Induzione matematica

Informatica@SEFA 2017/2018 - Lezione 8

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

Mercoledì, 18 Ottobre 2017

> **Induzione** *[in-du-zió-ne]* s.f. Elaborazione logica con la quale dall'osservazione di un caso o di più casi particolari si ricavano i princìpi generali che ne sono alla base.

In matematica ed informatica è spesso necessario ragionare su strutture infinite o potenzialmente illimitate. Nel primo caso possiamo pensare all'espansione decimale di un numero in $\mathbb{R}$, mentre nel secondo caso possiamo pensare ai numeri naturali, dove ogni numero è finito ma esistono numeri di grandezza arbitraria.

É quindi necessario avere strumenti che permettano di dimostrare proprietà insiemi infiniti di oggetti. Uno strumento del genere è **l'induzione matematica.** Naturalmente l'induzione come metodo di ragionamento delle scienze naturali è un azzardo. Osservazioni successive potrebbero contraddire i principi generali elaborati. In matematica questo problema non esiste. L'induzione matematica è un processo **corretto** per definire/dimostrare.

Induzione matematica

L'induzione matematica è un metodo che permette di

- definire famiglie di oggetti
- dimostrare proprietà

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

Nella sua versione più semplice possiamo considerarla legata ai numeri naturali.

Definizioni per induzione

É possibile definire una famiglia di oggetti, limitati da un parametro, ed estendere la definizione a tutti i valori di quel parametro.

Esempio: consideriamo il valore numerico di una stringa di bit, ovvero una sequenza di zeri e uni. In sostanza definiamo una funzione

$$V : \{0,1\}^* \to \mathbb{N}.$$

in questo modo. Prima definiamo V sulle stringhe di dimensione zero,

- $V(\epsilon) = 0$

che V sia stata definita per le stringhe di dimensione n. In particolare se s è una stringa di $n+1$ simboli allora deve essere composta dalla concatenazione di una stringa s' di n simboli e una cifra che è o zero o uno (ed i due casi sono mutuamente esclusivi). Quindi definiamo $V(s)$ come

- $V(s'0) = 2V(s')$;
- $V(s'1) = 2V(s') + 1$.

La definizione di V è corretta, nel senso che V è definita per ogni stringa in $\{0,1\}^*$ e la definizione non è ambigua. Per assicurarsi che la definizione non sia ambigua, è necessario verificare che una stringa non cada in più casi simultaneamente, in modo tale che esista un'unica definizione applicabile. Ad esempio i tre casi di

- stringa vuota
- stringa che termina con zero
- stringa che termina con uno

sono **mutuamente esclusivi.**

Notazione: Dato un alfabeto Σ (generalmente un insieme finito di simboli) la notazione Σ^k indica tutte le sequenze (dette "parole") di lunghezza k ottenute concatenando simboli in Σ.

$$\Sigma^* = \bigcup_{k=0}^{\infty} \Sigma^k$$

$$\Sigma^+ = \bigcup_{k=1}^{\infty} \Sigma^k$$

Osservate che Σ^* contiene la stringa vuota, generalmente denotata con il simbolo ϵ (ma anche λ, dipende dal contesto).

Dimostrazione per induzione

La dimostrazione per induzione è un tipo di dimostrazione matematica il cui scopo (nella sua formulazione più semplice) è dimostrare che una certa proprietà P sia vera su tutti i numeri naturali.

$$P(n) \text{ per ogni } n \in \mathbb{N}$$

Per fare questo è sufficiente dimostrare due cose:

- (**Caso base**) che $P(0)$ è vera
- (**Passo induttivo**) che se $P(n-1)$ allora è (n) è vera, per $n > 0$ arbitrario.

Se questi due fatti sono veri allora abbiamo che

$$P(n) \text{ per ogni } n \in \mathbb{N}$$

è vero. Durante il passo induttivo l'ipotesi $P(n-1)$ è detta **ipotesi induttiva**. Facciamo un esempio, diciamo che vogliamo dimostrare il seguente fatto, riguardante i cosiddetti numeri **piramidali**.

