Ancora con l'induzione matematica

Informatica@SEFA 2017/2018 - Lezione 9

Massimo Lauria <massimo.lauria@uniroma1.it>*

Venerdì, 21 Ottobre 2017

L'induzione matematica sembra, per come vi è stata presentata la scorsa lezione, un pasto precotto da utilizzare in maniera molto rigida. Oggi vedremo degli esempi nei quali l'uso dell'induzione è utile o addirittura necessario, ma il modo in cui viene usata è leggermente meno ovvio. Prima però vediamo un esempio di induzione sbagliata che non siamo riusciti a fare la scorsa lezione.

Un esempio di induzione errata

Una classica applicazione sbagliata del principio d'induzione è la seguente "dimostrazione" che porta a concludere che

> Tutti i cavalli sono dello stesso colore

- Vediamo il caso base $P(1)$. Ovviamente in un insieme con un solo cavallo, tutti i cavalli dell'insieme sono nello stesso colore.
- Assumiamo che tutti gli insiemi di n cavalli siano dello stesso colore. Se prendiamo un I insieme di $n+1$ cavalli, possiamo ottenere due insiemi A e B di n cavalli togliendo da I due cavalli distinti. A e B sono rispettivamente costituiti da cavalli dello stesso colore (per l'ipotesi induttiva), e hanno $n-1$ cavalli in comune, che sono simultaneamente dello stesso colore dei cavalli in A e dei cavalli in B. Pertanto tutti i cavalli di A e B hanno lo stesso colore e quindi questo vale anche per i cavalli in I, poiché $I = A \cup B$.

*http://massimolauria.net/courses/infosefa2017/

Dunque tutti i cavalli hanno lo stesso colore, giusto? **Ovviamente no**. L'errore qui è nel caso del passo induttivo per $n = 1$. Ovvero la dimostrazione che $P(1)$ implica $P(2)$. Il fatto (vero) che gli insiemi di un solo cavallo sono monocromatici, non implica che anche gli insiemi di due cavalli lo siano. Nella dimostrazione abbiamo usato il fatto che l'intersezione di A e B è di $n-1$ cavalli, ma per $n = 1$ questa è vuota, e quindi non implica nessuna identità tra il colore dei cavalli residui in A e B.

Una breve panoramica degli assiomi di Peano

La scorsa lezione ho accennato all'aritmetica di Peano ed al fatto che il ragionamento matematico si basa sull'uso della logica formale per dedurre nuovi fatti da un sistema di assiomi. Non vedremo molte cose di logica, ma a questo punto mi sembra il caso di darvi l'assiomatizzazione formale dell'insieme $\mathbb{N}$ dei numeri naturali.

- Esiste $0 \in \mathbb{N}$
- Esiste una funzione *successore* $S : \mathbb{N} \to \mathbb{N}$
- Se $x \neq y$ allora $S(x) \neq S(y)$
- $S(x) \neq 0$ for every x
- Se $U \subseteq \mathbb{N}$ tale che
  - $0 \in U$
  - $x \in U$ implica $S(x) \in U$

  allora $U = \mathbb{N}$.

É quindi evidente che il principio di induzione è inerente ai numeri naturali, essendo parte della loro definizione assiomatica.

Dimostrazione. Definire U come l'insieme degli n per cui vale $P(n)$. □

Induzione su variabili multiple (e.g. due)

L'induzione su un parametro (nel nostro caso n) è l'esempio più semplice. É possibile fare induzione su parametri più complicati, ad esempio su variabili multiple.

Ordine lessicografico delle stringhe

Assumiamo di avere un alfabeto A di caratteri, e consideriamo le stringhe in A^*. In Python esiste un concetto di ordine tra stringhe, o più precisamente delle operazioni di confronto <, >, >=, <=. Queste operazioni determinano quale stringa è maggiore o minore basandosi sull'ordine lessicografico, che può essere definito per induzione.

L'ordine lessicografico di A^* si basa sull'ordine di A. Una volta che quest'ordine è ben definito allora si possono estendere le relazioni <, >, >=, <=. Ci limitiamo all'operazione <.

Definizione di $s < t$ dove $s, t \in A^*$. per induzione su due variabili $n = |s|$ e $m = |t|$.

