Decomposizione primaria in $k[x_1, \ldots, x_n]$
P.Gianni

Ideali 0-dimensionali

Indichiamo con $A = k[x_1, \ldots, x_n] = k[\mathbf{x}]$ l'anello dei polinomi in n variabili su un campo k di caratteristica 0 e con $I \subset A$ un ideale. Se $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, $\mathbf{x}^\alpha = x_1^{\alpha_1} .. x_n^{\alpha_n}$ è il monomio di A con esponente α.
Ricordiamo che I si dice $0-$*dimensionale* se vale una delle seguenti affermazioni equivalenti:

1. L'anello A/I ha dimensione di Krull 0, ossia ogni ideale primo di A/I è massimale.
2. A/I é intero su k.
3. per ogni x_i esiste un polinomio (monico) $f_i(t) \in k[t]$ tale che $f_i(x_i) \equiv 0 \pmod I$.
4. Se G è una base di Gröbner di I rispetto ad un ordinamento monomiale allora per ogni x_i esiste $m_i > 0$ e $g_i \in G$ tale che $lt(g_i) = x_i^{m_i}$.
5. A/I è un k-spazio vettoriale di dimensione finita $d = \#\{\mathbf{x}^\alpha \mid \mathbf{x}^\alpha \notin \mathrm{Lt(G)}\}$.
6. Se indichiamo con $\bar{k}$ la chiusura algebrica di k e con $\bar{I} = I\bar{k}[x_1, \ldots, x_n]$ allora $\bar{I}$ è zero dimensionale e $\dim_{\bar{k}} \bar{k}[x_1, \ldots, x_n]/\bar{I} = \dim_k k[x_1, \ldots, x_n]/I$.

Proposizione 1. Sia $I \subset A$ un ideale primo 0-dimensionale e $G = \{g_1, \ldots, g_s\}$ sia la sua base di Gröbner ridotta rispetto all'ordinamento lex con $x_1 > \cdots > x_n$ allora:

- $s = n$,
- $g_n \in k[x_n]$ è irriducibile,
- $g_i(x_i, \ldots, x_n)$ è irriducibile sul campo $k[x_{i+1}, \ldots, x_n]/(I \cap k[x_{i+1}, \ldots, x_n])$ per ogni $1 \leq i \leq n-1$

Osservazione Se $k = \overline{k}$ la precedente proposizione garantisce che se un ideale I è primo 0-dimensionale (ossia massimale) allora $I = (x_1 - a_1, \ldots, x_n - a_n)$, con $a_i \in k$.

Proposizione 2. Sia $I \subset A$ un ideale primario 0-dimensionale.
Se $G = \{G_1, \ldots, G_n\}$, $0 \neq G_i \subset k[x_i, \ldots, x_n]$ è la base di Gröbner ridotta di I rispetto all'ordinamento lex con $x_1 > \cdots > x_n$ allora:

- $G_n = p_n^{s_n}(x_n)$, è potenza di un polinomio irriducibile

- Se $G_i = \{g_1^{(i)}(x_i, \ldots, x_n), \ldots, g_{s_i}^{(i)}(x_i, \ldots, x_n\}$ allora
  - $g_1^{(i)} \equiv {p_i}^{s_i} \pmod{\sqrt{I \cap k[(x_{i+1}, \ldots, x_n]}}$ e p_i è irriducibile,
  - $g_j^{(i)} \equiv 0 \pmod{\sqrt{I \cap k[(x_{i+1}, \ldots, x_n]}}$ per ogni $2 \leq j \leq s_j$

Proposizione 3. Sia $I \subset A$ un ideale 0-dimensionale e siano $f_i(x_i) \in k[x_i]$ i polinomi monici univariati di grado minimo tali che $f_i \in I \cap k[x_1]$. Se indichiamo con $\bar{f}_i = f_i/(f_i, f_i')$ le parti libere da quadrati dei polinomi f_i allora si ha

$$\sqrt{I} = (I, \bar{f}_1, \ldots, \bar{f}_n)$$

Lemma Sia $Q \in A$ un ideale radicale 0 dimensionale allora ogni ideale $J \subsetneq A$ tale che $Q \subset J$ è radicale.

