

# METODI MATEMATICI PER L'INFORMATICA

La **logica** è alla base di tutti i ragionamenti matematici.

In Matematica la verità è determinata tramite una dimostrazione, un ragionamento logico che stabilisce la verità di un'affermazione. In campo informatico le dim. verificano la correttezza di un sistema.

La ricorsione è un concetto spesso presente quando si parla di algoritmi, in quanto indica quei particolari algoritmi espressi in termini di se stessi: la loro esecuzione su un insieme di dati comporta la suddivisione dell'insieme e la riapplicazione dell'alz. sui nuovi dati.  
Per usarla serve una definizione induttiva del modello dei dati.

Nel linguaggio naturale spesso si usano frasi imprecise o ambigue, mentre quello matematico richiede certezza, cioè che ogni affermazione sia determinabile (vera o falsa).

Una **proposizione** è una frase che può essere vera ( $T$ ) o falsa ( $F$ ), ma non entrambe. Esse sono collegabili tramite **connettivi logici** per creare di più complesse.

**Negazione (not)**      **Congiunzione (and)**

$$P \neg P$$

$$\begin{array}{cc} T & F \\ F & T \end{array}$$

$$P \quad q \quad P \wedge q$$

$$\begin{array}{ccc} T & T & T \\ T & F & F \\ F & T & F \\ F & F & F \end{array}$$

**Disgiunzione (or)**

$$P \quad q \quad p \vee q$$

$$\begin{array}{ccc} T & T & T \\ T & F & T \\ F & T & T \\ F & F & F \end{array}$$

**Disgiunzione esclusiva (xor)**

$$P \quad q \quad p \oplus q$$

$$\begin{array}{ccc} T & T & F \\ T & F & T \\ F & T & T \\ F & F & F \end{array}$$

Implicazione      ↓ ipotesi      ↓ conclusione

$$P \ q \quad p \rightarrow q$$

T	T	T
T	F	F
F	T	T
F	F	T

Se  $p$  allora  $q$

$p$  è sufficiente per  $q$

$q$  è necessaria per  $p$

• Inteso che  $p \rightarrow q$

$$q \Rightarrow p \quad \left. \begin{array}{l} \\ \end{array} \right\} \text{equivalenti}$$

• Opposto  $\equiv$

$$\neg p \rightarrow \neg q$$

• Controinomiale  $\equiv$

$$\neg q \rightarrow \neg p \quad (\text{dim. per assurdo}) \equiv p \rightarrow q$$

Bicondizione

$$P \ q \quad p \Leftrightarrow q$$

equivalente a  $(p \rightarrow q) \wedge (q \rightarrow p)$

T	T	T
T	F	F
F	T	F
F	F	F

ESEMPIO: Costruire la tavola di verità di  $(p \rightarrow q) \wedge (\neg p \leftrightarrow q)$

$$P \ q \quad \neg p \quad p \rightarrow q \quad \neg p \leftrightarrow q \quad (p \rightarrow q) \wedge (\neg p \leftrightarrow q)$$

T	T	F	T	F	F
T	F	F	F	T	F
F	T	T	T	T	T
F	F	T	T	F	F

Una **tautologia** è una proposizione sempre vera  $p \vee \neg p$

Una **contraddizione**  $\equiv$  sempre falsa  $p \wedge \neg p$

Una **contingenza**  $\equiv$  che non è né l'una né l'altra  $p \wedge \neg p$

Un modo per verificare che due proposizioni sono logicamente equivalenti (oltre alle tavole) è quello di ricorrere alle **trasformazioni logiche**.

Leggi di De Morgan  $\neg(p \vee q) \equiv \neg p \wedge \neg q$      $\neg(p \wedge q) \equiv \neg p \vee \neg q$

**Identità**  $p \wedge T \equiv p$      $p \vee F \equiv p$

**Nominazione**  $p \vee T \equiv T$      $p \wedge F \equiv F$

**Idempotenza**  $p \vee p \equiv p$      $p \wedge p \equiv p$

**Doppia negazione**  $\neg(\neg p) \equiv p$

Commutativa  $p \vee q \equiv q \vee p$      $p \wedge q \equiv q \wedge p$

Associativa  $(p \vee q) \vee z \equiv p \vee (q \vee z)$

$$(p \wedge q) \wedge z \equiv p \wedge (q \wedge z)$$

Distributiva  $p \vee (q \wedge z) \equiv (p \vee q) \wedge (p \vee z)$

$$p \wedge (q \vee z) \equiv (p \wedge q) \vee (p \wedge z)$$

$$p \vee \neg p \equiv T \quad p \wedge \neg p \equiv F \quad p \oplus q \equiv (p \wedge \neg q) \vee (\neg p \wedge q)$$

$$p \rightarrow q \equiv \neg p \vee q \quad p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$$

[E.S.] Dim.  $(p \wedge q) \rightarrow p$  è una tautologia

$$\begin{aligned} & \cancel{(p \wedge q) \rightarrow p} \equiv \neg(p \wedge q) \vee p \\ & \equiv (\neg p \vee \neg q) \vee p \quad \text{De Morgan} \\ & \equiv (\neg q \vee \neg p) \vee p \quad \text{Comm.} \\ & \equiv \neg q \vee (\neg p \vee p) \quad \text{Ass.} \\ & \equiv \neg q \vee T \\ & \equiv T \quad \text{Dominazione} \end{aligned}$$

[E.S.]

