta|$: se $\alpha_i - \beta_i$ è la prima entrata non nulla da destra di $\alpha - \beta$ allora lo sarà anche di $(\alpha + \gamma) - (\beta + \gamma)$: infatti $((\alpha_i + \gamma_i) - (\beta_i + \gamma_i)) = \alpha_i - \beta_i$ mentre $((\alpha_k + \gamma_k) - (\beta_k + \gamma_k)) = ((\alpha_k - \beta_k) + (\gamma_k - \gamma_k)) = 0 \ \forall k = i + 1 \ldots n$, dunque anche in questo caso $\alpha >_{degrevlex} \beta$ implica $\alpha + \gamma >_{degrevlex} \beta + \gamma$.

3. Come nell'esempio precedente, se $S := \{\alpha_j\}_{j \in \Lambda}$ è un sottoinsieme non vuoto di $\mathbb{Z}^n_{\geq 0}$, nella catena in $\mathbb{Z}_{\geq 0}$
$$|\alpha_1| \geq |\alpha_2| \geq \cdots \geq |\alpha_k| \geq \cdots \tag{5}$$
abbiamo l'uguaglianza da un certo n_0 in poi; ora il minimo in $\{\alpha_n\}_{n \geq n_0}$ è dato dall'elemento α_j che ha la prima entrata da destra non nulla minima, cioè tale che $\forall n \ \alpha_{ji} < \alpha_{ni}$ dove i è la prima entrata non nulla da destra di α_n.

Definizione 2.5. Sia $f = \sum_\alpha a_\alpha x^\alpha$, $f \in K[x_1, \ldots, x_n]$ e sia " $>$ " un ordine monomiale. Si danno le seguenti definizioni:

- il **multigrado** di f è $\text{multideg}(f) = \max_>\{\alpha \in \mathbb{Z}^n_{\geq 0} | a_\alpha \neq 0\}$;
- il **coefficiente direttore** di f è:

$$LC(f) = a_{\text{multideg}(f)} \in K \tag{6}$$

- il **monomio direttore** di f è:

$$LM(f) = x^{\text{multideg}(f)} \tag{7}$$

- il **termine direttore** di f è:

$$LT(f) = LC(f) \cdot LM(f) \tag{8}$$

Esempio 2.6. Scriviamo $\text{multideg}(f)$, $LC(f)$, $LM(f)$ e $LT(f)$ di $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2 \in K[x, y, z]$ per `LEX`, `GRLEX` e `DEGREVLEX` rispettivamente. Definiamo i gradi corrispondenti a ciascun monomio: $\alpha_1 := (1, 2, 1)$, $\alpha_2 := (0, 0, 2)$, $\alpha_3 := (3, 0, 0)$, $\alpha_4 := (2, 0, 2)$.

`LEX`: Si ha chiaramente $\alpha_3 >_{lex} \alpha_4 >_{lex} \alpha_1 >_{lex} \alpha_2$ e quindi $\text{multideg}(f) = (3, 0, 0)$, $LC(f) = -5$, $LM(f) = x^3$ e $LT(f) = -5x^3$

`GRLEX`: in questo caso abbiamo $|\alpha_1| = 4$, $|\alpha_2| = 2$, $|\alpha_3| = 3$, $|\alpha_4| = 4$, e $\alpha_4 >_{lex} \alpha_1$ per cui l'ordine è $\alpha_4 >_{grlex} \alpha_1 >_{grlex} \alpha_3 >_{grlex} \alpha_2$ e $\text{multideg}(f) = \alpha_4$, $LC(f) = 7$, $LM(f) = x^2z^2$ e $LT(f) = 7x^2z^2$

`DEGREVLEX`: poiché $\alpha_4 >_{degrevlex} \alpha_1$ l'ordine è uguale a quello di `GRLEX`.

2.2 Algoritmo della divisione in $K[x_1, \ldots, x_n]$

Fissato un ordine monomiale " $>$ " in $K[x_1, \ldots, x_n]$ e una s-upla di polinomi $(f_1, \ldots, f_s)$ in $K[x_1, \ldots, x_n]$, ogni polinomio f può essere scritto come $f = a_1 f_1 + \cdots + a_s f_s + r$ con $a_i, r \in K[x_1, \ldots, x_n]$; inoltre o $r = 0$ oppure r è una combinazione lineare a coefficienti in K di monomi nessuno dei quali è divisibile per alcun $LT(f_1), \ldots, LT(f_s)$. Se $a_i f_i \neq 0$ si ha che multideg$(f) \geq$ multideg$(a_i f_i)$. Il seguente algoritmo procede dividendo successivamente il resto ausiliario, che all'inizio è posto uguale a f, per $LT(f_1), \ldots, LT(f_s)$ e ha termine quando il resto ausiliario diventa nullo: questo accade sempre perché il multigrado del resto ausiliario decresce strettamente e l'ordine monomiale scelto è un buon ordinamento. Osserviamo che l'algoritmo non garantisce l'unicità della decomposizione o del resto.

