Appunti per Geometria e Algebra Computazionale 3-1. Matrici compagne, interpolazione polinomiale.

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

Giorgio Ottaviani

12 maggio 2020

Introduzione alle matrici compagne

In questa sezione ricordiamo come il calcolo delle radici di un polinomio può essere ricondotto al calcolo degli autovalori di una matrice, detta matrice compagna. Questo è interessante perché esistono molti algoritmi per calcolare numericamente gli autovalori di una matrice.
La struttura algebrica che nasce da questa problema ha delle generalizzazioni nel caso di più variabili, che studieremo successivamente

L'anello quoziente e la matrice compagna

Sia $f(x) = \sum_{i=0}^{d} a_i x^i$ un polinomio di grado d, che possiamo supporre monico, cioè $a_d = 1$. Chiamiamo R l'anello quoziente $K[x]/(f(x))$ che ha dimensione d ed è generato dalle classi $[1], [x], \ldots, [x^{d-1}]$. Infatti x^d può essere scritto come combinazione delle potenze precedenti modulo f, $[x^d] = -\sum_{i=0}^{d-1} a_i [x^i]$ e cosìanche le potenze successive, ad esempio
$[x^{d+1}] = -\sum_{i=0}^{d-1} a_i [x^{i+1}] = -\sum_{i=0}^{d-2} a_i [x^{i+1}] + a_{d-1} \sum_{i=0}^{d-1} a_i [x^i]$

Definizione

La moltiplicazione per x induce un'applicazione lineare

$$R \xrightarrow{M_x} R$$

$$[g] \mapsto [gx]$$

la matrice di M_x rispetto alla base $[1], [x], \ldots, [x^{d-1}]$ si dice matrice compagna di $f(x)$.

Espressione esplicita della matrice compagna

Proposizione

La matrice compagna di $f(x)$ è

$$\begin{bmatrix} 0 & 0 & \ldots & -a_0 \\ 1 & 0 & \ldots & -a_1 \\ 0 & 1 & \ldots & -a_2 \\ \vdots & & & \vdots \\ 0 & 0 & 1 & -a_{d-1} \end{bmatrix}$$

Dimostrazione.

È un calcolo immediato dalle espressioni precedenti. □

La matrice M_h e le sue proprietà

Definizione

Analogamente la moltiplicazione per $h(x)$ induce un'applicazione lineare

$$R \xrightarrow{M_{h(x)}} R$$

$$[g] \mapsto [gh]$$

Proposizione

$\forall\ h(x), k(x) \in K[x]$ *vale che*
(i) $M_{h(x)} + M_{k(x)} = M_{h(x)+k(x)}$
(ii) $M_{ah(x)} = aM_{h(x)} \quad \forall a \in K$
(iii) $M_{h(x)} \cdot M_{k(x)} = M_{k(x)} \cdot M_{h(x)} = M_{h(x)k(x)}$
(iv) $M_{h(k(x))} = h(M_{k(x)})$*, in particolare* $M_{h(x)} = h(M_x)$.

Dimostrazione delle proprietà di M_h

Dimostrazione.

(i), (ii) e (iii) sono immediate dalla definizione. Notiamo che la commutatività in (iii) segue dalla commutatività dei polinomi. Per provare (iv) supponiamo dapprima $h = x^i$. Allora $M_{(k(x))^i} = \left(M_{k(x)}\right)^i$ come diretta applicazione di (iii).
In generale, se $h(x) = \sum a_i x^i$ allora utilizzando anche (i)-(iii)

$$M_{h(k(x))} = M_{\sum a_i (k(x))^i} = \sum a_i M_{(k(x))^i} = \sum a_i \left(M_{(k(x))}\right)^i = h(M_{k(x)})$$

$\square$

Teorema

(i) A meno di scalari moltiplicativi, $f(x)$ è il polinomio minimo di M_x.
(ii) A meno di scalari moltiplicativi, $f(x)$ è il polinomio caratteristico di M_x.
(iii) M_x è diagonalizzabile su $\mathbb{C}$ se e solo se $f(x)$ ha radici distinte.
(iv) $f(x_0) = 0$ se e solo se x_0 è un autovalore di M_x.
(v) $tr(M_{h(x)}) = \sum_{i=1}^{n} h(\lambda_i)$ dove $\lambda_1, \ldots, \lambda_n$ sono le radici di $f(x)$
(vi) $\det(M_{h(x)}) = \prod_{i=1}^{n} h(\lambda_i)$, in particolare $\det(M_{h(x)})$ si annulla se e solo se f e h hanno una radice in comune, e costituisce un metodo alternativo (in generale più economico) di calcolo del risultante $Res(f, h)$.