Sia  $m \in \mathbb{N} = \{1, 2, 3, \dots\}$

Se  $\underbrace{m \geq 5}$  allora  $\underbrace{m}$  è dispari

$$p \rightarrow q$$

Che è vera quando entrambi sono vere :  $\{5, 7, 9, \dots\}$

E quando  $p$  è falsa :  $\{1, 2, 3, 4\}$

$$S = \{1, 2, 3, 4\} \cup \{m \in \mathbb{N} \mid m = 2k+1, k \geq 2\}$$

Nella logica proposizionale uno dei limiti più evidenti è che le affermazioni vanno ripetute per ogni singolo oggetto, dunque per snellire la ripetizione ricorriamo a variabili e quantificatori, entiendo nella

## LOGICA PREDICATIVA

- Costante: modella uno specifico oggetto (Rocco)
- Variabile: rappresenta un oggetto di un certo tipo
- Universo del discorso: definisce il tipo della variabile
- Predicato: rappresenta la proprietà / relazione tra gli oggetti
- Quantificatori: consentono di fare affermazioni su un gruppo di oggetti

### Quantificatore universale $\forall$

$\forall x P(x)$  = per tutti i valori di  $x$  nel dominio,  $P(x)$  è vera  
Da ciò si ha che il  $\forall$  corrisponde ad un 1 tra tutti i valori possibili

Se individuiamo un elemento per cui  $P(x)$  è falsa allora  $\forall x P(x)$  è falsa e l'elemento è detto controesempio

### Quantificatore esistenziale $\exists$

$\exists x P(x)$  = esiste almeno un elemento nel dominio (esempio) per cui  $P(x)$  è vera

L'affermazione è falsa quando non c'è nessun elemento per il quale  $P(x)$  risulta vera

Corrisponde ad un V totale

ES

Tutti gli studenti di INF sono simpatici.

1. Dominio : Studenti INF

Trad. :  $\forall x \text{ Simp}(x)$

Spero al V  $\rightarrow$   
associa  $\rightarrow$   
nelle traduz.

2. D : Studenti

Tr. :  $\forall x (\text{INF}(x) \rightarrow \text{Simp}(x))$

3. B : Persone

Tr. :  $\forall x ((\text{Stud}(x) \wedge \text{Inf}(x)) \rightarrow \text{Simp}(x))$

Qualche studente d. ING è simpatico

1. D : Studenti ING

Tr. :  $\exists x \text{ Simp}(x)$

$\exists$  è legato all' A

2. D : Studenti

Tr. :  $\exists x (\text{Ing}(x) \wedge \text{Simp}(x))$

Tutti S(x) sono P(x)

$\forall x (S(x) \rightarrow P(x))$

Nessun S(x) è P(x)

$\forall x (S(x) \rightarrow \neg P(x))$

Qualche S(x) è P(x)

$\exists x (S(x) \wedge P(x))$

Qualche S(x) non è P(x)

$\exists x (S(x) \wedge \neg P(x))$

Ama (x, y) = " $x$  ama  $y$ "

$\forall x \exists y \text{ Ama}(x, y)$  = Ognuno ama qualcuno

$\exists y \forall x \text{ Ama}(x, y)$  = Esiste qualcuno che è amato da tutti

$\exists x \forall y \neg \text{Ama}(x, y)$  = c'è qualcuno che non ama nessun altro

$\neg \forall x P(x) \equiv \exists x \neg P(x) \quad \neg \exists x P(x) \equiv \forall x \neg P(x)$

# GLI INSIEMI

Collezione non ordinata di oggetti, chiamati elementi

$$S = \{10, 12, 14, 16, 18, 20, 22\} \quad \text{Elenco}$$

$$S = \{x \mid x \text{ è pari e } 10 \leq x \leq 23\} \quad \text{Proprietà}$$

Insieme universale  $U$  - insieme vuoto  $\emptyset$

$$\{2, 2, 3\} = \{1, 2, 2, 3\} = \{3, 1, 2\}$$

Non importano duplicati e ordine

$$A = B \quad \forall x (x \in A) \Leftrightarrow (x \in B)$$

$$A \subseteq B \quad \forall x (x \in A) \rightarrow (x \in B)$$

**Teorema**  $\emptyset \subseteq S$

$$\text{DIM. } \forall x (x \in \emptyset) \rightarrow (x \in S)$$

implicazione con ipotesi falsa sempre, dunque  
l'espressione è vera

Cardinalità  $m$ : intero non negativo che indica il numero  
di elementi contenuti in un insieme  $|S|$

Insieme delle parti (o potenza): insieme di tutti i sottinsiemi  
di  $S$ , indicato con  $P(S)$   $|P(S)| = 2^{|S|}$

Prodotto cartesiano  $S \times T$ : insieme di tutte le coppie ordinate  
 $(s, t)$ ,  $s \in S \wedge t \in T$ , è anti-commutativo  
 $S \times T = \{(s, t) \mid s \in S \wedge t \in T\} \quad |S \times T| = |S| \cdot |T|$

$$A \cup B = \{x \mid x \in A \vee x \in B\} \quad |A \cup B| = |A| + |B| - |A \cap B|$$

$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$

$$A - B = \{x \mid x \in A \wedge x \notin B\}$$

$$\overline{A} = \{x \mid x \in U \wedge x \notin A\}$$

Identità  $A \cup \emptyset = A$   $A \cap U = A$

Dominazione  $A \cup U = U$   $A \cap \emptyset = \emptyset$

Idempotenza  $A \cup A = A$   $A \cap A = A$

Doppio complemento  $\bar{\bar{A}} = A$

Commutativa  $A \cup B = B \cup A$   $A \cap B = B \cap A$

Associativa  $(A \cup B) \cup C = A \cup (B \cup C)$

$(A \cap B) \cap C = A \cap (B \cap C)$

Distributiva  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

De Morgan  $\overline{A \cup B} = \bar{A} \cap \bar{B}$   
 $\overline{A \cap B} = \bar{A} \cup \bar{B}$

Leggi dell'assorbimento  $A \cup (A \cap B) = A$   $A \cap (A \cup B) = A$

Leggi del complemento  $A \cup \bar{A} = U$   $A \cap \bar{A} = \emptyset$

BIM. La prima legge di De Morgan

A	B	$\bar{A}$	$\bar{B}$	$\overline{A \cap B}$	$\overline{A \cup B}$
1	0	0	1	1	1
1	1	0	0	0	0
0	0	1	1	1	1
0	1	1	0	1	1

$\overline{A \cap B} = \{x \mid x \notin A \cap B\}$  complemento

$\{x \mid \neg(x \in A \cap B)\}$  non app.