Algoritmo 2

Input: $f_1, \ldots, f_s, f$
Output: $a_1, \ldots, a_s, r$

$a_1 := 0, \ldots, a_s := 0, r := 0$
$p := f$
while $p \neq 0$ **do**
  i:=1 divisibile := **false**
  while $i \leq s$ **and** divisibile = **false do**
    if $LT(f_i)$ divide $LT(p)$ **then**
      $a_i := a_i + \frac{LT(p)}{LT(f_i)}$
      $p := p - \frac{LT(p)}{LT(f_i)} f_i$
      divisibile := **true**
    else
      $i := i + 1$
    end if
  end while
  if divisibilie = **false then**
    $r := r + LT(p)$
    $p := p - LT(p)$
  end if
end while

Esempio 2.7. Testiamo l'algoritmo di divisione nei seguenti casi con l'ordine `LEX` $x > y$

1. $f = xy^2+1$ e $f_1 = xy+1$ e $f_2 = y+1$. I termini a_1, a_2 rappresentano rispettivamente i quozienti di f_1, f_2, riportati sulla sinistra, mentre sulla colonna di destra vengono

segnati i resti. Il dividendo è scritto sotto radice.

$$\begin{array}{rll} a_1: & x+y & \\ a_2: & 1 & \textit{resto} \\ xy+1 & \sqrt{xy^2+1} & \text{———} \\ y+1 & x^2y+y & \\ & \hline & \\ & 1-y & \\ & y-1 & \\ & \hline & \\ & 2 & \to 2 \end{array}$$

La decomposizione è $xy^2+1 = y(xy+1) - (y+1) + 2$.

2. Dividiamo ora, in due modi diversi, $f = x^2y+xy^2+y^2$ per $f_1 = xy-1$ e $f_2 = y^2-1$.

$$\begin{array}{rll} a_1: & x & \\ a_2: & x+1 & \textit{resto} \\ xy-1 & \sqrt{x^2y+xy^2+y^2} & \text{———} \\ y^2-1 & x^2y-x & \\ & \hline & \\ & xy^2+x+y^2 & \\ & xy^2-x & \\ & \hline & \\ & 2x+y^2 & \to 2x \\ & y^2 & \\ & \hline & \\ & y^2-1 & \\ & \hline & \\ & 1 & \to 1 \end{array}$$

Abbiamo diviso una volta per f_1 e due per f_2 e la decomposizione risulta $x^2y + xy^2 + y^2 = x(xy+1) + (x+1)(y^2-1) + 2x + 1$.
Dividiamo ora due volte per f_1 e una volta per f_2: in questo modo otteniamo una decomposizione diversa.

$$\begin{array}{rll} a_1: & x+y & \\ a_2: & 1 & \textit{resto} \\ xy-1 & \sqrt{x^2y+xy^2+y^2} & \text{————} \\ y^2-1 & x^2y-x & \\ & \hline & \\ & xy^2+x+y^2 & \\ & xy^2-y & \\ & \hline & \\ & x+y^2+y & \to x \\ & \hline & \\ & y^2+y & \\ & y^2-1 & \\ & \hline & \\ & y+1 & \to y+1 \end{array}$$

$$xy^2 + xy^2 + y^2 = (x + y)(xy - 1) + (y^2 - 1) + x + y + 1.$$

Sia ora $f = xy^2 - x$ e siano $f_1 = y^2 - 1$ e $f_2 = xy - 1$. Chiaramente $xy^2 - x = x(y^2 - 1) = xf_1$, dunque $f \in (f_1, f_2)$ ma se procediamo con l'Algoritmo 2 dividendo f dapprima per f_2 si trova che il resto della divisione è diverso da zero e non più divisibile per f_1 e f_2. Procediamo dividendo prima per f_2:

$$\begin{array}{rll} a_1: & 0 & \\ a_2: & y & \quad resto \\ xy-1 & \sqrt{xy^2 - x} & \quad \text{---------} \\ y^2-1 & x^2y - y & \\ & \text{---------} & \\ & -x + y & \to -x + y \end{array}$$

La fattorizzazione in questo modo è $xy^2 - x = y(xy - 1) + 0(y^2 - 1) - x + y$.
Da questo esempio possiamo capire che se il resto della divisione è nullo allora $f \in (f_1, \ldots, f_s)$ ma è falso il viceversa.

