UNIVERSITÀ DEGLI STUDI DI TRENTO

Dipartimento di Matematica

Corso di Laurea in Matematica

Elaborato finale

Algoritmo di Sylvester

Supervisore
Prof. Alessandra Berardi

Laureando
Nicolò Insalaco

Anno accademico 2016/2017

Indice

Introduzione

Questo elaborato ha come obiettivo presentare l'algoritmo di Sylverster, il cui scopo è quello di decomporre un dato polinomio omogeneo, assumendo sia di grado d, nella somma di d-esime potenze di forme lineari. Nel primo capitolo si elencano definizioni fondamentali per comprendere i risultati ottenuti nelle sezioni successive. Si presenta quindi nel secondo capitolo la mappa di Veronese, funzione attorno alla quale si costruisce l'algoritmo. Segue il capitolo terzo in cui si dimostrano risultati riguardo alla decomposizione di polinomi in somme di forme lineari e alla definizione di condizioni per cui essa è unica. Nel quarto e ultimo capitolo si elencano i passi dell'algoritmo di Sylvester dalla versione pubblicata nel 2001 dai professori G. Comas e M. Seiguer ([3]). Concludono l'elaborato due esempi operativi, nel primo caso si soddisfano le condizioni per cui la decomposizione è unica mentre nel secondo si producono due decomposizioni distinte per lo stesso polinomio.

Capitolo 1

Nozioni Preliminari

Lo scopo di questo capitolo è quello di introdurre alcune definizioni di algebra necessarie alla comprensione della tesi.

Definizione 1.1. Sia $\mathbb{K}$ un campo. Lo **spazio proiettivo** di dimensione $n-1$ sul campo $\mathbb{K}$, denotato con $\mathbb{P}(\mathbb{K}^n)$ (o anche $\mathbb{P}^{n-1}$), è il quoziente di $\mathbb{K}^n \setminus \{0\}$ rispetto alla relazione di equivalenza $\sim$ definita come segue:

$$\text{siano } P, R \in \mathbb{K}^n \text{ allora } P \sim R \iff \exists \lambda \in \mathbb{K} \setminus \{0\} \text{ tale che } \lambda P = R. \quad (1.1)$$

Il fatto che la relazione $\sim$ sia di equivalenza si dimostra banalmente grazie alle proprietà di campo di $\mathbb{K}$.

Nelle prossime definizioni si assumerà sempre $\mathbb{K} = \mathbb{C}$, il campo dei numeri complessi.

Definizione 1.2. Sia $f \in \mathbb{C}[z_0, \ldots, z_{n-1}]$ un polinomio a n variabili e coefficienti complessi. Si dice che f è un polinomio omogeneo di grado d se tutti i monomi che lo compongono sono di grado d o, equivalentemente, se:

$$f(\lambda z_0, \ldots, \lambda z_{n-1}) = \lambda^d f(z_0, \ldots, z_{n-1}) \ \forall \lambda \in \mathbb{C}. \quad (1.2)$$

Definizione 1.3. $X \subseteq \mathbb{P}(\mathbb{C}^n)$ si dice **insieme algebrico proiettivo** se X è luogo di zeri di un insieme di polinomi omogenei $S \subseteq \mathbb{C}[z_0, \ldots, z_{n-1}]$.

Alternativamente, sia $I \subseteq \mathbb{C}[z_0, \ldots, z_{n-1}]$ allora essendo $\mathbb{C}[z_0, \ldots, z_{n-1}]$ un anello noetheriano, poiché è un campo, per il teorema della base di Hilbert I è finitamente generato, dunque $\exists f_1, \ldots, f_m \in \mathbb{C}[z_0, \ldots, z_{n-1}]$,
polinomi omogenei, tali che I è generato da essi, in simboli $I = \langle \{f_1, \ldots, f_m\} \rangle$ (che per semplicità si scriverà come $\langle f_1, \ldots, f_m \rangle$).
Si definisce dunque l'insieme:

$$V(I) = \{z \in \mathbb{P}(\mathbb{C}^n) \mid f_i(z) = 0 \text{ per ogni } i = 1, \ldots, m\}. \tag{1.3}$$

Si può quindi riscrivere la Definizione 1.3 nel seguente modo:
$X \subseteq \mathbb{P}(\mathbb{C}^n)$ si dice **insieme algebrico proiettivo** se esiste un insieme di polinomi omogenei $S \subseteq \mathbb{C}[z_0, \ldots, z_{n-1}]$ tale che $X = V(\langle S \rangle)$ dove $\langle S \rangle$ è l'ideale generato da S.

Definizione1.4. Se $I \subseteq \mathbb{C}[z_0, \ldots, z_{n-1}]$ è un ideale primo allora $X = V(I)$ si dice **insieme algebrico proiettivo irriducibile** o **varietà proiettiva**.