Lemma . Sia $I \subset A$ un ideale primo 0-dimensionale, allora $\bar{I} = I\bar{k}[x_1, \ldots, x_n]$ è un ideale radicale.

Lemma Siano $P_1, \ldots, P_s \in \bar{k}^n$, allora esistono infiniti $\mathbf{c} = (c_1, \ldots, c_n) \in k^n$ tali che dopo il cambiamento lineare di coordinate dato da $\varphi_{\mathbf{c}}(x_i) = x_i$ per $i < n$ e $\varphi_{\mathbf{c}}(x_n) = \sum c_i x_i$ se $\varphi_{\mathbf{c}}(P_i) = (\gamma_1^{(i)}, \ldots, \gamma_n^{(i)})$, si abbia $\gamma_n^{(i)} \neq \gamma_n^{(j)}$ se $i \neq j$.

Proposizione. Sia $I \subset A$ un ideale primo 0-dimensionale. A meno di un cambiamento lineare di coordinate (come nel lemma) la base di Gröbner ridotta di I, G, rispetto all'ordinamento lessicografico con $x_1 > \ldots > x_n$ è $G = (x_1 - p_1(x_n), \ldots, x_{n-1} - p_{n-1}(x_n), p_n(x_n))$ con p_n irriducibile di grado $d = \dim_k k[x_1, \ldots, x_n]/I$.
Dim. I è primo e zero dimensionale, quindi $\bar{I} = I\bar{k}[x_1, \ldots, x_n]$ è zero dimensionale, radicale, $\#V_{\bar{k}}(\bar{I}) = \{P_1, \ldots, P_d\}$ è finito e $d = \dim_{\bar{k}} \bar{k}[x_1, \ldots, x_n]/\bar{I} = \dim_k A/I$. A meno di un cambiamento lineare di coordinate, possiamo supporre che i punti $P_i = (\gamma_1^{(i)}, \ldots, \gamma_n^{(i)})$ abbiano ultima coordinate distinte. Se consideriamo il polinomio $f = \Pi_i(x_n - \gamma_n^{(i)})$ allora $f \in \sqrt{\bar{I}} = \bar{I}$. Dato che $I \subset \bar{I}$ si ha che $p_n = I \cap k[x_n] \in \bar{I}$ e f divide p_n, da cui segue che $\deg(p_n) \geq \deg f = d = \dim_k A/I \geq \deg p_n$. Quindi gli elementi $1, x_n, \ldots, x_n^{d-1}$ sono una base di A/I, e per ogni i, $x_i \equiv p_i(x_n) \pmod{I}$ e quindi necessariamente $x_i - p_i(x_n) \in G$.

Definizione. Sia $I \subset A$ un ideale 0-dimensionale in A allora I si dice in **posizione generale** se:

- se I è primo e G è la sua base di Gröbner ridotta, rispetto all'ordinamento lessicografico con $x_1 > \ldots > x_n$ allora

  $$G = (x_1 - p_1(x_n), \ldots, x_{n-1} - p_{n-1}(x_n), p_n(x_n))$$

  con p_n irriducibile di grado $d = \dim_k k[x_1, \ldots, x_n]/I$

- se $I = \cap Q_i$ è una decomposizione primaria minimale di I allora per ogni i gli ideali primi $P_i = \sqrt{Q_i}$ sono in posizione generale e se $P_i \cap k[x_n] = (q_i)$ si ha $(q_i, q_j) = 1$ quando $i \neq j$.

Proposizione 4. Sia $I \subset A$ un ideale primario zero dimensionale e sia $G = \{G_1, \ldots, G_n\}$, $0 \neq G_i \subset k[x_i, \ldots, x_n]$ la sua base di Gröbner ridotta rispetto all'ordinamento lex con $x_1 > \cdots > x_n$ allora sono fatti equivalenti:

- I è in posizione generale
- esistono polinomi $p_1(x_n), \ldots, p_n(x_n) \in k[x_n]$ e $s_1, \ldots s_n \in \mathbb{N}$ tali che :
  - $G_n = p_n^{s_n}(x_n)$, è potenza di un polinomio irriducibile
  - per ogni $i < n$ se $G_i = \{g_1^{(i)}(x_i, \ldots, x_n), \ldots, g_{s_i}^{(i)}(x_i, \ldots, x_n\}$ allora

$$g_1^{(i)} \equiv (x_i - p_i(x_n))^{k_i} \pmod{(x_{i+1} - p_{i+1}, x_{i+2} - p_{i+2}, \ldots, p_n)}$$

Il risultato precedente ci permette di definire la seguente procedura.