Osservazione 2.8. In tutti gli esempi precedenti i divisori erano della forma $x^\alpha + 1$ e il LT secondo l'ordine LEX era x^α. Si può vedere che questo vale in generale, più precisamente: per ogni ordine monomiale $x^\alpha > 1 \ \forall \alpha$. Se così non fosse avremmo $1 > x^\alpha$ per qualche α; ma allora, per la proprietà 2 in Definizione 2.1 degli ordini monomiali, moltiplicando per x^α si ottiene $x^\alpha > x^{2\alpha}$ e successivamente $x^\alpha > x^{2\alpha} > x^{3\alpha} > \ldots > x^{n\alpha} > \ldots$ ma questo è in contraddizione con il fatto che un ordine monomiale è un buon ordinamento.

2.3 Basi di Gröbner

Definizione 2.9. Sia fissato un ordine monomiale " $>$ " su $K[x_1, \ldots, x_n]$. Sia $I \subseteq K[x_1, \ldots, x_n]$ un ideale. Sia $G \subseteq I$, $G = \{g_1, \ldots, g_s\}$ una famiglia di elementi di I. La famiglia G è detta una **base di Gröbner** di I rispetto a " $>$ " se $(LT(g_1), \ldots, LT(g_s)) = (LT(I)) :=$ ideale generato dai termini direttori degli elementi di I.

Questa definizione è sensata perché, dato un ideale $I \in K[x_1, \ldots, x_n]$ e un suo qualsiasi sottoinsieme di polinomi $f_1, \ldots, f_t$, vale sempre $LT(f_1), \ldots, LT(f_t) \subset (LT(I))$, ma l'inclusione può essere stretta, come mostra il seguente

Esempio 2.10. Sia $I = (f_1, f_2, f_3) \subseteq \mathbb{R}[x, y, z]$ con $f_1 = xy^2 - xz + y$, $f_2 = xy + z^2$ e $f_3 = x - yz^4$. Fissiamo l'ordinamento lessicografico con $x > y > z$. Il polinomio $(xy^2 - xz + y) - (xy + z^2)y + (x - yz^4) = y + yz - yz^5$ appartiene ad I, ma il suo termine direttore è $LT(y + yz - yz^5) = y$, che di certo non appartiene a $(LT(f_1), LT(f_2), LT(f_3)) = (xy^2, xy, x)$.

In casi semplici è facile individuare una base di Gröbner.

Esempio 2.11. Sia $I = (g_1, g_2) \in \mathbb{R}[x, y, z]$ con $g_1 = x - z, g_2 = y + z$. Si ha $LT(g_1) = x$, $LT(g_2) = y$ con `LEX`; gli elementi g_1, g_2 formano una base di Gröbner: verifichiamo l'inclusione $(LT(I)) \subset (x, y)$. Se f appartiene ad I esistono $A(x, y, z), B(x, y, z) \in \mathbb{R}[x, y, z]$ tali che $f = A(x, y, z)(x - z) + B(x, y, z)(y + z)$, ovvero

$$f = A(x, y, z)x - A(x, y, z)z + B(x, y, z)y + B(x, y, z)z.$$

Se vale $LT(f) \notin (x, y)$, ovvero $LT(f)$ non è divisibile né per x né y, non può che essere $LM(f) = z^m$ per qualche $m \geq 0$. Ma allora non dovremmo avere monomi in x, y, ma questo è impossibile.

Definizione 2.12. Un ideale si dice *monomiale* se possiede un sistema di generatori costituito solo da monomi.

Il seguente risultato permette di dimostrare l'unicità del resto se l'insieme dei divisori è una base di Gröbner.

Teorema 2.1 (Lemma di Dickson)**.** *Sia $I \subset K[x_1, \ldots, x_n]$ un ideale monomiale. Allora I può essere scritto nella forma $I = (x^{\alpha(1)}, \ldots, x^{\alpha(s)})$ con $(\alpha(1), \ldots, \alpha(s)) \in \mathbb{Z}^n_{\geq 0}$. In particolare I ha una base finita.*

Dimostrazione. La dimostrazione procederà per induzione sul numero n di variabili.
Se $n = 1$, $K[x_1]$ è un PID: l'ideale $I = (x^\alpha : \alpha \in A \subset \mathbb{Z}_{\geq 0})$ è generato dall'unico monomio x^β tale che $\beta \leq \alpha \; \forall \alpha \in A$.
Supponiamo ora $n \geq 1$ e che la tesi sia vera per $n - 1$. Indicheremo per chiarezza $x_n =: y$ e di conseguenza i monomi come $x^\epsilon y^m$ con $\epsilon \in \mathbb{Z}^{n-1}_{\geq 0}$ e $m \in \mathbb{Z}_{\geq 0}$. Consideriamo quindi un ideale monomiale $I \subset K[x_1, \ldots, x_{n-1}, y]$ e la sua proiezione in $K[x_1, \ldots, x_{n-1}]$, $J := \{x^\epsilon : x^\epsilon y^m \in I\}$, ovvero generato dai monomi x^ϵ che moltiplicati per y^m stanno in I. L'ideale J è monomiale, dunque per ipotesi induttiva ha un numero finito di generatori: $J = (x^{\epsilon(1)}, \ldots, x^{\epsilon(s)})$. Per definizione di J, per ogni $i = 1 \ldots s$, esiste un $m_i \geq 0$ tale che $x^{\epsilon(i)} y^{m_i} \in I$; selezioniamo $m := \max\{m_i : i = 1 \ldots s\}$ e definiamo gli ideali