Teorema 1. *Per ogni $n \geq 0$, la somma dei primi n quadrati è uguale a $\frac{n(n+1)(2n+1)}{6}$, ovvero*

$$\sum_{i=0}^{n} i^2 = \frac{n(n+1)(2n+1)}{6} . \tag{1}$$

Dimostrazione. quindi in questo caso $P(n)$ vuol dire: l'equazione (1) è vera per il valore n. Ad esempio $P(4)$ vuol dire: l'equazione

$$1 + 4 + 9 + 16 = 4 * 5 * 9/6$$

è vera. Dunque per dimostrare questo fatto per ogni $n \in \mathbb{N}$ possiamo applicare il "principio di induzione matematica". Per prima cosa si dimostra il caso base $P(0)$. Per $n = 0$ entrambi i lati dell'equazione (1) sono uguali a zero, pertanto l'equazione è verificata. Adesso per dimostrare il passo induttivo assumiamo che l'equazione sia verificata per $n-1$. Dunque possiamo scrivere $\sum_{i=0}^{n} i^2$ come

$$n^2 + \sum_{i=0}^{n-1} i^2 = n^2 + \frac{(n-1)n(2n-1)}{6} = \frac{n(n+1)(2n+1)}{6}$$

dove la prima uguaglianza è vera per l'ipotesi induttiva, e la seconda è un calcolo che potete verificare manualmente. □

Ma perché il principio di induzione è corretto? Lo possiamo dimostrare **per assurdo** ovvero ipotizzando che non lo sia e raggiungendo una contraddizione logica.

Teorema 2. *Se per una proprietà P vale*

- $P(0)$ *è vera,*
- *che se* $P(n-1)$ *allora è* $P(n)$ *è vera, per* $n > 0$ *arbitrario,*

allora la proprietà P è vera per ogni $n \in \mathbb{N}$.

Dimostrazione. Supponiamo che il caso base e passo induttivo valgano, ma che invece la proprietà P non sia vera per tutti i numeri naturali, allora vuol dire che esiste un numero h per cui la proprietà non vale. Di conseguenza esiste un numero m con $0 \leq m \leq h$ per cui la proprietà P non vale, e che sia il minimo per cui non valga.

Poiché $P(0)$ è vera, allora m deve essere più grande di 0, e perciò possiamo considerare $P(m-1)$. $P(m-1)$ deve essere vera perché m è il minimo numero per cui P è falsa. Ma visto che il passo induttivo è verificato, allora il fatto che $P(m-1)$ sia vera implica che lo è anche $P(m)$. Questo contraddice la scelta di m e l'ipotesi che esista un numero n per cui $P(n)$ sia falsa. □

Esercizio: dimostrare che per ogni stringa binaria $b_n b_{n-1} \ldots b_0$ vale che

$$V(b_n b_{n-1} \ldots b_0) = \sum_{i=0}^{n} b_i 2^i \ ,$$

utilizzando la tecnica dell'induzione matematica.

Esercizio: dimostrare che per ogni $n > 0$ il numero 5 divide $n^5 - n$.

Esempi classici di funzioni definite per induzione

Vengono dette (un po' impropriamente) **funzioni ricorsive**, quelle funzioni che per effettuare un calcolo richiamano loro stesse, possibilmente su input più piccoli. Un esempio molto classico di funzione il cui programma è scritto in questo modo è il calcolo del fattoriale. Il fattoriale di n è indicato come $n!$ ed è definition come

$$\prod_{k=1}^{n} k$$

con la convenzione che $0!$ sia uguale a 1. Calcoliamo il fattoriale con una funzione ricorsiva.

```
def fattoriale(n):
    if type(n) is not int or n<0:
        raise ValueError("Il parametro deve essere un num. naturale")

    if n==0:
        return 1
    else:
        return n * fattoriale(n-1)

print(fattoriale(0))
print(fattoriale(21))
```

```
1
51090942171709440000
```

Naturalmente per questi casi così semplici esiste una versione non ricorsiva abbastanza ovvia.

```
def fattoriale2(n):
    if type(n) is not int or n<0:
        raise ValueError("Il parametro deve essere un num. naturale")

    res = 1
    for k in range(1,n+1):
        res *= k

    return res

print(fattoriale2(0))
print(fattoriale2(21))
```

```
1
51090942171709440000
```

o addirittura ancora più compatta usando delle caratteristiche un po' più oscure del linguaggio Python.

```
from functools import reduce

def moltiplica(seq):
    '''Moltiplica gli elementi nella sequenza 'seq' '''
    return reduce(int.__mul__,seq,1)

def fattoriale3(n):
    if type(n) is not int or n<0:
        raise ValueError("Il parametro deve essere un num. naturale")

    return moltiplica( range(1,n+1) )

print(fattoriale3(0))
print(fattoriale3(21))
```

```
1
51090942171709440000
```

Varianti del principio di induzione

Consideriamo piccola variazioni del principio di induzione.

