Logica e Reti Logiche

Episodio 2

Richiami di Matematica: dimostrazioni per induzione

Francesco Pasquale

10 ottobre 2024

Nell'episodio precedente abbiamo richiamato le dimostrazioni *per assurdo*. In questo episodio parliamo di un'altra tecnica di dimostrazione molto usata in ambito informatico: *l'induzione matematica*.

1 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. **Base dell'induzione**: Si verifica che $P(b)$ è vero;
2. **Passo induttivo**: Si dimostra che, dato un qualunque $k \geqslant b$, se $P(k)$ è vero allora anche $P(k+1)$ è vero.

Nel passo induttivo, $P(k)$ si chiama **ipotesi induttiva**, $P(k+1)$ si chiama **tesi induttiva**.

Per dimostrare per induzione che una proprietà $P(n)$ è vera per ogni $n \geqslant b$

$P(b)$ ———

$P(b+1)$ ———

$P(b+2)$ ———

$\vdots$

$P(n)$ ———

$\vdots$

Si verifica che è vera la prima

(1) $P(b)$ ———

E si dimostra che dato un k qualunque, se è vera per k allora è vera anche per $k+1$

(2) $P(k)$ ———

$P(k+1)$ ———

Esercizio 1. Riflettere con attenzione sul perché i due passaggi qui sopra garantiscono che la proprietà P è vera per ogni $n \geqslant b$.

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 $k \geqslant 0$, dimostriamo che se $P(k)$ è vero allora anche $P(k+1)$ deve essere vero. Riscriviamoci prima di tutto chi sono $P(k)$ e $P(k+1)$,

$$P(k) : \quad (1-\alpha)\sum_{i=0}^{k} \alpha^i = 1 - \alpha^{k+1} \tag{1}$$

$$P(k+1) : \quad (1-\alpha)\sum_{i=0}^{k+1} \alpha^i = 1 - \alpha^{k+2} \tag{2}$$

?

Quindi dobbiamo dimostrare che, dato un qualunque $k \geqslant 0$, se è vera la (1) (la nostra *ipotesi induttiva*) allora è vera anche la (2) (la nostra *tesi induttiva*).

Ci sono naturalmente diversi modi in cui si potrebbe procedere. Un modo è il seguente. Nella (2) scriviamo l'espressione a sinistra dell'uguale:

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

Osserviamo che possiamo spezzare la sommatoria in (3) nei primi k termini più l'ultimo termine

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

PK

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

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

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

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

che è proprio la (2). Quindi abbiamo dimostrato che se $P(k)$ è vero allora anche $P(k+1)$ deve essere vero. □

Esercizio 2. Ora dimostrate per induzione che $n^2 + 3n + 5$ è dispari, per ogni $n \geqslant 0$

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.

In alcuni casi risulta difficile fare il passo induttivo assumendo come ipotesi induttiva soltanto $P(k)$.

Esercizio 6. Considerate la seguente ricorrenza
$$\begin{cases} a_1 & = & 1 \\ a_2 & = & 2 \\ a_3 & = & 3 \\ a_n & = & a_{n-1} + a_{n-2} + a_{n-3} \quad \text{per ogni } n \geqslant 4 \end{cases}$$
Provare a dimostrare per induzione che $a_n \leqslant 2^n$ per ogni $n \geqslant 1$.

Il principio di induzione può essere riformulato in un modo che risulti di più facile applicazione in alcuni casi.

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. **Base dell'induzione**: Si verifica che $P(h)$ è vero per ogni h tale che $b \leqslant h \leqslant c$;
2. **Passo induttivo**: Si dimostra che, dato un qualunque $k \geqslant c$, se $P(h)$ è vero per ogni h tale che $b \leqslant h \leqslant k$, allora anche $P(k+1)$ è vero.

Nel passo induttivo, $\{P(b), P(b+1), \ldots, P(k)\}$ è l'**ipotesi induttiva**, $P(k+1)$ è la **tesi induttiva**.

Esercizio 7. Riflettere con attenzione sul perché i due passaggi qui sopra garantiscono che la proprietà P è vera per ogni $n \geqslant b$.

Esercizio 8. Provate a risolvere l'Esercizio 6 usando quest'altra versione dello schema di dimostrazione per induzione.

Esercizio 9. 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 mod m si intende il resto della divisione di n per m. Per esempio, $10 \bmod 3 = 1$, $15 \bmod 5 = 0$