$$J_k \subset K[x_1, \ldots, x_{n-1}],\ J_k := \{x^\beta : x^\beta y^k \in I\} \text{ per ogni } k \text{ tra } 0 \text{ e } m - 1.$$

Questi ideali sono ancora monomiali e ricadono nell'ipotesi induttiva, perciò, per ogni k, $J_k = (x^{\epsilon_k(1)}, \ldots, x^{\epsilon_k(s_k)})$. Vediamo che I è generato dai seguenti monomi:

$$x^{\epsilon(1)} y^m, \ldots, x^{\epsilon(s)} y^m \qquad \text{da } J =: J_m$$

$$x^{\epsilon_0(1)}, \ldots, x^{\epsilon_0(s)} \qquad \text{da } J_0$$

$$x^{\epsilon_1(1)} y, \ldots, x^{\epsilon_1(s)} y \qquad \text{da } J_1$$

$$\ldots$$

$$\ldots$$

$$x^{\epsilon_{m-1}(1)} y^{m-1}, \ldots, x^{\epsilon_{m-1}(s)} y^{m-1} \qquad \text{da } J_{m-1}$$

infatti ogni monomio di I è divisibile per almeno un elemento della lista, per costruzione degli ideali J_k. Sia $x^\alpha y^p \in I$: se $p \geq m$ allora $x^\alpha y^p$ è divisibile per qualche $x^{\epsilon(i)} y^m$, mentre se $p \leq m - 1$ allora è divisibile per un $x^{\epsilon_p(j)} y^p$. Ne segue che i suddetti monomi generano un ideale contenente gli stessi monomi di I, dunque sono uguali. Resta da provare che l'insieme finito di generatori può essere estratto da un dato insieme di generatori dell'ideale, ovvero che, se $I = \{x^\alpha : \alpha \in A\}$ e $A \subset \mathbb{Z}^n_{\geq 0}$, allora I è generato da un numero finito di tali x^α. Abbiamo visto che $I = (x^{\beta(1)}, \ldots, x^{\beta(s)})$ per certi $x^{\beta(i)} \in I$. Ma allora ogni $x^{\beta(i)}$ è divisibile per un qualche $x^{\alpha(i)}$, $\alpha(i) \in A$. □

Esempio 2.13. Per vedere meglio come funziona la dimostrazione del Lemma di Dickson calcoliamo una base per l'ideale $I \in K[x, y]$, $I = (x^3y^6, x^5y^4, x^6)$ ordinato lessicograficamente. La proiezione di I in $K[x]$ è $J = (x^3)$; la massima potenza in cui compare y in I è $m = 6$, dunque le sezioni di I sono

$$J_0 = (x^6)$$

$$J_1 = J_2 = J_3 = \{0\}$$

$$J_4 = J_5 = (x^5)$$

ne segue che una base per I è data da $(x^3y^6, x^6, x^5y^4, x^5y^5)$.

2.4 Proprietà delle basi di Gröbner

Proposizione 2.2. *Sia $I \subseteq K[x_1, \ldots, x_n]$ un ideale. Allora*

1. *$(LT(I))$ è un ideale monomiale;*
2. *esistono $g_1, \ldots, g_s \in I$ tali che $(LT(I)) = (LT(g_1), \ldots, LT(g_s))$.*

Dimostrazione. 1. Se $K[x_1, \ldots, x_n]$ è noetheriano allora I è finitamente generato, dunque possiamo prendere come sistema di generatori $LT(f)$ per ogni $f \in I$;

2. Per il Lemma di Dickson 2.1 esistono $m_1, \ldots, m_s \in I$ tali che $(LT(I)) = (m_1, \ldots, m_s)$. Quindi $\{m_1, \ldots, m_s\} \subset (LT(I))$, perciò per ogni $i = 1, \ldots, s$, m_i è il termine direttore di qualche $g_i \in I$ (è sufficiente prendere $g_i = m_i + f_i$ con $f_i \in I$ e multideg$(f_i) \leq$ multideg(m_i)). Abbiamo trovato $g_1, \ldots, g_s \in I$ tali che $(LT(I)) = (LT(g_1), \ldots, LT(g_s))$.