Test-Primario-0

Input: $I = (f_1, \ldots, f_k) \subset A$ ideale 0-dimensionale.
Output: (0) se I non è primario o non in posizione generale. $\sqrt{I}$ se I è primario in posizione generale.

1. G:= Gröbner(I)
2. $g := G \cap k[x_n]$
3. **if** $g = g_n^m$ con g_n irriducibile **then**

   radicale := (g)

   else return (0)
4. $i := n$
5. while $i > 1$ **repeat**

   $i := i - 1$

   scegli $h \in G$ tale che $\mathrm{lt}(h) = x_i^m$

   $b :=$ coefficient$_{x_i}(h, m-1)$

   $q := x_i + b/m$

   if $q^m \equiv h \pmod{\text{radicale}}$ **then** radicale:= (q)+radicale

else return (0)

6. return radical

Osservazione. Se $I \subset A$ è radicale 0-dimensionale in posizione generale allora la su abase lex ridotta è $(x_1 - p_1(x_n), \ldots, p_n(x_n))$, on $p_n(x_n)$ libero da quadrati.

Teorema. Sia $I \subset A$ un ideale 0-dimensionale in posizione generale e sia G la sua base di Gröbner ridotta, rispetto all'ordinamento lessicografico con $x_1 > \ldots > x_n$. Se $(g) = (G) \cap k[x_n] (= I \cap k[x_n])$ e consideriamo la fattorizzazione in fattori irriducibili di $g = \Pi_{i=1}^{s} g_i^{k_i}$, allora $I = \cap_{i=1}^{s} (I, g_i^{k_i})$ è una decomposizione primaria di I.
Dim. Dato che $(g_i, g_j) = 1$, quando $i \neq j$, il teorema cinese del resto garantisce che $I = \cap_i (I, g_i^{k_i})$. Proviamo ora che questa decomposizione è una decomposizione primaria minimale di I. Osserviamo innanzitutto che per ogni i si ha che $(I, g_i^{k_i}) \subsetneq A$: se $1 = f + a g_i^{k_i}$ con $f \in I$ allora $\dfrac{g}{\Pi_{i \neq j} g_j^{k_j}} \in (f, g) \subset I$ e questo contraddice il fatto che la base di Gröbner è ridotta. È anche immediato vedere che $\mathrm{Ass}((I, g_i^{k_i})) \subset \mathrm{Ass}(I)$. Infatti se $I = \cap_{i=1}^{r} Q_i$ è una decomposizione primaria minimale di I e $P_i = \sqrt{Q_i} \in \mathrm{Ass}(I)$, dato che $\sqrt{I} = \cap P_i \subset \sqrt{(I, g_i^{k_i})} = \tilde{P}_1 \cap \ldots \cap \tilde{P}_t \subset \tilde{P}_j$ allora esiste i tale che $P_i \subset \tilde{P}_j$ e dal momento che P_i è massimale si deve avere $P_i = \tilde{P}_j$. Se consideriamo poi $P_i \cap k[x_n] = (q_i)$ dato che l'ideale è in posizione generale si ha che $(q_i, q_j) = 1$ se $i \neq j$ e quindi $\sqrt{I} \cap k[x_n] = (\cap_i P_i) \cap k[x_n] = \cap_i (P_i \cap k[x_n]) = \cap_i (q_i) = (\Pi_i q_i)$. Per ipotesi $g = I \cap k[x_n] \subset \sqrt{I} \cap k[x_n]$ e quindi si deve avere che $\Pi_i (q_i) | g$ e che esiste m tale che $g | (\Pi_i q_i)^m$, da cui segue che $r = t$ e che (eventualmente riordinando gli indici) $q_i = g_i$. Da questo segue che P_i è l'unico primo associato di I che contiene g_i, ossia che $\mathrm{Ass}((I, g_i^{k_i})) = P_i$ e quindi, dal momento che P_i è massimale, che l'ideale $(I, g_i^{k_i})$ è primario.