Si userà più avanti, considerato un insieme $X \subseteq \mathbb{P}(\mathbb{C}^n)$, anche l'insieme:

$$I(X) := \{f \in \mathbb{C}[z_0, \ldots, z_{n-1}] \mid f(P) = 0 \text{ per ogni } P \in X\}.$$

Questo insieme definisce un ideale in $\mathbb{C}[z_0, \ldots, z_{n-1}]$, infatti considerando X come sopra, $f \in I(X) = J$ e $g \in \mathbb{C}[z_0, \ldots, z_{n-1}]$ è evidente $fg(P) = 0$ allora $fg \in J$.

Nella seguente definizione si useranno le varietà proiettive per costruire una topologia sullo spazio proiettivo.

Definizione 1.5. La **topologia di Zariski** su $\mathbb{P}(\mathbb{C}^n)$ è la topologia ottenuta scegliendo come chiusi gli insiemi algebrici proiettivi in $\mathbb{P}(\mathbb{C}^n)$.

Si dimostra facilmente che questa è effettivamente una topologia poiché valgono:

1. $V(x_0, \ldots, x_{n-1}) = \emptyset$ e $V(0) = \mathbb{P}(\mathbb{C}^n)$;
2. siano $I, J \subseteq \mathbb{C}[z_0, \ldots, z_{n-1}]$ due ideali, allora:
   $V(I) \cup V(J) = V(I \cap J) = V(IJ)$;
3. sia $\{I_i\}_i$ una famiglia numerabile di ideali in $\mathbb{C}[z_0, \ldots, z_{n-1}]$, allora:
   $\bigcap_i V(I_i) = V(\sum_i I_i)$.

Quando si parlerà nei capitoli successivi di chiusura rispetto alla topologia di Zariski di un insieme A, denotata con $\overline{A}$, si intenderà il più piccolo insieme proiettivo contenente A.

Osservazione 1.1. Riprendendo la definizione dell'insieme $I(X)$ dove X è un insieme in $\mathbb{P}(\mathbb{C}^n)$ vale:

$$V(I(X)) = \overline{X}.$$

Nel caso particolare in cui X sia un insieme algebrico proiettivo:

$$V(I(X)) = X.$$

Per semplicità di notazione nel capitolo successivo si indicherà lo spazio dei polinomi omogenei di grado d in n variabili brevemente come $S^d\mathbb{C}^n$.

Capitolo 2

Curva di Veronese

In questo capitolo è definita la mappa di Veronese, che risulta fondamentale per la costruzione dell'algoritmo di Sylvester e la dimostrazione della sua funzionalità.

Definizione 2.1. Si dice mappa di Veronese la mappa:

$$\begin{aligned} \upsilon_d : \mathbb{P}(\mathbb{C}^{n+1}) = \mathbb{P}^n &\longrightarrow \mathbb{P}(S^d\mathbb{C}^{n+1}) \\ \mathbb{P}(\mathbb{C}^{n+1}) \ni [v] = [a_0, \ldots, a_{n-1}] &\longrightarrow [a_0^d, \ldots, \binom{d}{i_0, \ldots, i_n} a_0^{i_0} \cdots a_n^{i_n}, \ldots, a_n^d] \end{aligned} \tag{2.1}$$

dove $\sum_{j=0}^{n} i_j = d$, una mappa tra lo spazio proiettivo complesso $\mathbb{P}^n$ e lo spazio dei polinomi omogenei complessi in n variabili di grado d, $\mathrm{S}^d\mathbb{C}^{n+1}$, che valuta la base dello spazio $\mathrm{S}^d\mathbb{C}^{n+1}$ in punto dello spazio proiettivo.

Definizione 2.2. La varietà ottenuta dall'immagine della mappa di Veronese come 2.1, $\upsilon_d(P^n)$, si dice Varietà di Veronese o curva razionale normale di grado d.

Nel caso particolare in cui n=2 si dirà semplicemente Curva di Veronese.

Ora si vedranno degli esempi introduttivi che allacceranno evidentemente queste definizioni con lo scopo della tesi.