□

Proposizione 2.3. *Sia $G = \{g_1, \ldots, g_t\}$ una G-base dell'ideale $I \subseteq K[x_1, \ldots, x_n]$ e sia $f \in K[x_1, \ldots, x_n]$, quindi esiste ed è unico $r \in K[x_1, \ldots, x_n]$ tale che*

(i) nessun termine di r è divisibile per uno dei $LT(g_i)$;

(ii) esiste $g \in I$ tale che $f = g + r$.

Dimostrazione. L'esistenza di un tale r è data dall'algoritmo di divisione visto nella sezione precedente: esistono $h_1, \ldots, h_t, r \in K[x_1, \ldots, x_n]$ tali che $f = h_1g_1 + \cdots + h_tg_t + r$ e $g := h_1g_1 + \cdots + h_tg_t$ appartiene a I perché $g_1, \ldots, g_t$ è una G-base. Per quanto riguarda l'unicità, supponiamo che $f = g + r = g' + r'$ con $g, g' \in I$; allora $r - r' = g' - g \in I$ e $LT(r - r') \in (LT(I))$. Ne segue che o $LT(r - r')$ è divisibile per qualche $LT(g_1), \ldots, LT(g_t)$, ma questo contraddice le ipotesi fatte su r e r', oppure $r = r'$. □

Corollario 2.4. *Sia $G = \{g_1, \ldots, g_t\}$ una G-base dell'ideale $I \subseteq K[x_1, \ldots, x_n]$ e sia $f \in K[x_1, \ldots, x_n]$. Si ha che $f \in I$ se e solo se il resto della divisione di f per G è 0.*

Dimostrazione. Abbiamo già visto che se il resto della divisione di f per $G = \{g_1, \ldots, g_t\}$ è nullo allora $f \in (g_1, \ldots, g_t) \subseteq I$. Viceversa, sia $f \in I$; per l'algoritmo della divisione possiamo sempre scrivere

$$f = \sum_{i=1}^{t} a_i g_i + r \text{ con } \ a_i, r \in K[x_1, \ldots, x_n]$$

dove r è il resto della divisione. Quindi $r = f - \sum_{i=1}^{t} a_i g_i \in I$, da cui $LT(r)$ è divisibile per almeno uno tra $LT(g_1), \ldots, LT(g_t)$, ma questo è assurdo per la definizione di r. Ne segue che $r = 0$. □

Dunque per risolvere il Problema 1 per un ideale I e un polinomio f in $K[x_1, \ldots, x_n]$ si usa l'Algoritmo 2, prendendo come insieme di divisori una G-base per I.

3 Algoritmo di Buchberger

Presentiamo qui una prima versione di un algoritmo per estrarre una base di Gröbner da un insieme di polinomi, basato sull'uso degli S-polinomi, di cui diamo subito la definizione.

Definizione 3.1. Siano f, g due polinomi non nulli in $K[x_1, \ldots, x_n]$; indichiamo con α e β i loro rispettivi multigradi. Sia $\gamma = (\gamma_1, \ldots, \gamma_n)$ con $\gamma_i = \max(\alpha_i, \beta_i)$ per ogni i. Il **minimo comune multiplo** di $LM(f)$ e $LM(g)$ è definito come

$$x^\gamma = LCM(LM(f), LM(g)).$$

L'**S-polinomio** di f e g è la combinazione

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

Esempio 3.2. Facciamo un esempio di un S-polinomio: siano $f = 4x^2z - 7y^2$ e $g = xyz^2 + 3xz^4$ in $\mathbb{R}[x, y, z]$. Secondo l'ordine lessicografico $LT(f) = 4x^2z, LT(g) = xyz^2$ e mentre il minimo comune multiplo è x^2yz^2, dunque:

$$S(f, g) = \frac{x^2yz^2}{4x^2z}4x^z - 7y^2 - \frac{x^2yz^2}{xyz^2}xyz^2 + 3xz^4 = -3x^2z^4 - \frac{7}{4}y^3z$$

e $LT(S(f, g)) = -3x^2z^4 <_{lex} x^2yz^2$.