Induzione traslata

Questa è ottenuta spostando il caso base.

Variante traslata

- (**Caso base**) $P(n_0)$ è vera per un qualche $n_0 \in \mathbb{N}$;
- (**Passo induttivo**) se $P(n-1)$ allora è (n) è vera, per $n > 0$ arbitrario.

in questo caso otteniamo che $P(n)$ è vera per ogni $n \geq n_0$. Nell'esercizio seguente ha senso avere il caso base per $n = 1$.

Esercizio (numeri triangolari): dimostrare che per ogni $n \geq 1$,

$$\frac{n(n+1)}{2} = \sum_{i=1}^{n} i \,,$$

Esercizio: dimostrare questa variante traslata del principio di induzione a partire dal principio di induzione standard.

Induzione e forte

Un'altra variante è il cosiddetto principio di **induzione forte** dove l'ipotesi induttivo riguarda tutti i casi precedenti. Le due ipotesi sono:

- (**Caso base**) $P(0)$ è vera;
- (**Passo induttivo**) se $P(k)$ è vera per $k < n$ allora è $P(n)$ è vera, per $n > 0$ arbitrario.

La conclusione è di nuovo che $P(n)$ è vera per $n \in \mathbb{N}$.

Esercizio dimostrare che il principio di induzione forte a partire dal principio di induzione standard.

Esercizi

Dimostrare le seguenti affermazioni:

1. se $x > -1$ allora $(1+x)^n > 1 + nx$;
2. $n^2 > 2n + 1$ per $n \geq 3$;
3. ogni insieme di n elementi ha 2^n sottoinsiemi;
4. $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + a^2b^{n-3} + ab^{n-2} + b^{n-1})$ da cui segue che
$$\sum_{k=0}^{n} q^k = \frac{1-q^{n+1}}{1-q}$$
per ogni $q \neq 1$. Da cui peraltro segue che per $|q| < 1$
$$\lim_{n\to\infty} \sum_{k=0}^{n} q^k = \frac{1}{1-q} \; ;$$
5. $n! > 2^{n-1}$

Principio di buon ordinamento

Quando ho dimostrato il Teorema 2 ho fatto un po' il furbo. Ho utilizzato la seguente affermazione, detta **principio del buon ordinamento**

> Ogni insieme non vuoto di numeri naturali ha un elemento minimo.

Questo non è vero se si considerano i numeri interi $\mathbb{Z}$ o i numeri reali $\mathbb{R}$. La ragione per cui questa è una furbizia è che il principio di induzione e quello del buon ordinamento sono equivalenti.

Esercizio guidato: dimostrare il principio di buon ordinamento a partire dall principio di induzione. Per farlo va ovviamente impostata una proprietà $P(n)$. Allora consideriamo un insieme $I \subseteq \mathbb{N}$ che non ha un elemento minimo. Dimostreremo che questo insieme è vuoto. La proprietà $P(n)$ è che I non contiene numeri $\leq n$. Se dimostriamo che $P(n)$ è vera per ogni $n \in \mathbb{N}$ allora I è l'insieme vuoto.

- (Caso base) Se 0 fosse in I allora ne sarebbe il minimo.
- (Passo induttivo) Se $P(n-1)$ allora I non contiene numeri minori di n, quindi I contenesse n, questo ne sarebbe il minimo. Perciò I non contiene né n né numeri $< n$, e quindi $P(n)$ è vera.

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, 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 $I = A \cup B$.

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 $P(2)$, cioè che se tutti gli insiemi di un cavallo sono monocromatici, allora anche gli insiemi di due cavalli lo sono. 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 del cavallo residuo in A e quello in B.