Analizzando il caso più semplice in cui $d = 2$ la curva di Veronese risul-

ta:

$$\begin{aligned} \upsilon_2 : \mathbb{P}^1 &\longrightarrow \mathbb{P}^2 \ni [z_0, z_1, z_2] \\ [a_0, a_1] &\longrightarrow [a_0^2, 2a_0a_1, a_1^2]. \end{aligned} \tag{2.2}$$

Per verificare se un punto di $\mathbb{P}^2$ appartiene alla curva di Veronese è sufficiente verificare che annulli i minori $2 * 2$ della matrice, che solitamente si chiama cataletticante, $\begin{bmatrix} c_{11} & c_{12} \\ c_{12} & c_{22} \end{bmatrix}$ ove $c_{ij} = \binom{d}{i}^{-1} z_{i+j-2}$. In questo caso si trova banalmente che la matrice cataletticante è $\begin{bmatrix} z_0 & \frac{z_1}{2} \\ \frac{z_1}{2} & z_2 \end{bmatrix}$ e che l'unico minore $2 * 2$ è il determinante, da cui deve valere $z_0z_2 - \frac{z_1^2}{4} = 0$.
Mostrare che i punti della curva soddisfano questa proprietà è molto semplice in quanto sostituendo le coordinate dell'immagine di un punto nell'equazione si trova immediatamente:

$$a_0^2a_1^2 - (a_0a_1)^2 = 0. \tag{2.3}$$

Osservazione 2.1. Si può vedere in questo caso che, essendo $I(\upsilon_2(\mathbb{P}^1)) = (z_0z_2 - \frac{z_1^2}{4})$ che risulta essere un ideale primo, la varietà di Veronese è effettivamente una varietà (i calcoli sono stati fatti con Macaualy2).

Ora si mostra un secondo esempio in cui si impone d=3.

In questo caso si osserva che la mappa di Veronese è:

$$\begin{aligned} \upsilon_3 : \mathbb{P}^1 &\longrightarrow \mathbb{P}^3 \ni [z_0, z_1, z_2, z_3] \\ [a_0, a_1] &\longrightarrow [a_0^3, 3a_0^2a_1, 3a_0a_1^2, a_1^3]. \end{aligned} \tag{2.4}$$

Costruendo anche in questo caso la matrice cataletticante $\begin{bmatrix} c_{11} & c_{12} & c_{13} \\ c_{12} & c_{13} & c_{22} \end{bmatrix}$ dove c_{ij} è definito come nel caso precedente, si ottiene svolgendo i calcoli la matrice $\begin{bmatrix} z_0 & \frac{z_1}{3} & \frac{z_2}{3} \\ \frac{z_1}{3} & \frac{z_2}{3} & z_3 \end{bmatrix}$, i cui minori $2 * 2$ definiscono il sistema:

$$\begin{cases} z_0\frac{z_2}{3} - (\frac{z_1}{3})^2 = 0 \\ z_0z_3 - \frac{z_2z_1}{9} = 0 \\ \frac{z_1}{3}z_3 - (\frac{z_2}{3})^2 = 0 \end{cases} . \tag{2.5}$$

Nel prossimo esempio si analizza il comportamento nel caso generale.

Sia $d \in \mathbb{N}$ allora vale in generale la mappa di Veronese:

$$\begin{aligned} &\upsilon_d : \mathbb{P}^1 \longrightarrow \mathbb{P}(S^d\mathbb{C}^n) \\ &[a_0, a_1] \longrightarrow [a_0^d, \ldots, \binom{d}{i} a_0^i a_1^{d-i}, \ldots, a_1^d] \text{ con } i \in (0, \ldots, d). \end{aligned} \tag{2.6}$$

In questo caso la matrice cataletticante risulta essere della forma:

$$\begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1,d} \\ c_{12} & c_{13} & \cdots & c_{1,d-1} \end{bmatrix} \tag{2.7}$$

i cui minori $2 * 2$ formano un sistema di equazioni che definisce una varietà proiettiva.

Remark. Nel caso generale considetato l'ideale generato dai minori $2 * 2$ della matrice cataletticante risulta ancora un ideale primo.

Si procede dunque con il passaggio successivo che porterà alla definizione del metodo di Sylvester.

Capitolo 3

Polinomi e intersezioni con la curva di Veronese

Si consideri un polinomio $p(w_0, w_1) = z_0 w_0^d + z_1 w_0^{d-1} w_1 + \cdots + z_d w_1^d \in \mathbb{P}(S^d\mathbb{C}^2)$ di grado d, lo scopo dell'algoritmo di Sylvester è definire $\lambda_i \in \mathbb{C}$ e $\mathbf{L}_i = a_{0,i} w_0 + a_{1,i} w_1$, ovvero dei polinomi omogenei di primo grado chiamati comunemente forme lineari, tali che per un certo $m \in \mathbb{N}$ valga $p(w_0, w_1) = \sum_{i=1}^{m} \lambda_i \mathbf{L}_i^d$.

Si può considerare il polinomio $p(w_0, w_1)$ come un punto $\mathbf{P} = [z_0, \ldots, z_d] \in \mathbb{P}^d = \mathbb{P}(S^d\mathbb{C}^2)$, scegliendo come base di $\mathbb{P}^d$ i vettori indipendenti $[w_0^d, w_0^{d-1} w_1, \ldots, w_1^d]$.