Lemma 3.1. *Sia $\sum_{i=1}^{s} c_i f_i$ una somma di polinomi tali che multideg$(f_i) = \delta \in \mathbb{Z}^n_{\geq 0}$ per ogni i e $c_i \in K$. Se multideg$(\sum_{i=1}^{s} c_i f_i) < \delta$ allora la somma può essere scritta come combinazione lineare a coefficienti in K degli S-polinomi $S(f_j, f_k)$ per $1 \leq j, k \leq s$. Inoltre per ogni j, k vale multideg$(S(f_j, f_k) < \delta)$.*

Dimostrazione. Sia $d_i = LC(f_i)$. Poiché multideg$(\sum_{i=1}^{s} c_i f_i) < \delta$ ma
multideg$(f_i) = \delta$ non può che essere $\sum_{i=1}^{s} c_i d_i = 0$, ovvero il termine direttore si cancella. Calcoliamo ora gli S-polinomi, definendo i polinomi monici $p_i = \frac{f_i}{d_i}$. Per ipotesi $LCM(LM(f_j), LM(f_k)) = x^\delta$, quindi

$$S(f_j, f_k) = \frac{x^\delta}{LT(f_j)}f_j - \frac{x^\delta}{LT(f_k)}f_k = \frac{x^\delta}{d_j x^\delta}f_j - \frac{x^\delta}{d_k x^\delta}f_k = p_j - p_k \tag{9}$$

ogni p_i ha multigrado pari a δ e coefficiente direttore 1, dunque le differenze $p_j - p_k$ hanno multigrado strettamente minore di δ e dall'equazione precedente questo vale anche per gli S-polinomi. Riscriviamo ora la somma in termini dei p_i

$$\sum_{i=1}^{s} c_i f_i = c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + \cdots + (c_1 d_1 + \cdots + c_{s-1} d_{s-1})(p_{s-1} - p_s) + (c_1 d_1 + \cdots + c_s d_s) p_s. \quad (10)$$

Usando (9) e $\sum_{i=1}^{s} c_i d_i = 0$ otteniamo la combinazione lineare voluta

$$\sum_{i=1}^{s} c_i f_i = c_1 d_1 S(f_1, f_2) + (c_1 d_1 + c_2 d_2) S(f_2, f_3) + \cdots + (c_1 d_1 + \cdots + c_{s-1} d_{s-1}) S(f_{s-1}, f_s). \quad (11)$$

□

Il prossimo teorema è la base su cui si fonda l'algoritmo per calcolare delle basi di Gröbner, ideato da Bruno Buchberger [5].

Teorema 3.2 (criterio di Buchberger)**.** *Sia $I \in K[x_1, \ldots, x_n]$ un ideale non vuoto. Una base $G = g_1, \ldots, g_s$ per I è una G-base per I se e solo se per ogni coppia i, j con $i \neq j$, la divisione di $S(g_i, g_j)$ per G (in un qualche ordine) dà resto nullo.*

Dimostrazione. Se G è una base di Gröbner, allora il resto della divisione di $S(g_i, g_j) \in I$ per G è nullo per il Corollario 2.4.
Viceversa, supponiamo che $f \in I$ sia un polinomio non nullo. Dobbiamo mostrare che $LT(f) \in (LT(g_1), \ldots, LT(g_s))$. Dal momento che G è una base per I, esistono $h_1, \ldots, h_s \in K[x_1, \ldots, x_n]$ tali che

$$f = \sum_{i=1}^{s} h_i g_i. \quad (12)$$

Definiamo $m(i) = \text{multideg}(h_i g_i)$ e $m = \max\{m(i) : i = 1 \ldots s\}$. Allora si ha $\text{multideg}(f) \leq m$. Se vale l'uguaglianza allora $LT(f) \in (LT(g_1), \ldots, LT(g_s))$, mentre se vale il minore stretto allora è avvenuta qualche cancellazione tra i LT di $g_1, \ldots, g_s$. Osserviamo ora che la scrittura di (12) non è unica, ovvero possiamo prendere altri polinomi $h'_1, \ldots, h'_s$ ed ottenere comunque f, variando solo il multigrado m. Tuttavia un ordine monomiale è un buon ordinamento, quindi esisterà un m minimale. Vediamo che con questo m vale l'uguaglianza $\text{multideg}(f) = m$ tramite una dimostrazione per assurdo. Riscriviamo f nel modo seguente

$$f = \sum_{m(i)=m} h_i g_i + \sum_{m(i)\leq m} h_i g_i = \sum_{m(i)=m} LT(h_i) g_i + \sum_{m(i)=m} (h_i - LT(h_i)) g_i \sum_{m(i)\leq m} h_i g_i. \quad (13)$$

Assumendo per assurdo che multideg$(f) < m$, la prima somma deve avere anch'essa multigrado $< m$, dal momento che i monomi nella seconda e terza ce l'hanno per costruzione. Possiamo ulteriormente riscrivere f ponendo $LT(h_i) = c_i x^{\alpha_i}$, per cui

$$f = \sum_{m(i)=m} c_i x^{\alpha_i} g_i + \sum_{m(i)=m} (h_i - c_i x^{\alpha_i}) g_i \sum_{m(i)\leq m} h_i g_i. \tag{14}$$