- Se $m = 0$ allora $s < t$ è falso.
- Se $n = 0$ e $m > 0$ allora $s < t$ è vero.
- In tutti i casi rimanenti $n > 0$ e $m > 0$ quindi possiamo scrivere $s = as'$ e $t = bt'$ con $a, b \in A$
  - se $a < b$ allora $s < t$ è vero;
  - se $a > b$ allora $s < t$ è falso;
  - se $a = b$ allora $s < t$ se e solo se $s' < t'$.

```
def strless(s1,s2):
    if not isinstance(s1,str) or not isinstance(s1,str):
        raise ValueError("Gli argomenti devono essere due stringhe.")
    elif len(s2)==0:
        return False
    elif len(s1)==0:
        return True
    elif s1[0]<s2[0]:
        return True
    elif s1[0]>s2[0]:
        return False
    else:
        return strless(s1[1:],s2[1:])

def test_string_less(s1,s2):
  if strless(s1,s2) != (s1 < s2):
      return "Errore di implementazione."
  else:
      return min(s1,s2)

print(test_string_less("",""))
print(test_string_less("b","a"))
print(test_string_less("AB","AB"))
print(test_string_less('',"afsa17381b "))
print(test_string_less('prefisso',"pre"))
print(test_string_less('20',"100"))
```

```
a
AB

pre
100
```

In questo esempio ci sono due variabili in gioco, n e m, ma in realtà si sta facendo induzione matematica su un numero solo.

Esercizio: quale?

Coefficienti binomiali e fattoriali

Sappiamo che il coefficiente binomiale $\binom{n}{m}$ rappresenta una quantità intera: il numero di possibili sottoinsiemi di $\{1, 2, \ldots, n\}$ costituiti da m elementi.

Una nota proprietà di $\binom{n}{m}$ è che questo sia uguale a

$$\frac{(m+n)!}{n!m!}$$

che quindi deve essere un numero intero.

Esercizio: dimostrate per induzione che $n!m!$ divide $(m+n)!$. Anche qui ci sono due variabili in gioco, ma si può impostare un numero solo su cui fare induzione.

Indizio: può essere utile dimostrare che qualunque prodotto di r numeri consecutivi è divisibile per $r!$.

Esempio genuino di induzione doppia

Considerate la fuzione $f(m, n)$ definita per $m, n \geq 1$ per induzione doppia in questo modo:

- $f(1, 1) = 2$;
- $f(m+1, 1) = f(m, 1) + 2(m+1)$ per $m > 1$;
- $f(m, n+1) = f(m, n) + 2(m+n-1)$ per $m \in \mathbb{N}$ e $n > 1$.

Osservate ancora come i casi della definizione siano **mutuamente esclusivi**. Avremmo potuto definire la stessa funzione come una formula chiusa, infatti

$$f(m,n) = (m+n)^2 - (m+n) - 2n + 2\ . \tag{1}$$

Dimostrazione. Eseguiamo una doppia induzione su m e n. Per prima cosa mostriamo la proprietà per $n = 1$ e $m \in \mathbb{N}$, per induzione su m. Ovvero mostriamo che

$$f(m,1) = (m+1)^2 - (m+1)\ . \tag{2}$$

Nel caso base la proprietà è verificata: $f(1,1) = 2$. Per il passo induttivo assumiamo che (2) sia vera e allora abbiamo che $f(m+1,1) = f(m,1) + 2(m+1) = (m+1)^2+2(m+1)-(m+1)$. Scriviamo $(m+1)^2+2(m+1)-(m+1)$ come $(m+1)^2+2(m+1)+1-(m+2)$ ovvero $(m+1+1)^2-(m+2)$. Questo verifica il passo induttivo e quindi l'equazione (2) è vera.

Adesso possiamo fare un'altra induzione su n, con m fisso ma arbitrario. In questa seconda induzione il caso base è per $f(m,1)$, ed è dato immediatamente dall'equazione (2) dimostrata in precedenza.

Per il passo induttivo di questa secondo livello di induzione vediamo che $f(m,n+1) = f(m,n)+2(m+n-1) = (m+n)^2-(m+n)-2n+2+2(m+n-1)$ che può essere scritto come $(m+n)^2+2(m+n)+1-(m+n)-2n+2-3$ ovvero $(m+n+1)^2-(m+n+1)-2(n+1)-2$. □

Induzione non lineare

L'induzione non è una ricetta o uno schema fisso. A volte è solo un ingrediente ed è necessario avere altre idee per farne uso. Vediamo ora il caso di una dimostrazione per induzione nel quale l'uso dell'ipotesi induttiva non è così lineare.

Osservate questa disuguaglianza: $\sqrt{xy} \leq \frac{x+y}{2}$ per $x, y > 0$. Se la riscriviamo come $4\sqrt{xy} \leq 2x + 2y$ questa disuguaglianza ci dice che

- tra tutti i rettangoli con area fissa, quello con il **perimetro minore** è il quadrato; oppure
- tra tutti i rettangoli con perimetro fisso, quello con **l'area maggiore** è il quadrato.