Il caso più fortunato è quello in cui:
$\exists\ a_0, a_1, \lambda \in \mathbb{C}$ tali che $p(w_0, w_1) = \lambda(a_0 w_0 + a_1 w_1)^d = \lambda \mathbf{L}^d$, non c'è nulla da dire a riguardo.

Si passa dunque al caso successivo, comunque semplice, che permette di intuire quello che sarà il comportamento nel caso generale.

Sia $\mathbf{P} = p(w_0, w_1) = \lambda_1(a_{0,1} w_0 + a_{1,1} w_1)^d + \lambda_2(a_{0,2} w_0 + a_{1,2} w_1)^d = \lambda_1 \mathbf{L}_1^d + \lambda_2 \mathbf{L}_2^d$ con $a_{i,j}, \lambda_j \in \mathbb{C}$ per $i = 0, 1$ e $j = 1, 2$.
Si denoti con C_d la curva di Veronese di grado d, ovvero $C_d := \upsilon_d(\mathbb{P}^1)$. In questo caso il polinomio interseca la curva di Veronese in due punti, denotati con P_1, P_2 (che sono appunto $\mathbf{L}_1^d, \mathbf{L}_2^d$ in cui si scompone il polinomio),

dunque vale:

$$\mathbf{P} \in \bigcup_{P_1,P_2 \in C_d} \langle P_1, P_2 \rangle \tag{3.1}$$

l'insieme di tutte le rette che intersecano C_d in due punti, denotato con $\sigma_2^0(C_d)$.
Si può notare ora che $\sigma_2^0(C_d)$ non è una varietà. Infatti tutti i polinomi che si annullano in $\sigma_2^0(C_d)$ si annullano pure su tutte le tangenti alla curva C_d. Si definisce dunque l'insieme $\sigma_2(C_d)$, detta varietà delle bi-secanti a C_d nel seguente mondo:

$$\sigma_2(C_d) = (\bigcup_{P_1,P_2 \in C_d} \langle P_1, P_2 \rangle) \cup (\bigcup_{P \in C_d} Tg_P C_d) = \overline{\bigcup_{P_1,P_2 \in C_d} \langle P_1, P_2 \rangle}. \tag{3.2}$$

dove la chiusura è stata presa rispetto alla topologia di Zariski che è stata definita nel primo capitolo e $\bigcup_{P \in C_d} Tg_P C_d$ è lo spazio delle tangenti alla curva.
Il nome deriva dal fatto che si costruisce l'insieme partendo dallo spazio delle rette secanti in due punti la curva di Veronese e si è imposto storicamente nonostante, pur essendo esso un insieme algebrico proiettivo, non sia necessariamente una varietà proiettiva.

Osservazione 3.1. Un risultato in questo ambito è che costruendo la varietà delle secanti partendo da un insieme che è una varietà, essa è effettivamente una varietà. Un semplice esempio del fatto che questà proprietà non si verifichi se si sceglie un insieme qualsiasi si ha costruendo la varietà delle bi-secanti partendo da tre generici punti nello spazio.

Le equazioni che definiscono la varietà $\sigma_2(C_d)$ si trovano calcolando i minori $3 * 3$ della matrice cataletticante:

$$\begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1,d-2} \\ c_{12} & c_{13} & \cdots & c_{1,d-1} \\ c_{13} & c_{14} & \cdots & c_{1,d} \end{bmatrix} \text{ dove } c_{ij} = \binom{d}{i}^{-1} z_{i+j-2}. \tag{3.3}$$

Se ora viceversa si considerasse un polinomio $p(w_0, w_1) = z_0 w_0^d + z_1 w_0^{d-1} w_1 + \cdots + z_d w_1^d$ tale che $\mathbf{P} = [z_0, \ldots, z_d]$ soddisfi le equazioni che definiscono

$\sigma_2(C_d)$, ovvero $\mathbf{P} \in \sigma_2(C_d) \setminus C_d$, allora ci sono due possibilità:

$$p(w_0, w_1) = \begin{cases} \lambda_1 \mathbf{L}_1^d + \lambda_2 \mathbf{L}_2^d, \text{ se } \mathbf{P} \in \sigma_2^0(C_d) \text{ per } \mathbf{L}_1, \mathbf{L}_2 \text{ forme lineari} \\ \mathbf{P} \text{ sta sullo spazio delle tangenti a } C_d. \end{cases} \tag{3.4}$$

Per studiare il secondo caso è necessario introdurre il seguente risultato, per la dimostrazione si consulti [4] in bibliografia:

Teorema di Bertini
Sia X una varietà proiettiva di dimensione n tale che $X \subset \mathbb{P}^N$ con $n < N$.
Sia $H \subset \mathbb{P}^N$ uno spazio lineare generico tale che
dim(H)=codim(X)=N-n.
Allora $H \cap X$ è un insieme di punti e $\#(H \cap X)$ =grado di X.