Ora, la prima somma è una combinazione lineare degli S-polinomi $S(x^{\alpha_j} g_j, x^{\alpha_k} g_k)$ per il Lemma 3.1. Vediamo come sono fatti: per costruzione, ogni termine $x^{\alpha_i} g_i$ ha lo stesso multigrado m, dunque

$$S(x^{\alpha_j} g_j, x^{\alpha_k} g_k) = \frac{x^m}{x^{\alpha_j} LT(g_j)} x^{\alpha_j} g_j - \frac{x^m}{x^{\alpha_k} LT(g_k)} x^{\alpha_k} g_k = x^{m-\gamma_{jk}} S(g_j, g_k) \tag{15}$$

dove $\gamma_{jk} = LCM(LM(g_j), LM(g_k))$. Ne segue che esistono $c_{jk} \in K$ tali che

$$\sum_{m(i)=m} LT(h_i) g_i = \sum_{j,k} c_{jk} x^{m-\gamma_{jk}} S(g_j, g_k). \tag{16}$$

Dall'Algoritmo 2 e dall'ipotesi che gli S-polinomi abbiano resti nulli modulo G sappiamo che esistono $a_{ijk} \in K[x_1, \ldots, x_n]$ tali che

$$S(g_j, g_k) = \textstyle\sum_{i=1}^{s} a_{ijk} g_i \text{ e}$$

$$\text{multideg}(a_{ijk} g_i) \leq \text{multideg}(S(g_j, g_k)) \text{ per ogni } i, j, k$$

ovvero, quando il resto è nullo possiamo scrivere $S(g_j, g_k)$ come una combinazione lineare di G dove non tutti i termini direttori si cancellano. Moltiplicando da entrambe le parti per $x^{m-\gamma_{jk}}$ abbiamo la disuguaglianza

$$\text{multideg}(x^{m-\gamma_{jk}} a_{ijk} g_i) \leq \text{multideg}(x^{m-\gamma_{jk}} S(g_j, g_k)) < m. \tag{17}$$

Ora sostituendo $x^{m-\gamma_{jk}} S(g_j, g_k)$ in (16) e ponendo $b_{ijk} = x^{m-\gamma_{jk}} a_{ijk}$ otteniamo

$$\sum_{m(i)=m} LT(h_i) g_i = \sum_{j,k} c_{jk} x^{m-\gamma_{jk}} S(g_j, g_k) =$$

$$= \sum_{j,k} c_{jk} \left(\sum_i b_{ijk} g_i \right) = \sum_i d_i g_i \tag{18}$$

con multideg$(d_i g_i) < m$ per ogni i. Sostituendo ancora in (14) otteniamo una espressione per f come combinazione lineare di G dove ogni monomio ha multigrado minore di m, il che contraddice la minimalità di m. □

Una volta scelto un ordine monomiale si può procedere con la seguente versione elementare dell'algoritmo di Buchberger.

Algoritmo 3

Input: $I = (f_1, \ldots, f_s)$
Output: una base di Gröbner $GB = (g_1, \ldots, g_t)$ per I

```
1: GB := F
2: repeat
3:    G := GB
4:    for (p, q) coppia in G con p ≠ q do
5:       R:= resto della divisione di S(p, q) per G
6:       if S ≠ 0 then
7:          G := G ∪ {S}
8:       end if
9:    end for
10: until GB = G
```

Esempio 3.3. Calcoliamo una base di Gröbner per l'ideale $I = (f_1, f_2)$, con $f_1 = x^2y - 1$, $f_2 = xy^2 - x$, usando l'Algoritmo 3 e l'ordine lessicografico.
Impostiamo $G := GB := \{f_1, f_2\}$ e calcoliamo il primo S-polinomio:

$$S(f_1, f_2) = \tfrac{x^2y^2}{x^2y}(x^2y - 1) - \tfrac{x^2y^2}{xy^2}(xy^2 - x) = x^2 - y$$

che non è divisibile per G ed è non nullo, dunque aggiungiamo $R := f_3 := x^2 - y$ a G. Risulta quindi $G \neq GB$, perciò proseguiamo.

$S(f_1, f_3) = y^2 - 1$, non divisibile per $G \to R := y^2 - 1 \to$ aggiungiamo $f_4 := y^2 - 1$ a G

$S(f_2, f_3) = y^3 - 1$, che, diviso per G dà $R := y - 1 \to$ aggiungiamo a G il nuovo polinomio $f_5 := y - 1$

$S(f_1, f_4) = x^2 - y = f_3 \to R := 0$ e non aggiungiamo termini a G

$S(f_2, f_4) = 0 \to R := 0$, andiamo avanti

$S(f_3, f_4) = x^2 - y^3 \to R := 0$.