$\{x \mid \neg(x \in A \cap x \in B)\}$  intars.

$\{x \mid \neg(x \in A) \vee \neg(x \in B)\}$  De Morgan

$\{x \mid x \notin A \vee x \notin B\}$  non app.

$\{x \mid x \in \bar{A} \vee x \in \bar{B}\}$  compl.

$\{x \mid x \in \bar{A} \cup \bar{B}\}$  unione

Una **FUNZIONE** mette in relazione oggetti appartenenti ad un insieme con oggetti appartenenti ad un altro insieme (non necessariamente diverso dal primo)  $f: A \rightarrow B$

Iniettiva  $f(x) = f(y) \Rightarrow x = y$

Suriettiva  $\forall b \in B \exists a \in A : f(a) = b$

Biettiva  $\wedge$  entrambe

Due insiemi  $A$  e  $B$  hanno la stessa cardinalità se esiste una corrispondenza uno-a-uno (biiezione) tra gli elementi di  $A$  e quelli di  $B$

Un insieme che è finito o ha la stessa cardinalità di  $\mathbb{Z}^+$  è detto numerabile, cioè i suoi elementi possono essere enumerati

**Esercizio**

$A = \{0, 2, 4, 6, \dots\}$  è numerabile?

Dobbiamo cercare una  $f$ : biiettiva  $f: \mathbb{Z}^+ \rightarrow A$

$$f: x \in \mathbb{Z}^+ \rightarrow 2x - 2 \in A$$

$$1 \rightarrow 2 \cdot 1 - 2 = 0$$

$$2 \rightarrow 2 \cdot 2 - 2 = 2$$

$$3 \rightarrow 2 \cdot 3 - 2 = 4$$

$f$  è iniettiva  $f(x) = f(y) \Rightarrow 2x - 2 = 2y - 2 \Rightarrow x = y$

$f$  è suriettiva  $\forall a \in A \exists x \in \mathbb{Z}^+ : a = 2x - 2 \Rightarrow (a+2)/2$   
è un int pos.

$$|A| = |\mathbb{Z}^+|$$

**Teorema** L'insieme degli interi  $\mathbb{Z}$  è numerabile

**DIM.**

$$f: x \in \mathbb{Z}^+ \rightarrow \begin{cases} x/2 & x \text{ pari} \\ -(x-1)/2 & x \text{ dispari} \end{cases}$$

$$\text{pari: } f(x) = f(y) \Rightarrow \frac{x}{2} = \frac{y}{2} \Rightarrow x = y$$

$$\text{dispari: } -\frac{(x-1)}{2} = -\frac{(y-1)}{2} \Rightarrow x = y$$

$\forall z \in \mathbb{Z}$   $2z$  è pari positivo ( $z$  pos.)  
 $-2z+1$  è dispari positivo ( $z$  neg.)  
 $|z| = |z^+|$

**TEOREMA** I numeri razionali positivi sono numerabili

Poiché un numero razionale è espresso come  $p/q$ ,  $q \neq 0$

Formiamo una sequenza con tutti i  $p/q$

Disponiamoli per riga, con  $q=1$  nella prima,  $q=2$  nella 2<sup>a</sup> ...

Notiamo che lungo la stessa diagonale  $\swarrow$  i  $p/q$  hanno  $p+q$  uguali.

Poiché non vengono inseriti valori già incontrati ( $2/2 = 1/1 \dots$ )  
i numeri razionali positivi sono numerabili.

**TEOREMA**  $\mathbb{R}$  non è numerabile

Supponendo per assurdo che  $\mathbb{R}$  sia numerabile, ogni suo sottinsieme deve essere numerabile. Creiamo quindi una corrispondenza biunivoca tra  $\mathbb{Z}^+$  e l'intervallo  $[0, 1]$

$[0, 1] : z_1, z_2, z_3, \dots$

$z_1 = 0, d_{11} d_{12} d_{13} \dots$

$z_2 = 0, d_{21} d_{22} d_{23} \dots$

$z_3 = 0, d_{31} d_{32} d_{33} \dots$

...

$d_{i,j} \in \{0, 1, 2, \dots, 9\}$

Costruiamo un numero reale

$z = 0, b_1 b_2 b_3 \dots$  con  $b_i = \begin{cases} 4 & \text{se } d_{i,i} \neq 4 \\ 5 & \text{se } d_{i,i} = 4 \end{cases}$

Anche questo  $z$  dovrebbe appartenere all'intervallo, ma  
questo significa che dire  $b_i = d_{i,i}$  quando invece

$b_i = 4 \neq d_{i,i} = 5$  e  $b_i = 5 \neq d_{i,i} = 4$

ES. 1

$p \rightarrow q$  si traduce come "se  $p$  allora  $q$ ",  $p$  prende il nome di ipotesi e  $q$  di conclusione, inoltre  $p$  si dice condizione sufficiente per  $q$ , mentre  $q$  è necessaria per  $p$

$$p \quad q \quad p \rightarrow q$$

T	T	T
T	F	F
F	T	T
F	F	T

Da cui si ricava che  $p \rightarrow q$  può scrivere  
come  $\neg p \vee q$  in quanto equivalenti

ip.  $\neg p$  e cond.

