

DIMOSTRAZIONI >

TIPOLOGIE >

Le tipologie di dimostrazione possono essere:

DIRETTA > $p_1, p_2, p_n \vdash t_1, t_2, t_3$

Si calcola dalla semplice congiunzione logica applicando: Ipotesi, Assiomi per poter verificare la Tesi.

ESEMPIO: " $\forall m \forall n (2|m \wedge 2|n \Rightarrow 2|(m+n))$ " Per ogni m, n , se m è pari ed n è dispari allora $m+n$ è dispari.Se m è pari, allora è nella forma

$$m = 2 \cdot r \text{ per } r \in \mathbb{Z}$$

analogamente per n :

$$n = 2 \cdot q + 1 \text{ per } q \in \mathbb{Z} \quad \text{per cui } m+n = \overbrace{(2 \cdot r)}^{\substack{m \\ \in \mathbb{Z}}} + \overbrace{(2 \cdot q+1)}^{n} = z(r+q)+1$$

\Rightarrow
è nella forma $\underbrace{z \cdot a + 1}_{\in \mathbb{Z}}$ per cui è un num. disp.

ESEMPIO 2: "Per tutti gli insiemi X, Y, Z : $X \cap (Y - Z) = (X \cap Y) - (X \cap Z)$ "

$$X \cap (Y - Z) = \{a \in X \mid a \in Y \wedge a \notin Z\} \quad \text{per def}$$

$$(X \cap Y) - (X \cap Z) = \{a \in X \mid a \in Y \wedge a \notin Z\} \quad \text{per def}$$

I due insiemi per definizione sono equivalenti per cui:
 $a \in X \cap (Y - Z) \Leftrightarrow a \in (X \cap Y) - (X \cap Z)$ per qualche a

Dimostrazioni >

Tipologie >

$$P \wedge Q \rightarrow P \wedge Q$$

ASSURDO >

$$P_0, P_1, \dots \models Q \rightarrow P_0, P_1, \dots \models \neg Q$$

Le dimostrazioni per
di negare le Teesi e prove che provate che appunto l'ipotesi
contraddizioni.

Esse sono delle teorie del tipo $P \wedge \neg P$, dalle quali si
conclude che se $P_0, P_1, \dots, P_n \models \neg Q$ è falso, allora $P_0, P_1, \dots, P_n \models Q$
è vero.

ESEMPIO: "Dimostrare che per ogni $n \in \mathbb{Z}$, se n^2 è pari, allora n è pari"

Tradotta in $\forall n \in \mathbb{Z} (n^2 \models \text{pari})$ ovvero $\text{Ipotesi} = n^2 \models \text{pari}$

Supponendo per assurdo $\neg Q$, $Q \Rightarrow \text{Teesi} = n \text{ pari}$

si dimostra che $P \models \neg Q$:

Se n è pari, allora è nella forma $2k+1$: $n = 2k+1$ per $k \in \mathbb{Z}$
per ipotesi n^2 deve essere divisibile per 2:

$$2 | (2k+1)^2 \Rightarrow 2 | 4k^2 + 4k + 1 \Rightarrow 2 | \underbrace{4k^2 + 4k}_{\text{pari}} + 1$$

↓
G2

In maniera analoga, se n è pari
e si vuole dimostrare che n^2 è pari

$n = 2k$ per $k \in \mathbb{Z}$

$$n^2 = (2k)^2 \Rightarrow 4k^2 + \cancel{4k} + \cancel{4k} + 1$$

che come prima non è div. per 2

Ne consegue che se $P \models \neg Q$ è falso, allora $P \models Q$
ovvero che se n^2 è pari, necessariamente deve essere divisibile

ESEMPIO 2: "Dimostrare che $\sqrt{2}$ è irrazionale"

un num è irrazionale se non è rappresentabile nella forma $\frac{p}{q}$ con $p, q \in \mathbb{Z}$
quindi $\sqrt{2} \notin \mathbb{Q}$. $\models Q \Rightarrow \sqrt{2} \notin \mathbb{Q}$

Supponendo per assurdo $\neg Q$ ovvero che $\sqrt{2}$ sia nella forma $\frac{p}{q}$, allora
dovebbero esistere dei primi p_1, p_2, \dots, p_n t.c. $\frac{p_1 \cdot p_2 \cdots p_n}{q_1 \cdot q_2 \cdots q_n} = \sqrt{2}$ ma

$$\sqrt{\frac{n}{m}} = \sqrt{2} \Rightarrow n = m\sqrt{2} \quad n^2 = m^2$$

Quindi $2 | n^2 \wedge 2 | m^2$

questo però vuol dire che
non sono primi! contraddizione.

