Logica e Reti Logiche

Episodio 0: Dimostrazioni per assurdo e per induzione

Francesco Pasquale

11 marzo 2021

In questo episodio ricordiamo due tecniche di dimostrazione fondamentali, che vi troverete spesso ad utilizzare nel vostro percorso di studi in informatica: le dimostrazioni *per assurdo* e le dimostrazioni *per induzione*.

1 Dimostrazioni per assurdo

In una dimostrazione per assurdo, per dimostrare una certa affermazione P, si assume che sia vera la sua negazione $\sim P$ e si cerca di giungere a un "assurdo". L'assurdo può essere di vari tipi: per esempio, assumendo che $\sim P$ sia *vera* potremmo

1. Riuscire a dimostrare che $\sim P$ deve essere anche *falsa*;
2. Trovare un'affermazione Q che risulta sia vera che falsa;
3. Trovare un'affermazione Q non può essere né vera né falsa;
4. ...

Esempio: Il teorema di Cantor. Abbiamo visto come sia possibile mettere in corrispondenza biunivoca l'insieme dei numeri naturali $\mathbb{N}$ con alcuni insiemi che all'apparenza potrebbero sembrare "più grandi" o "più piccoli" di $\mathbb{N}$. Per esempio, la funzione $f : \mathbb{N} \to \{\text{numeri pari}\}$ definita da $f(n) = 2n$ è una funzione biunivoca fra l'insieme di tutti i numeri naturali e l'insieme dei numeri pari. Quindi, mentre è vero che l'insieme dei numeri pari è un sottoinsieme *proprio* di $\mathbb{N}$, non è vero che l'insieme dei numeri pari contiene "meno elementi" di quanti ne contiene tutto $\mathbb{N}$. Entrambi contengono un numero infinito di elementi, e gli infiniti sono dello stesso ordine.

Allo stesso modo non è difficile trovare delle corrispondenze biunivoche fra $\mathbb{N}$ e

1. L'insieme di tutti i numeri interi $\mathbb{Z}$ (positivi, negativi e lo zero);
2. L'insieme di tutte le coppie ordinate di numeri interi;
3. L'insieme di tutti i sottoinsiemi finiti di $\mathbb{N}$;
4. ...

Ma se proviamo a cercare una corrispondenza biunivoca fra $\mathbb{N}$ e l'insieme di tutti i sottoinsiemi di $\mathbb{N}$ (finiti e infiniti) non ci riusciamo. Il motivo per cui non ci riusciamo è che una tale corrispondenza non esiste.

Teorema 1.1 (Cantor)**.** Non esiste una funzione biunivoca fra $\mathbb{N}$ e $\mathcal{P}(\mathbb{N})$.

Dimostrazione. Supponiamo "per assurdo" che esista una tale funzione biunivoca, che ad ogni numero naurale $n \in \mathbb{N}$ associa un sottoinsieme $A_n \subseteq \mathbb{N}$. In particolare avemmo che per ogni sottoinsieme S di $\mathbb{N}$ deve esistere un numero naturale n tale che $A_n = S$ (perché la funzione è *suriettiva*).

Osservate che per ogni numero naturale n, siccome A_n è un sottoinsieme di numeri naturali, A_n può contenere oppure non contenere n stesso. Consideriamo allora l'insieme S di tutti i numeri naturali n tali che n non appartiene ad A_n,

$$S = \{n \in \mathbb{N} : n \notin A_n\} \tag{1}$$

Siccome S è un sottoinsieme di $\mathbb{N}$, allora dovrebbe esistere un numero k tale $S = A_k$. A questo punto chiediamoci se k appartiene o no a S.

Se $k \notin S$ allora $k \notin A_k$ *[perchè $S = A_k$]*. Ma se $k \notin A_k$ allora $k \in S$ *[per la definizione di S in (1)]*. Quindi k deve appartenere ad S. Ma se $k \in S$ allora $k \in A_k$ *[perchè $S = A_k$]* e quindi $k \notin S$ *[per la definizione di S]*. $\square$

Ora è il turno vostro di fare un po' di lavoro.

Esercizio 1. Dimostrare che i numeri primi sono infiniti.
(Suggerimento: Supponete per assurdo che siano finiti. Siano quindi $p_1, p_2, \ldots, p_n$ tutti i numeri primi. Considerate allora il prodotto di tutti i numeri primi e aggiungete uno: $p_1 p_2 \cdots p_n + 1$. Riuscite a trovare una qualche contraddizione su questo numero?)

Esercizio 2. Dimostrare che $\sqrt{2}$ non è un numero razionale.
(Suggerimento: Supponete per assurdo che si possa scrivere $\sqrt{2} = a/b$ con $a, b \in \mathbb{N}$ e fate vedere che allora a e b devono essere entrambi pari. Quindi...)

2 Dimostrazioni per induzione

Considerate l'affermazione seguente: $n^2 + 3n + 5$ è dispari, per ogni $n \geqslant 0$. Osservate che in realtà si tratta di una *infinità* di affermazioni, una per ogni valore di n. Possiamo verificare a mano che, per esempio, per $n = 0, 1, 2, 3$ il valore della formula è rispettivamente $5, 9, 15, 23$. Ma se vogliamo dimostrare che il valore di quella formula è *sempre* un numero dispari, non possiamo certo fare infinite verifiche...

Dimostrazioni per induzione (Versione I). Sia b un numero intero e sia $P(n)$ un enunciato definito per ogni $n \geqslant b$. Per dimostrare "per induzione" che $P(n)$ è vero per ogni $n \geqslant b$, si procede in due passi:

1. Si verifica che $P(b)$ è vero;
2. Si dimostra che, dato un qualunque $n \geqslant b$, se $P(n)$ è vero allora anche $P(n+1)$ è vero.