L'inverso si ottiene scambiando ip. e ipotesi:  $q \rightarrow p$

L'oppuesto // negando sia ip. che cond.:  $\neg p \rightarrow \neg q$

Il contrapposito unisce i precedenti:  $\neg q \rightarrow \neg p$

Se  $m$  è maggiore di  $6$  o  $m$  è dispari allora  $m$  è primo

~~definizione~~

$$[(m > 6) \vee (m \text{ disp.})] \Rightarrow (m \text{ primo})$$

$$\neg(m \text{ primo}) \rightarrow \neg[(m > 6) \vee (m \text{ disp.})]$$

$$m \text{ non primo} \rightarrow \neg(m > 6) \wedge \neg(m \text{ disp.})$$

$$m \text{ non primo} \rightarrow (m \leq 6) \wedge (m \text{ pari})$$

$$ES. 2 \quad P(x, y, z) \quad \Delta \quad \{1, 2\} \times \{1, 2\} \times \{1, 2\}$$

$$\exists x \exists y \exists z \ P(x, y, z)$$

$$\exists y \exists z \ P(1, y, z) \vee \exists y \exists z \ P(2, y, z)$$

$$[\exists z \ P(1, 1, z) \vee \exists z \ P(1, 2, z)] \vee [\exists z \ P(2, 1, z) \vee \exists z \ P(2, 2, z)]$$

$$P(1, 1, 1) \vee P(1, 1, 2) \vee P(1, 2, 1) \vee P(1, 2, 2) \vee$$

$$P(2, 1, 1) \vee P(2, 1, 2) \vee P(2, 2, 1) \vee P(2, 2, 2)$$

$$\forall x \exists y \exists z \ P(x, y, z)$$

$$\exists y \exists z \ P(1, y, z) \wedge \exists y \exists z \ P(2, y, z)$$

$$[\exists z \ P(1, 1, z) \vee \exists z \ P(1, 2, z)] \wedge [\dots]$$

$$[P(1, 1, 1) \vee P(1, 1, 2) \vee P(1, 2, 1) \vee P(1, 2, 2)] \wedge [\dots]$$

$$\forall x ((x > 0) \Rightarrow Q(x)) \quad Q(x) = \{-3, -2, -1, 1, 2, 3\}$$

$$\forall x (x \leq 0) \vee Q(x)$$

$$[-3 \leq 0] \vee Q(-3) \wedge [-2 \leq 0] \vee Q(-2) \wedge [-1 \leq 0] \vee Q(-1) \wedge$$

$$[0 \leq 0] \vee Q(0) \wedge [1 \leq 0] \vee Q(1) \wedge [2 \leq 0] \vee Q(2) \wedge [3 \leq 0] \vee Q(3)$$

$$[T \vee Q_0] \wedge [T \vee Q_{-2}] \wedge [T \vee Q_{-1}] \wedge [F \vee Q_1] \wedge [F \vee Q_2]$$

$$T \wedge T \wedge T \wedge Q(1) \wedge Q(2) \wedge Q(3)$$

$$Q(1) \wedge Q(2) \wedge Q(3)$$

ES. 3

$$A(x, y) = "y \text{ amico di } x" \quad R(x, z, y) = "x \text{ regala } z \text{ a } y" \quad \text{a Natale}$$

"A Natale si fanno regali agli amici" (ogni persona fa regali ad un'altra amica)

$$\forall x \forall y (A(x, y) \Rightarrow \exists z R(x, z, y))$$

$$P(x) = "x \text{ è una pietra preziosa}" \quad B(x) = "x \text{ è bolla}"$$

"Non tutte le pietre preziose sono bolle"

$$\neg \forall x (P(x) \Rightarrow B(x)) \equiv \exists x (P(x) \wedge \neg B(x))$$

ES. 4

$$P(x) : "x < 10 \Rightarrow x \text{ multiplo di } 3"$$

$$Q(x) : "x < 5 \Rightarrow x \text{ è pari}"$$

$$A = \{x \mid P(x)\} \cup B = \{x \mid Q(x)\} \quad \overline{A \cup B} = ?$$

$$A = \{3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96, 99\}$$

$$B = \{2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98\}$$

$$A = \{3, 6, 9\} \cup \{10, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48, 51, 54, 57, 60, 63, 66, 69, 72, 75, 78, 81, 84, 87, 90, 93, 96, 99\}$$

$$B = \{2, 4, 6, 8\} \cup \{10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98\}$$

$$A \cup B = \{2, 3, 4, 5, 6, 7, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98\}$$

$$\overline{A \cup B} = \{1\}$$

ES. 7

$D(x)$ : "x è una donna"

$A(x, y)$ : "x ama y"

$F(x, y)$ : "y è figlio di x"

Ogni donna ama i suoi figli. (alcuna) (tutti i suoi)

$$\forall x D(x) \rightarrow \exists y F(x, y) \wedge A(x, y) \quad \forall x \forall y [(D(x) \wedge F(x, y)) \rightarrow A(x, y)]$$

Maria non ama tutti i figli di Francesco

$$\exists y [F(\text{Francesco}, y) \wedge \neg A(\text{Maria}, y)] \quad (\text{Un figlio non è amato})$$

ES. 8

$A = \{x \mid P(x)\}$   $P(x) = "x > 8 \rightarrow x \text{ multiplo di } 2"$

$B = \{x \mid Q(x)\}$   $Q(x) = "x > 7 \rightarrow x \text{ pari}"$

$$A = \{1, 2, \dots, 8\} \cup \{12, 14, 20, \dots\}$$

$$B = \{2, 4, \dots, 7\} \cup \{8, 10, 12, \dots\}$$

$$A \cup B = \{1, 2, \dots, 8\} \cup \{10, 12, 14, \dots\} = \{1, 3, 5, 7\} \cup \{m \in \mathbb{N} \mid m = 2k, k \in \mathbb{N}\} = B$$