Dimostrazione.

Per ogni polinomio $p(x)$ abbiamo che $p(M_x) = M_{p(x)}$, che è nulla esattamente quando $p(x)$ è un multiplo di $f(x)$ (basta applicare $M_{p(x)}$ alla classe di 1). Pertanto $f(x)$ è il polinomio minimo di M_x, e siccome divide il polinomio caratteristico, che ha lo stesso grado, segue che polinomio minimo e polinomio caratteristico coincidono, a meno del segno. (iii) è conseguenza di (i) e del fatto che una matrice è diagonalizzabile se e solo se il polinomio minimo ha radici distinte. (iv) è immediata da (ii). (v) e (vi) seguono triangolarizzando A. □

Osservazione L'importanza della teoria spettrale delle matrici compagne risiede nel fatto che otteniamo le radici del polinomio f dal calcolo degli autovalori della matrice compagna, che può essere effettuato ad esempio col metodo QR.

Il teorema cinese dei resti per polinomi

Sia $n = \prod_{i=1}^{k} p_i^{m_i}$ con p_i primi distinti. La forma classica del teorema cinese dei resti, su $\mathbb{Z}$, descrive l'isomorfismo

$$q\colon \mathbb{Z}/n \to \oplus_{i=1}^{k}\mathbb{Z}/(p_i^{m_i})$$

L'estensione naturale ai polinomi è data dal seguente

Teorema (Teorema cinese dei resti per polinomi)

Sia $f(x) = \prod_{i=1}^{k} f_i^{n_i}$ con f_i irriducibili distinti. Sia $g_i = \frac{f}{f_i^{n_i}}$, siano b_i tali che $\sum_{i=1}^{k} b_i g_i = 1$ (ricavabili con l'algoritmo euclideo, o con M2). L'applicazione naturale

$$q\colon K[x]/(f(x)) \to \oplus_{i=1}^{k} K[x]/(f_i^{n_i})$$

definita da $q(h) = (h, \ldots, h)$ è un isomorfismo con inversa data da

$$\tilde{q}\colon \ \oplus_{i=1}^{k} K[x]/(f_i^{n_i}) \to K[x]/(f(x))$$

definita da $\tilde{q}(a_1, \ldots, a_k) = \sum_{i=1}^{k} b_i g_i a_i$.

Dimostrazione del teorema cinese dei resti per polinomi

Dimostrazione.

$b_i g_i$ modulo $f_j^{n_j}$ è uguale a 1 se $i = j$, è uguale a 0 se $i \neq j$. Pertanto $\sum_{i=1}^{k} b_i g_i a_i$ modulo $f_j^{n_j}$ è uguale ad a_j $\forall j$. Da queste condizioni si ricava che, componendo $q\tilde{q}$ e $\tilde{q}q$, si ottiene in entrambi i casi l'identità. $\square$

Osservazione

Con Macaulay2, b_i *puo' essere trovato tramite il comando*

```
quotientRemainder(matrix{{1}},matrix{{g_1,...g_k}})
```

Notiamo che per calcolare questi quozienti è necessario trovare la base di Groebner dell'ideale $(g_1, \ldots, g_k)$*, che è uguale a* 1*, e che essenzialmente questo calcolo corrisponde all'algoritmo euclideo del calcolo del MCD tra i* g_i*.*

Interpolazione di Hermite

Corollario (Interpolazione di Hermite)