Il punto 1 si chiama *base* dell'induzione. Il punto 2 si chiama *passo induttivo*. All'interno del punto 2, l'ipotesi che $P(n)$ sia vero si chiama *ipotesi induttiva*.

Esempio. Sia $\alpha \in \mathbb{R}$ un qualunque numero reale. Dimostriamo per induzione che per ogni $n \geqslant 0$

$$(1-\alpha)\sum_{i=0}^{n} \alpha^i = 1 - \alpha^{n+1}$$

Osserviamo che il nostro enunciato qui è $P(n)$: " $(1-\alpha)\sum_{i=0}^{n} \alpha^i = 1 - \alpha^{n+1}$ " ed è definito per ogni $n \geqslant 0$.

Base dell'induzione. Verifichiamo $P(0) : (1-\alpha)\sum_{i=0}^{0} \alpha^i = 1 - \alpha^{0+1}$. Vero, perché sia l'espressione a sinistra dell'uguale che quella a destra valgono $1 - \alpha$.

Passo induttivo. Dato un qualunque $n \geqslant 0$, supponiamo che $P(n)$ è vero (ossia, supponiamo che $(1-\alpha)\sum_{i=0}^{n} \alpha^i = 1-\alpha^{n+1}$) e dimostriamo che $P(n+1)$ è vero; ossia, dobbiamo dimostrare che

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

Scriviamo l'espressione a sinistra dell'uguale:

$$(1-\alpha)\sum_{i=0}^{n+1} \alpha^i \tag{3}$$

Possiamo spezzare la sommatoria in (3) nei primi n termini più l'ultimo termine

$$\begin{aligned} (1-\alpha)\sum_{i=0}^{n+1} \alpha^i &= (1-\alpha)\left[\left(\sum_{i=0}^{n} \alpha^i\right) + \alpha^{n+1}\right] \\ &= (1-\alpha)\left(\sum_{i=0}^{n} \alpha^i\right) + (1-\alpha)\alpha^{n+1} \end{aligned} \tag{4}$$

Per l'ipotesi induttiva, $(1-\alpha)\left(\sum_{i=0}^{n} \alpha^i\right) = 1-\alpha^{n+1}$, quindi possiamo riscrivere l'ultimo termine nella (4) in questo modo

$$\begin{aligned} (1-\alpha)\left(\sum_{i=0}^{n} \alpha^i\right) + (1-\alpha)\alpha^{n+1} &= 1-\alpha^{n+1} + (1-\alpha)\alpha^{n+1} \\ &= 1-\alpha^{n+1} + \alpha^{n+1} - \alpha^{n+2} = 1-\alpha^{n+2} \end{aligned} \tag{5}$$

Mettendo insieme la (4) e la (5) abbiamo che

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

che è proprio la (2). Quindi abbiamo dimostrato che $P(n+1)$ è vero. $\square$

Esercizio 3. Dimostrare per induzione che

1. Per ogni $n \geqslant 1$,
$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2} \quad \text{e} \quad \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$$

2. Per ogni $n \geqslant 1$, $n^3 - n$ è divisibile per 3

3. Per ogni $n \geqslant 5$, $2^n > n^2$.

Esercizio 4. Trovare una formula chiusa per $\sum_{k=1}^{n}(k+3)^2$.

Esercizio 5. Considerate la seguente ricorrenza

$$\begin{cases} a_1 &= 1 \\ a_{n+1} &= 2a_n + 1, \quad \text{per ogni } n \geqslant 1 \end{cases}$$

Trovare una formula chiusa per a_n e dimostrare per induzione che è corretta.

Dimostrazioni per induzione (Versione II). Sia b un numero intero, sia $P(n)$ un enunciato definito per ogni $n \geqslant b$ e sia c un numero intero maggiore o uguale a b. Per dimostrare "per induzione" che $P(n)$ è vero per ogni $n \geqslant b$, si procede in due passi:

1. Si verifica che $P(k)$ è vero per ogni k tale che $b \leqslant k \leqslant c$;

2. Si dimostra che, dato un qualunque $n \geqslant c$, se $P(k)$ è vero per ogni $b \leqslant k \leqslant n$ allora anche $P(n+1)$ è vero.

Il punto 1 si chiama *base* dell'induzione. Il punto 2 si chiama *passo induttivo*. All'interno del punto 2, l'ipotesi che $P(k)$ sia vero per ogni $b \leqslant k \leqslant n$ si chiama *ipotesi induttiva*.

Esercizio 6. Considerate la seguente ricorrenza

$$\begin{cases} a_1 &= 1 \\ a_2 &= 2 \\ a_3 &= 3 \\ a_n &= a_{n-1} + a_{n-2} + a_{n-3} \quad \text{per ogni } n \geqslant 4 \end{cases}$$

Dimostrare per induzione che $a_n \leqslant 2^n$ per ogni $n \geqslant 1$.

Esercizio 7. Considerate il seguente algoritmo[1]

Algorithm 1 `Eu`(n, m)

```
if m = 0 then
    return n
return Eu(m, n mod m)
```

1. Che cosa restituisce `Eu`$(15, 9)$? e `Eu`$(9, 15)$?

2. In generale cosa restituisce `Eu`(n,m) quando n e m sono due interi positivi? Riuscite a dimostrarlo per induzione?

3. Implementate l'algoritmo in un linguaggio di programmazione a piacere.

[1] Con $n \bmod m$ si intende il resto della divisione di n per m. Per esempio, $10 \bmod 3 = 1$, $15 \bmod 5 = 0$