Dal momento che per la Proposizione 4 sappiamo controllare se un ideale primario è in posizione generale, Il teorema precedente ci fornisce un algoritmo per calcolare la decomposizione primaria di un ideale 0-dimensionale.

Decomposizione-Primaria-0

Input: $I = (f_1, \ldots, f_k) \subset A$ ideale 0-dimensionale.
Output: Una lista $[(Q_i, P_i)]$ di coppie di ideali tali che $I = \cap Q_i$ è una decomposizione primaria di I e $P_i = \sqrt{Q_i}$.

1. decomp := []
2. Scegliamo $\mathbf{c} \in k^{n-1}$ random e sia $\varphi_{\mathbf{c}}$ il cambiamento lineare di coordinate dato da $\varphi_{\mathbf{c}}(x_i) = x_i$ per $i < n$ e $\varphi_{\mathbf{c}}(x_n) = x_n + \sum c_i x_i$.

3. $I' := \varphi_{\mathbf{c}}(I)$
4. G:= Gröbner(I') (ordinamento lex, $x_1 > \ldots > x_n$
5. $g = G \cap k[x_n]$
6. $g := \Pi_{i=1}^{s} g_i^{k_i}$ (fattorizzazione in irriducibili)
6. **for** i in $1 \ldots s$ **repeat**

   $Q_i' := (I', g_i^{k_i})$

   $P_i' :=$ **Test-Primario-0**(Q_i')

   if $P_i' = 0$ **then**

      decomp := cons(**Decomposizione-Primaria-0**(Q_i),decomp)

   else

      decomp := cons($(\varphi_{\mathbf{c}}^{-1}(Q_i'), \varphi_{\mathbf{c}}^{-1}(P_i'))$,decomp)
7. return decomp

Decomposizione Primaria
Analizziamo ora il caso di ideali di dimensione positiva. Sia $A = k[x_1, \ldots, x_n]$ e $I \subset A$ tale che $\dim I = \dim A/I > 0$. Cerchiamo una decomposizione di I in modo da ricondurci al caso 0-dimensionale, che abbiamo già risolto. Fissiamo su A l'ordinamento monomiale lessicografico con $x_1 > \ldots > x_n$.
Vale la seguente:

Proposizione. Se $r \in A$ è tale che $(I : r) = (I : r^2)$ allora $I = (I, r) \cap (I : r)$

Dal momento che A è noetheriano per ogni $r \in A$ la catena $(I : r) \subset (I : r^2) \subset ...$ si stabilizza, allora se indichiamo con r^* la potenza tale che $(I : r^k) = (I : r^{k+1})$ otteniamo che $IA_r \cap A = \cup_{k \in \mathbb{N}}(I : r^k) = (I : r^*)$.

Se $\dim I > 0$ allora esiste almeno una variabile x_i tale che $I \cap k[x_i] = (0)$. Se consideriamo l'insieme moltiplicativo $T_i = k[x_i] \setminus (0)$, abbiamo che l'anello $T_i^{-1}A = k(x_i)[\mathbf{x} \setminus \{x_i\}]$, ha dimensione $n - 1$ e $T_i^{-1}I \subsetneq T_i^{-1}A$. Per sfruttare la decomposizione della proposizione precedente dimostriamo i seguenti fatti:

Proposizione 5. Sia $I \subset A$, $\dim I > 0$, x_i la variabile più piccola (rispetto a $>$) per cui $I \cap k[x_i] = (0)$ e sia $T_i = k[x_i] \setminus (0)$. Se $G = \{g_1, \ldots, g_s\} \subset A$ è la base di Gröbner ridotta di I, allora si ha:

1. $T_i^{-1}G$ è una base di Gröbner di $T_i^{-1}I$.

2. Se esprimiamo $g_i \in k[x_i][\mathbf{x} \setminus \{x_i\}]$ e $r = \Pi_i \mathrm{lc}_{x_i} g_i$ allora

$$(I : r^*) = Ik(x_i)[\mathbf{x} \setminus \{x_i\}] \cap A$$

.