Tutti i restanti S-polinomi danno resto nullo, per cui otteniamo $G = GB$ e abbiamo terminato. Una base di Gröbner per I è

$$\{g_1, g_2, g_3, g_4, g_5\} = \{x^2y - 1, xy^2 - x, x^2 - y, y^2 - 1, y - 1\}.$$

Da questo solo esempio possiamo notare che l'Algoritmo 3 non è molto veloce: anche partendo da due polinomi in due variabili il ciclo principale può durare a lungo, perché ogni volta che viene aggiunto un nuovo termine è necessario considerare tutte le nuove coppie di polinomi. Notare che nell'Esempio abbiamo evitato di ricalcolare gli S-polinomi già esaminati, sebbene, così come è scritto, l'algoritmo prenda in considerazione ogni volta *tutte* le coppie in G. Nella prossima sezione vedremo una versione più avanzata dell'Algoritmo.

3.1 Ottimizzazioni dell'algoritmo di Buchberger

Le seguenti osservazioni sono tratte da [6].

1. La scelta dell'ordine monomiale influenza i tempi di calcolo: si è visto che `DEGREVLEX` produce i risultati migliori.

2. Scegliendo ad ogni ciclo coppie di polinomi (f, g) in I tali che il minimo comune multiplo dei rispettivi termini direttori sia il più piccolo possibile, $S(f, g)$ tenderà a fornire prima un resto non nullo durante il processo.

3. L'operazione più costosa è la divisione degli S-polinomi, ma fortunatamente è possibile ridurre il numero di tali divisioni:

   - se ad un certo punto troviamo un resto nullo, ovvero $S = 0$ al punto 5 nell'Algoritmo 3, questo rimarrà nullo anche aggiungendo altri elementi all'insieme generatore G, dunque non è necessario ricalcolarlo. Più precisamente, dal momento che i nuovi generatori vengono aggiunti uno per volta, sarà sufficiente calcolare i resti della divisione di $S(f_i, f_j)$ per G con $i \leq j - 1$;
   - quando $GCD(LT(f), LT(g)) = 1$, ovvero quando f e g hanno termini direttori senza variabili comuni, $S(f, g)$ dà resto nullo se diviso per $\{f, g\} \in G$, dunque non è necessario calcolarlo;
   - infine, se in G esistono p, f, g tali che $lt(p)$ divide $LCM(LT(f), LT(g))$ e i resti di $S(f, p)$, $S(g, p)$ sono già stati calcolati, possiamo trascurare la coppia (f, g).

Il seguente algoritmo tiene conto di quanto detto.

Algoritmo 4

Input: $I = (f_1, \ldots, f_s)$
Output: una base di Gröbner $G = (g_1, \ldots, g_t)$ per I

1: $GB := I$
2: $B := \{(i, j) : 1 \leq i < j \leq s \text{ e } GCD(LT(f_i), LT(f_j)) \neq 1\}$
3: $t := s$
4: **while** $B \neq \emptyset$ **do**
5: $(i, j) := (i, j) \in B$ con minimo $LCM(LT(f_i), LT(f_j))$
6: $B := B \setminus \{(i, j)\}$
7: **if** non esiste alcun $p \in GB$ tale che $(f_i, p) \notin B$, $(f_j, p) \notin B$ e $LT(p)$ divida $LCM(LT(f_i), LT(f_j))$ **then**
8: $S :=$ resto della divisione di $S(f, g)$ per GB
9: **if** $S \neq 0$ **then**
10: $t := t + 1$; $f_t := S$
11: $GB := GB \cup \{S\}$
12: $B := B \cup \{(i, t) : 1 \leq i \leq t - 1\}$
13: **end if**
14: **end if**
15: **end while**
16: **return** GB

Riferimenti bibliografici

[1] B. Buchberger. An algorithm for finding the basis elements of the residue classes ring of a zero dimensional polynomial ideal. University of Innsbruck, 1965.

[2] D. Cox, J. Little, D. O'Shea. Ideals, Varieties, and Algorithms, cap. 1 e 2. Springer-Verlag 2007.

[3] P.M. Cohn, Basic Algebra: Groups, Rings and Fields. Springer 2015.

[4] M. Reid. Undergraduate Commutative Algebra. Cambridge University Press 1995.

[5] B. Buchberger. Gröbner-Bases: An Algorithmic Method in Polynomial Ideal Theory, in Multidimensional Systems Theory - Progress, Directions and Open Problems in Multidimensional Systems. Reidel Publishing Company 1985.

[6] A. Heck. Introduction to Maple, pp. 697-746. Springer-Verlag 1993.