DIMOSTRAZIONI >

TIPOLOGIE >

CONTRAPPOSIZIONE > $\neg Q \vdash \neg P$

Le dimostrazioni per contrapposizione prevedono di invertire ipotesi e Tesi e di negare entrambe. Se si è in grado di provare la congiuntione logica, allora il Teorema iniziale sarà valido.

ESEMPIO: "Per tutti i numeri reali x e y , se $x+y \geq 2$ allora $x \geq 1 \vee y \geq 1$ "

$$\text{avero } \forall x \forall y (P(x,y) \vdash Q(x,y)) \quad P(x,y) = x+y \geq 2 \\ Q(x,y) = x \geq 1 \vee y \geq 1$$

Si procede a dim. per contrapposizione

$$\text{da } \neg Q \vdash \neg P \text{ ovvero } \vdash \neg Q \rightarrow \neg P \quad \neg P(x,y) = \neg(x+y \geq 2) \\ = x+y < 2$$

Ipotesi $\neg Q(x,y)$ per $x, y \in \mathbb{R}$

$$\text{Tesi: } \neg P(x,y) \quad \equiv \quad \neg Q(x,y) = x < 1 \wedge y < 1$$

Se $x < 1$ e $y < 1$ allora, $x+y < 1+1$

$$\downarrow x+y < 2 \text{ ovvero } \neg Q$$

analogamente con Ipotesi $\neg P$ c'è tesi $\neg Q$:

se $x+y \geq 2$ allora $x \geq 1 \wedge y \geq 1$

DIMOSTRAZIONI >

TIPOLOGIE >

PER CASI: $P_1 \vee P_2 \dots \vee P_n \models Q \equiv P_1 \models Q \wedge P_2 \models Q \wedge \dots \wedge P_n \models Q$

La dimostrazione per casi viene utilizzata quando si hanno più ipotesi in disegnazione.

È possibile semplificare la dimostrazione, provando che le singole ipotesi conducano alla Tesi.

ESEMPIO: "Dimostrare che l'equazione $2m^2 + 3n^2 = 40$ non ha soluzioni"

Ciò è equivalente a dire di dimostrare che $2m^2 + 3n^2 \neq 40$.

di conseguenza si montano

dei casi di risoluzione

		m	
		1	2
n	1	5	11
	2	14	20
3	29	35	45
			59

$$\frac{3n^2}{2} \neq \frac{40}{3}$$

$$\frac{2m^2}{2} \neq \frac{40}{2}$$

$$m^2 \neq 20$$

$$n^2 > 14$$

$$n > 4$$

per dimostrare che non è così.

ESEMPIO 2: "Dimostrare che, per ogni numero reale x , $x \leq |x|$ "

$$\text{Si sa che } |x| = \begin{cases} x & x \geq 0 \\ -x & x < 0 \end{cases}$$

Si montano di conseguenza i casi:

$$P_1 = x \geq 0 \quad P_2 = x < 0 \quad Q = x \leq |x|$$

$$\models P_1 \rightarrow Q$$

$$\models P_2 \rightarrow Q$$

Nel caso in cui $x \geq 0$, allora $x \leq |x|$
 $x \leq x$ è certa

Nel caso in cui $x < 0$, se $x \leq |x| \equiv x \leq -x$ per def $|x|$

PER PROVE DI EQUIVALENZA

che è verificata

È possibile usare le prove di equivalenza per poter dimostrare le bi-implicazioni $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$

ESEMPIO: "Per ogni intero n , se n è dispari, allora $n-1$ è pari"

$$p: \text{se } n \text{ è disp} \equiv z \mid n$$

$$q: n-1 \text{ è pari} \equiv z \mid n-1$$

$$\text{Caso 1: } q \rightarrow p$$

se $z \mid n-1$ allora

$$n-1 = 2k \text{ per cui}$$

$$n = 2k+1 \models 2 \mid 2k+1$$

Verificata

$$\text{Caso 2: } p \rightarrow q$$

se n è disp allora è nella

$$\text{forma } n = 2k+1. \text{ Allora}$$

$$n-1 = 2k+1-1 \text{ ovvero } 2k$$

che è divisibile per 2.