ES. 10

$$\neg [\exists x \forall y (x \geq y + 3)]$$

$$\neg \forall x \forall y \exists z (x^2 = y + z)$$

$$\forall x \neg [\forall y (x \geq y + 3)]$$

$$\exists x \exists y \forall z (x^2 \neq y + z)$$

$$\forall x \exists y (x < y + 3)$$

$$\forall x \exists y (x < y + 3)$$

ES. 11

$$\neg [\exists x \forall y (P(x, y) \wedge Q(x, y))] \equiv \forall x \exists y \neg [P(x, y) \wedge Q(x, y)] \equiv \neg P(x, y) \vee \neg Q(x, y)$$

$$\begin{aligned} \forall x \exists y \neg [(\rho(x, y) \Leftrightarrow \alpha(x, y))] &\equiv \neg [((\rho(x, y) \rightarrow \alpha(x, y)) \wedge (\alpha(x, y) \rightarrow \rho(x, y))) \\ &\equiv \neg ((\rho(x, y) \rightarrow \alpha(x, y)) \vee \neg (\alpha \rightarrow \rho)) \\ &\equiv \neg \forall x \exists y [(\rho \wedge \neg \alpha) \vee (\alpha \wedge \neg \rho)] \end{aligned}$$

ES. 12

$S(x)$ : " $x$  è uno studente d. INF"

$M(x, y)$ : " $x$  ha visitato  $y$ "

Qualche studente INF ha visitato Milano

$\exists x (S(x) \wedge M(x, \text{Milano}))$

Ogni studente d. INF ha visitato Milano

$\forall x (S(x) \rightarrow M(x, \text{Milano}))$

Non tutti gli studenti d. INF hanno visitato Roma

$\neg \forall x (S(x) \rightarrow M(x, \text{Roma})) \equiv \exists x (S(x) \wedge \neg M(x, \text{Roma}))$

ES. 13

$$A \cap B = A \Leftrightarrow A \subseteq B$$

Supponiamo  $A \not\subseteq B$ , dobbiamo arrivare a  $A \cap B \neq A$

Esiste  $a$  tale che  $a \in A \wedge a \notin B$ . Quindi  $a \in A$  ma  $a \notin A \cap B$ . Questo significa che  $A \subseteq A \cap B$ , dunque  $A \cap B \neq A$

$A \cap B \Leftrightarrow A \Rightarrow A \supseteq B$  deve essere una tautologia

$$\begin{array}{ccccc} A & B & A \cap B & A \cap B \Leftrightarrow A & (A \cap B \Leftrightarrow A) \Rightarrow A \supseteq B \\ \top & \top & \top & \top & \top \\ \top & \bot & \bot & \bot & \bot \\ \bot & \top & \bot & \bot & \bot \\ \bot & \bot & \bot & \bot & \bot \end{array}$$

ES 14

$$p \wedge q \Rightarrow r \equiv p \Rightarrow (q \Rightarrow r \wedge p)$$

$$p \Rightarrow (q \Rightarrow r \wedge p) \equiv \neg p \vee (q \Rightarrow r \wedge p) \equiv \neg p \vee (\neg q \vee (r \wedge p)) \equiv$$

$$\equiv (\neg p \vee \neg q \vee r) \wedge (\neg p \vee \neg q \vee p) \quad (\text{distrib.})$$

$$\equiv (\neg p \vee \neg q \vee r) \wedge (\top \vee \neg q) \quad (\text{tut.}) \equiv (\neg p \vee \neg q \vee r) \wedge \top \quad (\text{dom.})$$

$$\equiv (\neg p \vee \neg q) \vee r \equiv \neg(p \wedge q) \vee r \equiv p \wedge q \Rightarrow r$$

con

De Morgan

Es.

$p$  = Gli orsi guinzali sono stati visti in zona

$q$  : Camminare lungo il tragitto è sicuro

$r$  : Le more sono mature lungo il tragitto

1. Le more sono mature lungo il tragitto, ma gli orsi guinzali

non si sono visti in zona

$\neg r \wedge p$

2. Gli orsi non sono stati visti in zona  $\neg r$ , lungo il tragitto, camminare  
è sicuro  $\neg q$  le more sono mature

$\neg p \wedge \neg q \wedge \neg r$

3. Se le more sono mature lungo il tragitto allora camminare  
lungo il tragitto è sicuro se e solo se gli orsi non sono stati  
visti  
 $(\neg r \rightarrow q) \Leftrightarrow \neg p$

4. Non è sicuro camminare lungo il tragitto, ma gli orsi non  
sono stati visti se le more sono mature.

$\neg q \wedge \neg p \wedge \neg r$

5. Per camminare in maniera sicura lungo il tragitto, è necessario  
ma non sufficiente che le more non siano mature  $\neg q$  che gli  
orsi non siano stati visti

$q \rightarrow (\neg r \wedge \neg p)$

6. Non è sicuro camminare sul cammino ogni volta gli orsi  
sono stati visti se le more sono mature

$\neg q \rightarrow (\neg p \wedge \neg r) \quad (\neg p \wedge \neg r) \rightarrow \neg q$

Es.

"Se  $I+L=2$  allora i cani possono volare"

L'affermazione è falsa in quanto a trovaremo di fronte

ad una implicazione in cui l'ipotesi è vera

$(I+L=2)$ , ma la conclusione è falsa (i cani ... volano)

ES.

"Io vengo a lezione ogniqualvolta c'è un test"

"Se c'è un test allora io vengo a lezione"

Oposto: "Se vengo a lezione allora non c'è test"

Inversa: "Se vengo a lezione allora c'è un test"

Oposto: "Se non c'è un test allora non vengo a lezione"

contrario: "Se non vengo a lezione allora non c'è un test"

ES.

$$(p \Rightarrow q) \vee (\neg p \Rightarrow q)$$

p	q	$p \Rightarrow q$	$\neg p$	$\neg p \Rightarrow q$	$(p \Rightarrow q) \vee (\neg p \Rightarrow q)$
T	T	T	F	T	T
T	F	F	F	T	T
F	T	T	T	T	T
F	F	T	T	F	T

ES.

$$(p \Leftrightarrow q) \Leftrightarrow (\neg p \Leftrightarrow \neg q)$$

La tavola di verità è composta da 16 righe, cioè  $2^m$  con  
 $m = \text{num. delle variabili}$ .