Si supponga che $\mathbf{P}$ appertanga allo spazio delle tangenti:
allora esiste un punto P_1 sulla curva C_d tale che $\mathbf{P} \in Tg_{P_1} C_d$.
Si conisderi un generico iperpiano H che contenga $\mathbf{P}$. Quindi H è uno spazio linerare di dimensione $d-1$, poiché si lavora nello spazio $\mathbb{P}^d = \mathbb{P}(S^d\mathbb{C}^2)$ e C_d è una curva posso applicare il teorema di Bertini.
Questo mi assicura che H interseca C_d in d punti, poiché l'unico piano che contiene $\mathbf{P}$ e non ha questa proprietà è quello diretto lungo la tangente, poiché C_d è la curva razionale normale di grado d. Siano questi punti $\mathbf{L}_1, \ldots, \mathbf{L}_d$, essendo questi punti linearmente indipendenti (risultato che sarà dimostrato in seguito) generano uno spazio di dimensione $d-1$, dunque $\langle \mathbf{L}_1, \ldots, \mathbf{L}_d \rangle = H$.
Allora $\mathbf{P} \in \langle \mathbf{L}_1, \ldots, \mathbf{L}_d \rangle$ quindi, per concludere $\exists\, \lambda_1, \ldots, \lambda_n \in \mathbb{C}$ tali che $\mathbf{P} = \lambda_1 \mathbf{L}_1 + \cdots + \lambda_d \mathbf{L}_d$.

Si è appena dimostrato che se $\mathbf{P}$ sta nello spazio tangente allora $p(w_0, w_1)$ si decompone nella somma in al più d forme lineari.
Segue la dimostrazione del fatto che, nelle ipotesi precedenti, servano esattamente d forme lineari per decomporre $p(w_0, w_1)$.

Sia P_1 sulla curva C_d tale che $\mathbf{P} \in Tg_{P_1} C_d$ e si supponga esistano $\mathbf{M}_1, \ldots, \mathbf{M}_{d-1}$ forme lineari e $\alpha_1, \ldots, \alpha_d - 1 \in \mathbb{C}$ tali che $\mathbf{P} = \alpha_1 \mathbf{M}_1^d + \cdots + \alpha_{d-1} \mathbf{M}_{d-1}^d$.
Sia $H_1 = \langle \mathbf{M}_1, \ldots, \mathbf{M}_{d-1} \rangle = \mathbb{P}^{d-2}$, poiché insiemisticamente $H_1 \cap Tg_{P_1} C_d = \mathbf{P}$ allora $\langle H_1 \cap, Tg_{P_1} C_d \rangle = \mathbb{P}^{d-1}$.

Cosideriamo ora $Tg_{P_1}C_d$, esso è infatti generato da due punti (coincidenti all'limite) su C_d, essendo $H_1 \cap Tg_{P_1}C_d = \mathbf{P}$ e $\mathbf{P} \notin C_d$ allora questi punti non possono coincidere con i generatori di H_1. Dunque si può interpretare $\langle H_1 \cap, Tg_{P_1}C_d \rangle$ come uno spazio generato da $d+1$ punti su C_d che come si dimostrerà sono linearmente indipendenti, per cui $\langle H_1 \cap, Tg_{P_1}C_d \rangle = \mathbb{P}^d$, si verifica una contraddizione.

Segue la dimostrazione dell'indipendenza lineare dei punti in C_d.
Essendo la curva di Veronese:

$$\upsilon_d : \begin{array}{c} \mathbb{P}^1 \longrightarrow \mathbb{P}(S^d\mathbb{C}^n) \\ [a_0, a_1] \longrightarrow [a_0^d, \ldots, \binom{d}{i} a_0^{d-i} a_1^i, \ldots, a_1^d] \text{ con } i \in (0, \ldots, d). \end{array}$$

considerando n punti su C_d le loro coordinate sono:

$$P_j = [a_{0,j}^d, \ldots, \binom{d}{i} a_0^{d-i} a_1^i, \ldots, a_{1,j}^d] \text{ per } j = 1, \ldots, n \text{ e } i = 0, \ldots, d.$$

Deomogenizzando rispetto ad a_0 ed effettuando il cambio di variabile $T_j = \frac{a_{1,j}}{a_{0,j}}$ si riduce il problema alla dimostrazione del fatto che i punti $P_j = (1, dT_j, \ldots, \binom{d}{i} T_j^i, \ldots, T_j^d)$ per $j = 1, \ldots, n$ e $i = 0, \ldots, d$ siano linearmente indipedenti nello spazio affine $\mathbb{A}^{d+1}$ associato a $\mathbb{P}^d$.
Per la definizione di lineare indipendenza ciò si verifica se e solo se dato il sistema

$$\begin{cases} \alpha_1 + \cdots + \alpha_n = 0 \\ \alpha_1 dT_j + \cdots + \alpha_n dT_j = 0 \\ \vdots \\ \alpha_1 T_j^d + \cdots + \alpha_n T_j^d = 0 \end{cases} \tag{3.5}$$

ove le variabili sono $\alpha_1, \ldots, \alpha_n$, abbia unica soluzione
$(\alpha_1, \ldots, \alpha_n) = (0, \ldots, 0)$.
Che sia soluzione è evidente, per dimostrare che è unica si considera la matrice dei coefficienti, poiché se essa ha determinante non nullo la soluzione al sistema di equazioni è unica.