Per vedere questo è sufficiente fissare un'area A. Per tutte le possibili scelte di x e y con $A = xy$, la disuguaglianza ci dice che il perimetro $2x + 2y$ sarà sempre uguale o maggiore del perimetro del quadrato di area A, che è $4\sqrt{A}$.

Prima di discutere la nostra induzione speciale, notate che $\sqrt{xy} \leq x/2+y/2$ si ottiene facilmente da $(\sqrt{x}-\sqrt{y})^2 \geq 0$.

I due lati della disuguaglianza $\sqrt{xy} \leq x/2+y/2$ generalizzano rispettivamente nelle due medie

- **M. geometrica.**
$$(a_1 a_2 \cdots a_n)^{1/n} \tag{3}$$
- **M. aritmetica.**
$$\frac{a_1 + a_2 + \cdots + a_n}{n} \tag{4}$$

Teorema 1 (Disuguaglianza AM-GM)**.** *Per qualunque $n > 0$, sia $a_1, a_2, \ldots, a_n$ una sequenza di numeri reali non-negativi. Si verifica che*

$$(a_1 a_2 \cdots a_n)^{1/n} \leq \frac{a_1 + a_2 + \cdots + a_n}{n} \ . \tag{5}$$

Dimostrazione. La dimostrazione è per induzione. Diamo il nome $P(n)$ all'affermazione che la disuguaglianza valga per sequenze di lunghezza n.

Adottiamo $n = 1$ come caso base e vediamo immediatamente che $P(1)$ è vera banalmente.

La cosa che distingue questa dimostrazione per induzione è che non faremo vedere come da $P(n)$ segua $P(n+1)$. Invece facciamo vedere come $P(n)$ implichi $P(2n)$. Fissiamo

$$X_g = (a_1 a_2 \cdots a_n)^{1/n} \qquad X_a = \frac{a_1 + a_2 + \ldots + a_n}{n} \ , \tag{6}$$

e

$$Y_g = (a_{n+1} a_{n+2} \cdots a_{2n})^{1/n} \qquad Y_a = \frac{a_{n+1} + a_{n+2} + \ldots + a_{2n}}{n} \ . \tag{7}$$

per l'ipotesi induttiva abbiamo che $X_g \leq X_a$ e che $Y_g \leq Y_a$. Abbiamo che

$$(a_1 a_2 \cdots a_n a_{n+1} a_{n+2} \cdots a_{2n})^{1/2n} = \sqrt{X_g Y_g} \leq \sqrt{X_a Y_a} \leq \frac{X_a + Y_a}{2} \ . \tag{8}$$

La prima disuguaglianza è dovuta al fatto che la radice quadrata è una funzione crescente, la seconda è l'applicazione della formula dimostrata prima. Visto che $\frac{X_a+Y_a}{2}$ è uguale a $\frac{1}{2n}\sum_{i=1}^{2n} a_i$, abbiamo dimostrato $P(2n)$.

A questo punto non abbiamo ancora dimostrato la disuguaglianza per tutti i valori di n, ma solo per $n = 1, 2, 4, 8, \ldots, 2^k, \ldots$

Ora vediamo come "riempire i buchi": per n che non è una potenza di due, fissiamo l'unico k per cui $2^{k-1} < n < 2^k$ e vediamo come $P(2^k)$ implichi $P(n)$.

Dati $a_1, \dots a_n$ definiamo $A = \frac{a_1 + \cdots + a_n}{n}$ e costruiamo una nuova sequenza $b_1, b_2, \dots b_{2^k}$ come segue:

- se $i \leq n$ allora $b_i = a_i$;
- altrimenti $b_i = A$.

Applichiamo l'ipotesi induttiva $P(2^k)$, ed otteniamo

$$\left(a_1 a_2 \cdots a_n \cdot A^{(2^k - n)}\right)^{1/2^k} \leq \frac{a_1 + a_2 + \cdots + a_n + (2^k - n)A}{2^k} = \frac{2^k A}{2^k} = A \; . \tag{9}$$

Manipoliamo le potenze di A e abbiamo

$$(a_1 a_2 \cdots a_n)^{1/2^k} \leq A \cdot A^{-(2^k - n)/2^k/} = A^{n/2^k} \; , \tag{10}$$

e elevando a potenza $2^k/n$ entrambi i lati otteniamo $P(n)$. □

Avete visto che questa induzione si è mossa in maniera non lineare, saltando avanti e indietro sui valori di n. Questo non è un problema: è sufficiente essere certi che ogni $P(n)$ venga verificato e che non si sia circolari nel ragionamento.