ES.

$$(p \vee \neg q) \wedge (q \vee \neg z) \wedge (\neg z \vee \neg p)$$

La proposizione è vera solo quando le tre variabili hanno  
le stesse valori <sup>distanza</sup> opposti perché le coppie sono fatte in  
modo da garantire che almeno una variabile sia vera.

Se per esempio avessimo invece  $p = q = T$  e  $z = F$ :

$$(T \vee F) \wedge (T \vee T) \wedge (F \vee F) \equiv$$

$$\equiv T \wedge T \wedge F \equiv F$$

Lo stesso si ottiene negli altri casi di discordanza

es.  $((p \wedge q) \vee z) \rightarrow (z \wedge s)$  è falsa.

Ricordando che l'unica esito di implicazione falsa è quando l'ip. è vera e la cond. è falsa; analizziamo prima quella dell'ip.

~~se l'ip. è falsa qualsiasi cosa è vero è vero falso~~  
~~quindi la tesi è falsa~~  
~~falso è sempre falso~~  
 (entro in esercizi)

es.

Sono ammesse al concorso le persone che sono laureate e che hanno meno di 30 anni o hanno figli.

$p$  = persone laureate

$q$  = persone con meno di 30 anni

$r$  = persone che hanno figli

$$(p \wedge q) \vee r$$

1. Aldo non è laureato, ha 26 anni e un figlio ✓
2. Paolo è laureato, ha 40 anni e 2 figli ✓
3. Vincenzo è laureato, ha 32 anni e non ha figli ✗

es.

$$\begin{aligned}
 & \neg((p \vee q) \Rightarrow \neg q) \equiv q ? \\
 & \equiv \neg(\neg(p \vee q) \vee \neg q) \\
 & \equiv \neg(\neg p \wedge \neg q) \vee \neg q \\
 & \equiv \neg((\neg p \vee \neg q) \wedge (\neg q \vee \neg q)) \\
 & \equiv \neg((\neg p \vee \neg q) \wedge \neg q) \\
 & \equiv \neg(\neg(p \vee \neg q) \vee \neg \neg q) \\
 & \equiv (p \wedge q) \vee q
 \end{aligned}$$

ES.

$$(p \Rightarrow q) \Rightarrow z \equiv p \Rightarrow (q \Rightarrow z) ?$$

$$\begin{aligned} (p \Rightarrow q) \Rightarrow z &\equiv (\neg p \vee q) \Rightarrow z \\ &\equiv \neg(\neg p \vee q) \vee z \\ &\equiv (p \wedge \neg q) \vee z \\ p \Rightarrow (q \Rightarrow z) &\equiv p \Rightarrow (\neg q \vee z) \\ &\equiv \neg p \vee (\neg q \vee z) \\ &\equiv \neg p \vee \neg q \vee z \end{aligned}$$

ES.

$$p \Leftarrow q \equiv \neg p \Leftarrow \neg q ?$$

$$\begin{aligned} p \Leftarrow q &\equiv (p \Rightarrow q) \wedge (q \Rightarrow p) \\ &\equiv (\neg p \vee q) \wedge (\neg q \vee p) \end{aligned}$$

$$\begin{aligned} \neg p \Leftarrow \neg q &\equiv (\neg p \Rightarrow \neg q) \wedge (\neg q \Rightarrow \neg p) \\ &\equiv (\neg(\neg p) \vee \neg q) \wedge (\neg(\neg q) \vee \neg p) \\ &\equiv (p \vee \neg q) \wedge (q \vee \neg p) \\ &\equiv (\neg q \vee p) \wedge (\neg p \vee q) \\ &\equiv (\neg p \vee q) \wedge (\neg q \vee p) \quad \checkmark \end{aligned}$$

ES.

$$(p \Rightarrow q) \Rightarrow q \equiv \top ?$$

$$\begin{aligned} (p \Rightarrow q) \Rightarrow q &\equiv (\neg p \vee q) \Rightarrow q \\ &\equiv \neg(\neg p \vee q) \vee q \\ &\equiv (p \wedge \neg q) \vee q \\ &\equiv (p \vee q) \wedge (\neg q \vee q) \\ &\equiv (p \vee q) \wedge \top \\ &\equiv p \vee q \end{aligned}$$

es.

$$\begin{aligned}
 \neg(q \rightarrow \neg(q \Rightarrow p)) &\equiv q \wedge p & ? \\
 \neg(q \Rightarrow \neg(q \Rightarrow p)) &\equiv \neg(q \Rightarrow \neg(\neg q \vee p)) & \text{def. d. impl.} \\
 &\equiv \neg(q \Rightarrow (q \wedge \neg p)) & \text{De Morgan} \\
 &\equiv \neg(\neg q \vee (q \wedge \neg p)) & \text{def. d. impl.} \\
 &\equiv \neg(\neg q \vee q) \wedge (\neg q \vee \neg p) & \text{distrib.} \\
 &\equiv \neg(\top \wedge (\neg q \vee \neg p)) & \text{def. d. Taut.} \\
 &\equiv \neg(\neg q \vee \neg p) & \text{identità} \\
 &\equiv q \wedge p & \checkmark \quad \text{De Morgan}
 \end{aligned}$$

## DIMOSTRAZIONI

Una dimostrazione è un ragionamento corretto che stabilisce la verità di un'asserzione matematica (teorema) attraverso l'uso di altre asservizioni vere:

- ipotesi del teorema
- assiomi
- teoremi dimostrati in precedenza

Forma  $p \Rightarrow q$  Dim. DIRETTA

Viene mostrato che "se  $p \in T$ , allora  $q \in T$ "

Ese.: Sia  $m$  intero. Se  $m$  è dispari, allora  $m^2$  è dispari.