PROVE COSTRUTTIVE >

Data una dimostrazione, se essa esibisce un elemento a del Dominio del discorso per il quale $P(a)$ è vera, allora è una **prova costrettiva**.

In alternativa, viene detta **prova non costrettiva**.

NUM. PRIMI DI MARSENNE >

Essi sono una sequenza di primi generati da altri numeri primi nella forma $2^n - 1$

PROVE DI RISOLUZIONE >

Per prova di risoluzione si intendono delle tecniche risolutive applicate alle clausole (scritte nelle ipotesi e conclusioni).

CLAUSOLA > $p \vee q$

Per clausole si intende una serie di termini separati da OR.

BASI DELLA RISOLUZIONE > $(p \vee q) \wedge (\neg p \vee r) \models q \vee r$

Esse si basano sull'idea che, date 3 proposizioni p, q, r se $p \vee q$ e $\neg p \vee r$ sono entrambe vere, allora è $q \vee r$.

In poche parole, si semplifica la proposizione che oppure sia negata che non.

ESEMPPIO: "Prove che $a \vee b, \neg a \vee c, \neg c \vee d \models b \vee d$ "

semplificabile in $b \vee c, \neg c \vee d$ che è semplificabile in $b \vee d$: Dimostriamo per risoluzione.

a	b	c	d	$a \vee b$	$\neg c \vee d$	$\neg a \vee c$	$b \vee d$
0	0	0	0	0	1	1	0
0	0	0	1	0	0	1	1
0	0	1	0	1	1	1	0
0	0	1	1	1	0	1	1
0	1	0	0	1	1	1	1
0	1	0	1	1	1	1	1
0	1	1	0	1	0	1	1
0	1	1	1	1	1	1	1
1	0	0	0	1	1	0	0
1	0	0	1	1	0	1	1
1	0	1	0	1	1	1	1
1	0	1	1	1	1	1	1
1	1	0	0	1	1	0	1
1	1	0	1	1	1	1	1
1	1	1	0	1	0	1	1
1	1	1	1	1	1	1	1

→ 01

PRINCIPIO DI INDUZIONE >

Il principio di induzione è un principio che viene applicato sugli insiemi enumerabili, ovvero degli insiemi infiniti contabili o in bizione con \mathbb{N} .

Il PREDICATO > $P(n)$

In particolare, viene definito un predicato contenente la proprietà che si vuole dimostrare.

Il parametro rappresenta la posizione dell'insieme enumerabile in cui si vuole che la proprietà sia vera.

LA COMPOSIZIONE >

Una volta definito il predicato, bisognerà dimostrare che esso vale:

- Per $P(0)$
 - Per $P(n+1)$
- Per $n \geq 0$. In alternativa
si può vedere al contrario

Allora la dimostrazione verrà composta e sarà applicabile a tutti gli elementi dell'insieme enumerabile.

ESEMPIO > Dimostrare che la somma da 1 a n è equivalente a $\frac{n \cdot (n+1)}{2}$ per $n \geq 1$

La traccia chiede che $\sum_{i=1}^n i = \frac{n \cdot (n+1)}{2} \quad \forall n \geq 1 \in \mathbb{N}$

$$P(x) : \sum_{i=1}^n i = \frac{n \cdot (n+1)}{2}$$

CASO $P(1)$ BASE: $\sum_{i=1}^1 i = \frac{1 \cdot (1+1)}{2} \Rightarrow 1 = \frac{2}{2}$

IPOTESI ($P(n)$)

$$\text{CASO } P(n+1) : \sum_{i=1}^{n+1} i = (n+1) \cdot \frac{(n+1)+1}{2}$$

$$= \frac{n^2 + 2n + n + 2}{2} = \frac{n^2 + 3n + 2}{2}$$

Ovvero

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

$$= \frac{n \cdot (n+1) + 2(n+1)}{2} \Rightarrow \frac{(n+2)(n+1)}{2}$$

Verificata

Verificata

È quindi dimostrato che se $P(1)$, allora $P(n+1)$ è vero

2.00P INVARIANT >

Per 'loop invariant' si intende un metodo di dimostrazione che si serve delle tecniche di induzione per poter verificare la correttezza di un ciclo o ricorsione.