Si consideri dunque la matrice

$$\begin{bmatrix} 1 & \cdots & 1 \\ dT_1 & \cdots & dT_n \\ \vdots & \vdots & \vdots \\ T_1^d & \cdots & T_n^d \end{bmatrix} \tag{3.6}$$

se il suo determinante fosse nullo dovrebbe esistere una riga, si supponga sia la $(k+1)$-esima riga $(\binom{d}{k}T_1^k, \ldots, \binom{d}{k}T_n^k)$, che sia combianzione lineare delle altre, ovvero tale che esistano $\beta_m \in \mathbb{C}$ con $m = 0, \ldots, k-1, k+1, \ldots, d$ per cui

$$(\binom{d}{k}T_1^k, \ldots, \binom{d}{k}T_n^k) = \beta_0(1, \ldots, 1) + \cdots +$$

$$+\beta_{k-1}(\binom{d}{k-1}T_1^{k-1}, \ldots, \binom{d}{k-1}T_n^{k-1}) + \beta_{k-+}(\binom{d}{k+1}T_1^{k+1}, \ldots, \binom{d}{k+1}T_n^{k+1}) +$$

$$+ \cdots + \beta_d(T_1^d, \ldots, T_n^d)$$

ovvero che, più in breve , per $j = 1, \ldots, n$:

$$\binom{d}{k}T_j^k = \beta_0 + \cdots + \beta_{k-1}\binom{d}{k-1}T_j^{k-1} + \beta_{k-1}\binom{d}{k+1}T_j^{k+1} + \cdots + \beta_d T_j^d. \tag{3.7}$$

A membro destro compare un monomio di grado k e a mebro sinistro compare un polinomio di grado sempre diverso da k.
Allora i punti sono linearmente indipendenti. Chiaramente la stessa dimostrazione funziona per la scelta di qualunque altra riga anche se diversa dalla (k+1)-esima.

Un immediato corollario è che nel caso $\mathbf{P} = \lambda_1\mathbf{L}_1 + \cdots + \lambda_d\mathbf{L}_d$ la scrittura non è unica. Infatti cambiando la scelta di H, che era un generico iperpiano contenente $\mathbf{P}$ cambiano anche le intersezioni con la curva C_d.

Si utilizzano ora i riultati ottenuti per analizzare il caso generale.
Si consideri questa volta lo spazio genrato da r punti sulla curva C_d:

$$\sigma_r^0(C_d) = \bigcup_{P_1,\ldots,P_r \in C_d} \langle P_1, \ldots, P_r \rangle \tag{3.8}$$

e si definisce $\sigma_r(C_d)$ la varietà delle r-secanti a C_d, la chiusura rispetto alla topologia di Zariski di $\sigma_r^0(C_d)$:

$$\sigma_r(C_d) = \overline{\bigcup_{P_1,\dots,P_r \in C_d} \langle P_1, \dots, P_r \rangle} = (\bigcup_{P_1,\dots,P_r \in C_d} \langle P_1, \dots, P_r \rangle) \cup (\bigcup_{P \in C_d} Tg_P C_d) \tag{3.9}$$

Sia $\mathbf{P} \in \sigma_r(C_d) \setminus C_d$ allora:

$$p(w_0, w_1) = \begin{cases} \lambda_1 \mathbf{L}_1^d + \cdots \lambda_r \mathbf{L}_r^d, \text{ se } \mathbf{P} \in \sigma_r^0(C_d) \text{ per } \mathbf{L}_1, \dots, \mathbf{L}_r \text{ forme lineari} \\ \lambda_1 \mathbf{L}_1^d + \cdots + \lambda_d \mathbf{L}_d^d \text{ se } \mathbf{P} \text{ è nello spazio delle tangenti a } C_d. \end{cases} \tag{3.10}$$

Si dimostra ora la validità della seguente catena di inclusioni:

$$C_d = \sigma_1(C_d) \subset \sigma_2(C_d) \subset \sigma_3(C_d) \subset \cdots \ . \tag{3.11}$$