Siano $c_1, \ldots, c_k \in \mathbb{R}$ *punti distinti. Assegniamo, rispetto a ogni punto* c_i*, uno sviluppo di Taylor* $a_i(x)$ *di grado* $< m_i$*, questo equivale a dare* $a_i(x) = \sum_{j=0}^{m_i-1} \frac{\alpha_{j,i}}{j!}(x-c_i)^j$ *dove* $\alpha_{j,i} = a_i^{(j)}(c_i)$ *è la derivata* j*-esima di* a_i *valutata in* c_i*.*
Esiste un polinomio $H(x)$ *di grado* $< \sum_{i=1}^k m_i$*, tale che* $H^{(j)}(c_i) = \alpha_{j,i}$ *per* $0 \le j < m_i$*, definito da* $H = \sum_{i=1}^k b_i g_i a_i$ *modulo* $f(x) = \prod_{i=1}^k (x-c_i)^{m_i}$ *(cioè H%ideal(f)) dove , posto* $f_i = (x-c_i)^{m_i}$*,* $g_i = \prod_{j \neq i}(x-c_j)^{m_j}$*,* b_i *viene ottenuto dall'algoritmo euclideo come nel Teorema cinese, cioè dalla condizione* $b_i g_i + r_i f_i = 1$*.*

Dimostrazione.

La condizione $H(x) = a_i(x)$ modulo $(x-c_i)^{m_i}$, equivale a $H^{(j)}(c_i) = a_i^{(j)}(c_i)$. Il risultato segue allora dal Teorema cinese. □

Approfondimento sull'interpolazione di Hermite

Osservazione

Il polinomio $H(x) = \sum_{i=1}^{k} b_i(x) g_i(x) a_i(x)$ *ha le derivate richieste nei punti* c_i*. Considerare la sua forma normale rispetto a* f *serve soltanto per abbassare il grado fino a renderlo* $< \sum_{i=1}^{k} m_i = \deg f$*.*

Per $m_i = 1$ abbiamo come caso particolare l' interpolazione di Lagrange, dove si ricava un polinomio di grado $k-1$ che assume k valori assegnati.

Interpolazione di Lagrange

Corollario (Interpolazione di Lagrange)

Siano $c_1, \ldots, c_k \in \mathbb{R}$ *punti distinti. Assegniamo, rispetto a ogni punto* c_i*, un valore* $a_i \in K$*.*
Esiste un polinomio $H(x)$ *di grado* $< k$*, tale che* $H(c_i) = a_i$ *, definito da* $H = \sum_{i=1}^{k} b_i g_i a_i$ *dove* $g_i = \prod_{j \neq i}(x - c_j)$*,*
$b_i = \frac{1}{\prod_{j \neq i}(c_i - c_j)}$.

Dimostrazione.

Rispetto all'interpolazione di Hermite, si può scegliere b_i come lo scalare nell'enunciato, infatti $b_i g_i = \frac{\prod_{j \neq i}(x - c_j)}{\prod_{j \neq i}(c_i - c_j)}$ vale 1 su c_i e vale 0 su c_j per $j \neq i$. Il grado di $\sum_{i=1}^{k} b_i g_i a_i$ risulta immediatamente $< k$. $\square$

L'interpolazione di Hermite è utile nello sviluppo di una funzione razionale in fratti semplici, necessaria per la sua integrazione. Infatti, con le notazioni precedenti, dopo aver trovato un'espressione $1 = \sum_{i=1}^{k} b_i g_i$, dividendo per $f(x)$ si ottiene $\frac{1}{f(x)} = \sum_{i=1}^{k} \frac{b_i(x)}{(x-c_i)^{m_i}}$ da cui per un polinomio g

$$\frac{g(x)}{f(x)} = \sum_{i=1}^{k} \frac{g(x)b_i(x)}{(x-c_i)^{m_i}}$$

Calcolando lo sviluppo di Taylor dei numeratori $g(x)b_i(x)$ rispetto al punto c_i, si ottiene l'espressione che puo' essere facilmente integrata.

Esercizio

Si trovi, con l'ausilio di Macaulay2, un polinomio di grado 8 *tale che* $H(2) = \alpha$, $H'(2) = \beta$, $H(3) = 5$, $H'(3) = 7$, $H''(3) = 11$, $H(4) = 13$, $H'(4) = 17$, $H''(4) = 19$, $H'''(4) = 21$, *al variare di* α, β.