2.1. PER CICLI >

L'Invariante per i cicli viene definita a partire da 2 proposizioni:

- $P = \text{2° Inv. di ciclo}$ ovvero la cond. di correttezza.
- $B = \text{la condizione}$, che viene verificata ad ogni ciclo

P
 $\text{while } (B) \{$
 $P \wedge B$
 $\dots P$
 $\} P \wedge B$

ESEMPIO >

Dimostrare con loop invariant che il seguente calcolo è corretto:

$i=1;$

$\text{fact} \Rightarrow 1$

$\text{while } (i < n) \{$

$i=i+1$

$\text{fact} = \text{fact} \cdot i$

i

ovvero de a fine

esecuzione $\text{fact} = n!$

$$\text{Def: } n! = \begin{cases} 1 & \text{se } n=0 \\ n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1 & \text{se } n \geq 1 \\ \text{oppure } 1 \cdot 2 \cdot \dots \cdot (n-2) \cdot (n-1) \cdot n & \end{cases}$$

Definendo come $B \Rightarrow i < n$ e $P = \text{fact}$

CASO BASE: $n=0$: $\text{fact} = 1$ valido

CASO INDUCTIVO $P(n)$:

$$i' = i+1, \text{ fact}' = \text{fact} \cdot i'$$

$$= \text{Fact}(i+1) \equiv \frac{1 \cdot 2 \cdot (n-2) \cdot (n-1) \cdot n}{n!}$$

CONDIZIONE DI TERMINAZIONE ➤

Una volta dimostrata la correttezza di un programma tramite la loop invariant, per completare la dimostrazione bisogna dimostrare che il programma termina.

All'interno del loop si sfrutta la condizione degli insiemi ben ordinati:

Ovvero che dopo n cicli il contatore che va fino a n può essere rappresentato così

$i = 0, 1, \dots, n, (n-1), (n-2) \dots (n-n) \Rightarrow$ Ovvero ha un minimo e dovrà terminare.

INSIEMI BEN ORDINATI ➤ $I = \{i \mid i \geq 0 \in \mathbb{Z}\} = \exists \min$

Il teorema degli insiemi ben ordinati dice che dato un insieme di numeri naturali ≥ 0 allora deve esistere un minimo.

DIVISIONE CON RESTO ➤ $\forall n \in \mathbb{N} (\forall d > 0 \exists q \exists r \text{ con } r < d \wedge n = q \cdot d + r)$

Dato un num $n \in \mathbb{Z}$ e un divisore $d \in \mathbb{N}$, allora $d|n$ è rappresentabile con la divisione euclidea nella forma: $n = q \cdot d + r$

In cui sarà presente un resto ≥ 0 che è strettamente minore del divisore.

DIMOSTRAZIONE ➤

Definendo l'insieme X formato dai possibili resti $X = \{n - (q \cdot d) \mid n, q, d \in \mathbb{Z}\}$

- se $n=0 \rightarrow 0 - (q \cdot d) = -q \cdot d$ ovvero $x \neq 0$

- se $n \geq 0 \wedge q=0 \rightarrow n \in X$ ovvero $x \neq 0$

- Se $n < 0 \rightarrow$ deve esistere tale che $n - q \cdot d \geq 0$
per es. con $q=n$ allora $n - (n \cdot d) \geq 0$

tutto questo per dim.
che c'è almeno un resto ≤ 0
ovvero $x \neq 0$

Siccome gli elementi di X per il Teorema del buon ordinamento sono ≤ 0 e $x \neq 0$ allora esiste un minimo. $m = n - q \cdot d \rightarrow n = m + q \cdot d$

resto

È anche il minimo in quanto se non lo fosse allora ^{non} $\forall r \in X$ esisterebbe un altro.