Assumiamo vera d'ipotesi, dunque  $m = 2k + 1$ ,  $k \in \mathbb{N}$

$$m^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 \quad \text{dunque}$$

$m^2$  è dispari

Forma  $p \Rightarrow q$  Dim. CONTRAPPOSIZIONE

Dimostriamo che "se  $\neg q \in T$ , allora  $\neg p \in F$ " ( $\neg p \notin T$ )

Ese.: Se  $3m+2$  è dispari, allora  $m$  è dispari

Assumiamo  $m$  pari,  $m = 2k$ ,  $k$  intero

$$3m+2 = 3(2k)+2 = (3k+2) = 2(3k+1) \quad \text{dunque}$$

$3m+2$  è pari

**Forma  $p \Rightarrow q$**  Dim. ASSURDO

Dimostriamo che " $\neg p \vee q$  è  $\neg q \vee p$ , allora  $F$ "

È possibile perché :

$$(\neg p \vee q) \Rightarrow F \equiv \neg(\neg p \vee q) \vee F \equiv \neg(\neg p \vee q) \equiv \neg\neg p \vee \neg q \equiv p \Rightarrow q \quad 6$$

Es.: Se  $3m+2$  è dispari,  $m$  è dispari.

Assumiamo  $m$  pari :  $m=2k$ ,  $k$  intero

Per ip. supponiamo che  $3m+2$  è dispari :  $3m+2 = 2h+1$ ,  $h$  int.

$$2h+1 = 3m+2$$

$$= 3(2k)+2$$

$$= 2(3k+1) \text{ che è pari}$$

Es.: Date  $x$  e  $y$  reali, se  $5x+25y=1723$ , allora  $x$  o  $y$  non sono interi.

$\neg(x \circ y \text{ non sono interi}) \equiv x \circ y \text{ sono interi}$

$$\overline{5x+25y} = 1723$$

$$\overline{5(x+5y)} = 1723$$

$$x+\overline{5y} = \frac{1723}{5} \text{ che non è un intero e porta ad un assurdo} \quad 4$$

**Forma  $p \Leftrightarrow q$**  Dim. EQUIVALENZA

Dimostriamo  $(p \Rightarrow q) \wedge (q \Rightarrow p)$  ricordando ai casi precedenti:

Nel caso più generale siamo equivalenti:

$$p_1 \Leftrightarrow p_2 \Leftrightarrow \dots \Leftrightarrow p_m$$

o dimostriamo  $(p_1 \Rightarrow p_2) \wedge (p_2 \Rightarrow p_3) \wedge \dots \wedge (p_m \Rightarrow p_1)$ .

**Forma  $p \Rightarrow q$**  Dim. BANALE e Dim. VUOTA

Se la conclusione  $q$  è sempre vera, allora  $p \Rightarrow q$  è banalmente vera.

Es.: Se  $a \geq b$ , allora  $a^m \geq b^m$ .

Mostriamo che  $P(m) \Rightarrow P(0)$  :  $a^0 \geq b^0 \equiv 1=1$ , vero indipendentemente da  $m$

Se l'ipotesi  $p$  è sempre falsa, allora  $p \Rightarrow q$  è banalmente vera

Es.: Se  $m \geq 1$ , allora  $m^2 \geq 1$ .  $\forall (m=0) \Rightarrow P(0)$

per  $m=0$  l'ip.  $P(0)$  sempre  $T$

Forma  $(p_1 \vee p_2 \vee \dots \vee p_m) \geq q$  Dim ANALISI SCIENSI

Equivale a dire  $(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \dots \wedge (p_m \rightarrow q)$

Es.:  $|x| \cdot |y| = |x \cdot y|$  per  $x, y$  reali

$$1. x \geq 0, y \geq 0 \Rightarrow x \cdot y \geq 0 \wedge |x \cdot y| = x \cdot y = |x| \cdot |y|$$

$$2. x \geq 0, y < 0 \Rightarrow x \cdot y \leq 0 \wedge |x \cdot y| = -x \cdot y = x \cdot (-y) = |x| \cdot |y|$$

$$3. x < 0, y \geq 0 \Rightarrow x \cdot y \leq 0 \wedge |x \cdot y| = -x \cdot y = (-x) \cdot y = |x| \cdot |y|$$

$$4. x < 0, y < 0 \Rightarrow x \cdot y > 0 \wedge |x \cdot y| = -x \cdot y = (-x) \cdot (-y) = |x| \cdot |y|$$

$$|x \cdot y| = (-x) \cdot (-y) = |x| \cdot |y|$$

Tutti i casi sono provati

### Quantificatore esistenziale

Dim. COSTRUTTIVA: trovare un esempio

Es.: Esiste un intero scrivibile come somma di <sup>due</sup> cubi in 2 diversi modi

$$1729 = 10^3 + 9^3 = 12^3 + 1^3$$

NON COSTRUTTIVA: Si dimostra per assurdo negando la affermazione e giungendo a una contradd.