L'uguaglianza $C_d = \sigma_1(C_d)$ è immediatamente verificata poiché:

$$\sigma_1(C_d) = \bigcup_{P \in C_d} \langle P \rangle = \bigcup_{P \in C_d} P = C_d.$$

Valgono le inclusioni poiché:

$$\bigcup_{P_1,\dots,P_n \in C_d} \langle P_1, \dots, P_n \rangle \ni P = \lambda_1 P_1 + \cdots + \lambda_n P_n =$$

$$= \lambda_1 P_1 + \cdots + \lambda_n P_n + 0 P_{n+1} \in \bigcup_{P_1,\dots,P_{n+1} \in C_d} \langle P_1, \dots, P_{n+1} \rangle \ \forall\ \lambda_1, \dots, \lambda_n \in \mathbb{C}$$

e lo spazio delle tangenti alla curva è il medesimo per ogni scelta iniziale del numero dei punti.
Dunque la catena di inclusioni è dimostrata.

Un risultato fondamentale, ultimo passo per arrivare ad enunciare compiutamente l'algoritmo di Sylvester nella sua forma basilare, è il seguente.

Nel caso in cui $\mathbf{P} \in \sigma_r(C_d) \setminus \sigma_{r-1}(C_d)$ vale:

$$\mathbf{P} = \lambda_1 \mathbf{L}_1^d + \cdots + \lambda_{d-r+2} \mathbf{L}_{d-r+2}^d \text{ con } \lambda_1, \dots, \lambda_{d-r+2} \in \mathbb{C}. \tag{3.12}$$

Una dimostrazione si può trovare in [2].

Capitolo 4

Algoritmo di Sylvester

Lo scopo di questo capitolo è di elencare i passi che descrivono l'algoritmo e dare un esempio pratico dell'utilizzo dello stesso.

Inizialmente si costruisce la matrice cataletticante, come nel secondo capitolo, associata al polinomio omogeneo p su cui si intende applicare l'algoritmo, sia $p = \sum_{k=0}^{d} z_k w_0^k w_1^{d-k}$ allora si considera la matrice $M_{d-r,r}(p)$ associata a p come $M_{d-r,r}(p) = [c_{ij}]_{ij}$ dove $c_{ij} = \binom{d}{i}^{-1} z_{i+j-2}$ per $i = 1, \ldots, d-r$ e $j = 1, \ldots, r$.
Si può ora introdurre il vero algoritmo:
(1) si ponga inzialmente r=0;
(2) si incrementi $r \leftarrow r + 1$;
(3) si calcoli il rango della matrice $M_{d-r,r}(p)$, se il rango della matrice è massimo si torni al punto (2), altrimenti si proceda;
(4) si calcoli una base per il Kernel destro della matrice $M_{d-r,r}(p)$, ovvero una base $\{v_1, \cdots, v_m\}$ dello spazio dei vettori tale che, sia v un vettore generico, $M_{d-r,r}(p) * v = 0$;
(5) raffinamento:

- si prenda un vettore q nel kernel destro, in generale varrà $q = \sum_i \beta_i v_i$;
- si calcolino le radici del polinomio associato a q, $q(w_0, w_1) = \sum_{i=0}^{r} q_i w_0^i w_1^{r-i}$ dove q_i è la componente i-esima di q, si denotino le radici di questo polinomio come (α_j, γ_j) in modo che $|\alpha_j|^2 + |\gamma_j|^2 = 1$;
- se le soluzioni non sono distinte tra loro in $\mathbb{P}^1$ si ritorni al punto (2);

- altrimenti, trovate r distinte radici, si calcolino i coefficienti λ_j dati dalle soluzioni del sistema:
$$\begin{bmatrix} \alpha_1^d & \cdots & \alpha_r^d \\ \alpha_1^{d-1}\gamma_1 & \cdots & \alpha_r^{d-1}\gamma_r \\ \alpha_1^{d-2}\gamma_1^2 & \cdots & \alpha_r^{d-2}\gamma_r^2 \\ \vdots & \vdots & \vdots \\ \gamma_1^d & \cdots & \gamma_r^d \end{bmatrix} \lambda = \begin{bmatrix} z_0 \\ \frac{1}{d}z_1 \\ \binom{d}{2}^{-1} z_2 \\ \vdots \\ z_d \end{bmatrix}$$

(6) si scrive dunque la decomposizione di p come $p = \sum_{j=1}^{r} \lambda_j \mathbf{L}_j^d$ dove $\mathbf{L}_j^d = (\alpha_j z_0 + \gamma_j z_1)$.

4.1 Due Esempi

In questa sezione conclusiva si mostrerà la decomposizione di due polinomi attraverso l'utilizzo dell'algoritmo appena presentato.