INDUZIONE FORTE >

L'induzione forte è una variante dell'induzione. Il cambio fondamentale avviene nel passo induutivo, nel quale come ipotesi si ipotizza oltre a $P(n)$, anche tutti gli elementi da $0..n$.

ESEMPIO > "Dati una serie di n numeri, si pongono delle parentesi in delle posizioni arbitrarie sul loro prodotto.

Dimostrare che, indipendentemente da dove vengono messe le parentesi, il numero di prodotti sarà $n-1$

Es: con $n=4 \quad (a_1 \cdot a_2) \cdot (a_3 \cdot a_4) \quad 3$ prodotti"

Dim su n :

CASO BASE $n=1$: con 1 num. si hanno 0 moltiplicazioni ovvero $n-1$. Verificata.

CASO INDUTTIVO: Ipotesi: $P(1), P(2) \dots P(n)$

Tesi: $P(n+1)$

Supponendo di rappresentare il prodotto $(a_1 \dots a_{n+1}) = (a_1 a_2 \dots a_n) \cdot a_{n+1}$ con $\leq n+1$ scegliendo delle parentesi ad un determinato K arbitrario

Per ipotesi induuttiva si sa che il prodotto da $\leq K$ è $K-1$,

da $K+1$ ad $n+1$ è $n+1-K+1 = n-K$

Mettendole insieme: $(K-1) + (n-K) + 1 = n$ Verificata

ESEMPIO 2 > "Dati dei francobolli da 2 cent e da 5 cent allora dimostrare che è possibile affrancare un num. $n \geq 4$ di cent in Francobolli."

CASO BASE $P(1)$: 2 Francobolli da 2=4 Verificata

$$P(1) \leq 2 \geq 4 \quad \checkmark$$

$$P(2) \quad 3 \cdot 2 \quad \checkmark$$

$$P(3) \quad 5 + 2 \quad \checkmark$$

$$P(4) \quad 2 \cdot 4$$

CASO INDUTTIVO: Dato $P(k)$ e $P(k), P(k)$, Tesi $P(k+1)$

Per ipotesi induuttiva, $P(K-1)$ è verificata, per cui aggiungendo 2 cent si verifica $P(k+1)$ Verificata

F.D.I • 24 - 2023-11-17
VSAB

FUNZIONI > $A, B, A \times B \models^V f = \{ (a, b) \in A \times B \mid \forall a! \exists b (a, b) \in f \}$

Dato 2 funzioni A, B e il loro prodotto cartesiano $A \times B$,
le funzioni sono una relazione di $A \times B$ in cui ad ogni elemento
(rotace) del primo insieme corrisponde un unico elemento del secondo insieme.
(funzione)

Della funzione si definisce:

- Dominio: gli elementi della funzione appartenuti al primo insieme
- Co-dominio: Gli elem. del secondo insieme collegati nella funzione.

RELAZIONE => Sottoinsieme del Prodotto cartesiano

RANGE => Insieme di dest (B)

TIPOLOGIE DI FUNZIONI >

Una funzione viene detta

- Suriettiva: Se la funzione copre tutti gli elementi del co-dominio.
- Iniettiva: Se ogni elemento del dominio punta ad un elem. diverso del codominio.
- Biiettiva: Se la funzione è sia iniettiva che suriettiva.
ovvero ogni elemento del dominio è mappato ad un unico elemento del codominio.

FUNZIONE INVERSA > $x, y, R = \{ (x, y) \in x \times y \} \vdash f = \{ (x, y) \in R \}, \vdash f^{-1} = \{ (y, x) \in R \}$

Dato una funzione iniettiva, la sua inversa f^{-1} è
la funzione dove dominio e co-dominio scambiati.

COMPOSIZIONE > $f, g \models (f \circ g)(x) \equiv f(g(x)) \equiv x \rightarrow g \rightarrow y$

La composizione di funzioni è un'operazione in cui viene applicato
prima la f e dunque la g .

FUNZIONE CARATTERISTICA > $X \models c_x(y) = \begin{cases} 1 & \text{se } y \in x \\ 0 & \text{se } y \notin x \end{cases}$

Dato un insieme, la funzione caratteristica è la funzione
per cui restituisce 1 se un dato elem $\in X$, 0 altrimenti.