Dim. 1. Gli elementi $\frac{g_1}{1}, \ldots, \frac{g_s}{1}$ generano $T_i^{-1} I$.
Se $\frac{f}{q(x_i)} \in T_i^{-1} I$ allora si ha $\frac{f}{q(x_i)} = \sum_j \frac{b_j}{p_j(x_i)} \frac{g_i}{1}$. Eliminando i denominatori otteniamo $p(x_i) f = \sum_i a_i g_i$ da cui $x_i^m \mathrm{lt} f \in \mathrm{Lt}(G)$ e quindi $T_i^{-1}\mathrm{Lt}(G) = T_i^{-1}(\mathrm{LT}(I)) = \mathrm{Lt}(T_i^{-1} I)$.

2. Certamente $(I : r^*) \subset Ik(x_i)[\mathbf{x} \setminus \{x_i\}] \cap A = \cup_{t \in T_i} (I : t)$. Viceversa se $f \in Ik(x_i)[\mathbf{x} \setminus \{x_i\}] \cap A$, $\frac{f}{1} \in T_i^{-1} I$ e quindi riduce a 0 con $\frac{g_1}{1}, \ldots, \frac{g_s}{1}$. Dal momento che le riduzioni coinvolgono solo divisioni per i leading coefficients si ha $\frac{f}{1} = \sum_i \frac{b_i}{r^{k_i}} \frac{g_i}{1}$ da cui segue che esiste m tale che $r^m f \in I$ ossia $f \in (I : r^*)$.

L'elemento $s = r^* \in k[x_i]$ costruito nella proposizione precedente soddisfa allora le seguenti proprietà:

- $I = (I, s) \cap (I : s)$,
- (I, s) contiene una relazione univariata per x_i,
- $(I : s)$ è la contrazione dell'ideale $Ik(x_i)[\mathbf{x} \setminus \{x_i\}]$ che ha dimensione minore di I.

Iterando questa costruzione è cosí possibile ricondursi al caso di ideali di dimensione 0.

Decomposizione-Primaria

Input: $I = (f_1, \ldots, f_k)$ ideale in $k[var]$, $var \subseteq \{x_1, \ldots, x_n\}$
Output: Una $[Q_i]$ di ideali tali che $I = \cap Q_i$ è una decomposizione primaria (non necessariamente minimale) di I.

1. decomp := []
2. G := Gröbner(I)
3. $i := n$
4. **while** $G \cap k[x_i] \neq (0)$ and $i \geq 1$ **repeat** $i := i - 1$
5. **if** $i = 0$ **then return** [Q_i for Q_i in **Decomposizione-Primaria-0**(I)]

6. $r := \Pi_i \mathrm{lc}_{x_i} g_i$
7. $s := r$
8. $J := (I : s)$
9. **while** $J \neq (I : (s * r))$ **repeat** $s := r * s$
   – decomposizione in $k(x_i)[var \setminus \{x_i\}]$
10. $(\tilde{Q}_1, \ldots, \tilde{Q}_k)$:=**Decomposizione-Primaria**$(I, [\mathbf{x} \setminus \{\mathbf{x_i}\}])$
11. decomp:= $(\tilde{Q}_1^c, \ldots, \tilde{Q}_k^c) \cup$decomp (*)
12. $(\hat{Q}_1, \ldots, \hat{Q}_l)$:=**Decomposizione-Primaria**((I,s),var)
7. return $(\hat{Q}_1, \ldots, \hat{Q}_l) \cup$ decomp

(*) Per calcolare $\tilde{Q}_i^c$ si puo' calcolare $(\tilde{Q}_i : s)$.
Per concludere osserviamo che la stessa strategia può essere applicata per calcolare il radicale di un ideale dal momento che, usando s come in Proposizione 5 si ha:

$$\sqrt{I} = \sqrt{(I, s)} \cap \sqrt{I : s)} = \sqrt{I^{ec}} = (\sqrt{I^e})^c$$

e il radicale di un ideale 0-dimensionale può essere calcolato usando la Proposizione 3.