Primo esempio:
Si consideri il polinomio omogeneo di quarto grado (dunque d=4):

$$p = w_0^4 - 12w_0^2w_1^2 + 24w_0w_1^3 - 14w_1^4.$$

Svolgendo i primi passi dell'algoritmo si trova che la prima matrice a rango non massimo si ha con r=2 ed è:

$$M_{2,2}(p) = \begin{bmatrix} 1 & 0 & -2 \\ 0 & -2 & 6 \\ -2 & 6 & -14 \end{bmatrix}$$

infatti calcolando il rango si trova rk($M_{2,2}(p)$)=2.
Procedendo con il punto (4) si trova che il kernel destro è $Ker(M_{2,2}(p)) = \langle(2, 3, 1)\rangle$.
Dunque, cercando il polinomio associato ad un vettore nel kernel, si può scegliere come vettore semplicemente la base trovata ottenendo:

$$q(w_0, w_1) = 2w_0^2 + 3w_0w_1 + w_1^2.$$

La fattorizzazione di questo polinomio è immediata e risulta $q(w_0, w_1) = (w_0 + w_1)(2w_0 + w_1)$.

Considerando dunque le soluzioni normalizzate, per soddisfare il secondo punto del raffinamento, $(\alpha_1, \gamma_1) = (\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}})$ e $(\alpha_2, \gamma_2) = (-\frac{1}{\sqrt{5}}, \frac{2}{\sqrt{5}})$ si calcolano i coefficienti λ_1 e λ_2 attraverso il sistema:

$$\begin{bmatrix} \frac{1}{4} & \frac{1}{25} \\ -\frac{1}{4} & -\frac{2}{25} \\ \frac{1}{4} & \frac{4}{25} \\ -\frac{1}{4} & -\frac{8}{25} \\ \frac{1}{4} & \frac{16}{25} \end{bmatrix} \lambda = \begin{bmatrix} 1 \\ 0 \\ -2 \\ 4 \\ -14 \end{bmatrix} \text{ da cui } \lambda_1 = 8, \lambda_2 = -25.$$

Si può finalmente decomporre:

$$p = w_0^4 - 12w_0^2w_1^2 + 24w_0w_1^3 - 14w_1^4 = 8(\frac{1}{\sqrt{2}}w_0 - \frac{1}{\sqrt{2}}w_1)^4 - (-\frac{1}{\sqrt{5}}w_0 + \frac{2}{\sqrt{5}}w_1)^4$$

quindi semplificando:

$$p = 2(w_0 - w_1)^4 - (-w_0 + 2w_1)^4.$$

Secondo Esempio:
Si consideri questa volta un polinomio di grado 3:

$$r = 9w_0^2w_1 - 9w_0w_1^2 + 10w_1^3$$

In questo caso la prima matrice a rango non massimo è:

$$M_{0,3}(r) = \begin{bmatrix} 0 \\ 3 \\ -3 \\ 10 \end{bmatrix}.$$

Prendendo il vettore $t = [2, -1, -1, 0]$ che appartiene al kernel valendo:

$$M_{0,3}(r) \cdot t = -3 + 3 = 0$$

si calcola il polinomio:
$t(w_0, w_1) = 2w_0^3 - w_0^2w_1 - w_0w_1^2 = w_0(w_0 - w_1)(2w_0 + w_1)$.
Considerando, per il secondo punto del raffinamento, le soluzioni
$(0, 1), (\frac{1}{\sqrt{5}}, \frac{-2}{\sqrt{5}})$ e $(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$ si ricavano infine i tre coefficienti che risultano

essere $1, -5\sqrt{5}, 2\sqrt{2}$ per cui si può scrivere:

$$r = 9w_0^2w_1 - 9w_0w_1^2 + 10w_1^3 = w_1^3 - (w_0 - 2w_1)^3 + (w_0 + w_1)^3.$$

Ricordando che nel caso $r = d$ la scelta non è unica, si può, riferendosi all'ultimo esempio, scegliere come vettore nel kernel $t_1 = [0, 1, 1, 0]$ e seguendo gli stessi passaggi si ottiene una seconda decomposizione:

$$r = 9w_0^2w_1 - 9w_0w_1^2 + 10w_1^3 = w_1^3 + 3w_0^3 - 3(w_0 - w_1)^3.$$

Bibliografia

[1] J. Harris, *Algebraic geometry. A first course*, Springer Verlang, 1992;

[2] G. Comas & M. Seiguer, *On the rank of a binary form*, arXiv, 2001;

[3] M. Reid, *Undergraduate Commutative Algebra*, Cambridge University Press, 1995;

[4] R.Hartshorne, *Algebraic Geometry*,Springer-Verlag, 1977;

[5] Grayson, Daniel R. and Stillman, Michael E., Macaulay2, a software system for research in algebraic geometry, Available at `http://www.math.uiuc.edu/Macaulay2/`.