Es.: Principio della piccionaia

Se  $m+1$  oggetti sono distribuiti in  $m$  scatole, allora qualche scatola deve contenere almeno 2 oggetti

Assumiamo di avere  $m+1$  oggetti ed  $m$  scatole  $B_1, \dots, B_m$

Per assurdo supponiamo che nessuna scatola contenga più di 1 oggetto

$K_i =$  num. d. oggetti posti in  $B_i$ , per  $i = 1, \dots, m$ ,  $K_i \leq 1$

$$\text{Allora } K_1 + K_2 + \dots + K_m \leq 1 + 1 + \dots + 1 = m$$

che contraddice l'ipotesi

## Quantificatore universale

- Provando che la proprietà vale per tutti i valori nel dominio
- $\neg \forall x P(x) \equiv \exists x \neg P(x)$
- Per induzione

## INDUZIONE MATEMATICA

Usata per provare asezioni con dominio  $\mathbb{Z}^+$  della forma  $\forall m P(m)$

Base: La proposizione  $P(1)$  è vera

Passo di induzione: Fissato un intero positivo  $n$ , l'implicazione

$P(m) \rightarrow P(m+1)$  è vera.  $P(n)$  ipotesi induttiva

Si conclude quindi che  $\forall m P(m)$

Esempio: La somma dei primi  $m$  interi pos. dispari vale  $m^2$

$$P(m) = 1 + 3 + 5 + \dots + (2m-1) = m^2$$

Base:  $(m=1) \quad 1 = 1^2$  vero

Passo: Supponiamo  $P(m)$  vera.

$$P(m+1) \text{ vale } 1 + 3 + 5 + \dots + (2m-1) + [2(m+1)-1]$$

$$P(m+1) = \underbrace{1 + 3 + 5 + \dots + (2m-1)}_{= m^2} + (2m+1) \quad \checkmark$$

$$= m^2 + (2m+1) = (m+1)^2 \quad \checkmark$$

Esempio:  $m < 2^m$  per tutti gli interi positivi  $m$

$$P(m) : m < 2^m, m \geq 1$$

$$\text{Base: } P(1) : 1 < 2^1 \text{ (ovvio)}$$

Ipotesi: Supponiamo  $P(m) : m < 2^m$  vera

$$P(m+1) : m+1 < 2^{m+1} \text{ vera?}$$

$$m+1 < 2^m + 1 \quad (\text{aggiungiamo } +1 \text{ ambo i lati})$$

$$m+1 < 2^m + 1 < 2^m + 2^m \quad (\text{maggioriamo } 1)$$

$$2^m + 2^m = 2 \cdot 2^m = 2^{m+1}$$

Esercizio: Proviamo  $m^2 < 2^m$ , per ogni  $m \geq 5$

Base:  $P(5) : 5^2 < 2^5$  (ovvio)

Passo: mostriamo che  $P(m+1) : (m+1)^2 < 2^{m+2}$  è vera

$$(m+1)^2 = m^2 + 2m + 1 = m^2 + 2m + m \quad (\text{perché } m \geq 5 > 1)$$

$$= m^2 + 3m = m^2 + m \cdot m = m^2 + m^2 \quad (m \geq 5 > 0)$$

$$= 2m^2 < 2 \cdot 2^m = 2^{m+1} \quad \text{per ipotesi ind.}$$

Esercizio: Proviamo che un insieme con  $n$  elementi ha  $2^n$  sottinsiemi.

Base:  $P(0) : \text{Se un insieme ha } 0 \text{ elementi, ha un unico sottinsieme, se stesso}$

Passo: Sia  $T$  un insieme con  $n+1$  elementi e sia  $\alpha$  un elemento di  $T \Rightarrow T = S \cup \{\alpha\}$ , con  $|S|=n$

I sottinsiemi di  $T$  si possono costituire a partire da  $S$

cioè: Per ogni sottinsi.  $X$  di  $S$ , ci sono 2 sottinsi. di  $T$ .

$X$  stesso e  $X \cup \{\alpha\}$

Il num. di sottinsi. di  $T$  è pertanto  $2 \cdot 2^n = 2^{n+1}$

6

### Induzione forte

Passo base:  $P(1)$

Passo di induzione:  $[P(1) \wedge P(2) \wedge \dots \wedge P(n)] \Rightarrow P(n+1)$

Esercizio: Un int. pos.  $n > 1$  o è primo o si può scrivere come

BASE:  $P(2)$  è vera:  $2=2$

prodotto di primi

PASSO: Assumiamo vera  $P(2), \dots, P(n)$  e dimostriamo  $P(n+1)$

Se  $(n+1)$  è primo allora  $P(n+1)$  è banalmente vera

Se  $n+1$  è non primo allora vale  $n+1 = a \cdot b$

ma per ip. sappiamo che  $P(a)$  e  $P(b)$  sono vere e quindi  $n+1$  si può scrivere come prodotto di primi

ES. Sia  $x$  un n. paro e  $y$  dispari. Dim. per assurdo che  $x+y$  è dispari.

Per assurdo  $x+y$  è paro. Sappiamo per ipotesi che

$$x = 2K, K \geq 0 \quad \text{e} \quad y = 2h+1, h \geq 0$$

$$x+y = 2K+2h+1 = 2(K+h)+1 \quad \text{che è un numero disp.}$$

↯

ES. Sia  $m \in \mathbb{N}$ . Dim. che la somma dei primi  $m$  numeri è uguale a  $\frac{m(m+1)}{2}$

$$\text{P. B. } (m=1) : \frac{1 \cdot (1+1)}{2} = \frac{2}{2} = 1 \quad \checkmark$$

Supponiamo per ipotesi induttiva  $P(m)$  vera, cioè che

$$\sum_{K=1}^m K = \frac{m(m+1)}{2} \quad \text{e dimostriamo } P(m+1), \text{ cioè}$$

$$\sum_{K=1}^{m+1} K = \frac{(m+1)[(m+1)+1]}{2} \quad \text{da cui segue}$$

$$= \frac{(m+1)(m+2)}{2} = \frac{m^2+2m+m+2}{2} = \frac{m^2+m}{2} + \frac{2(m+1)}{2} =$$

$$= \sum_{K=1}^m K + (m+1) \quad \checkmark$$

Iniezione strutturale (provare proprietà d. oggetti def. ricorsiv.)

Dati  $A$  insieme di elem. def. ricorsiv. e  $P$  proprietà, si vuole provare  $\forall x \in A \ P(x)$ :

Base:  $P$  è vero per tutti gli elementi specificati nel passo

Base della def. ricors. d.  $A$

Passo: Se  $P$  è vero per gli elementi già presenti in  $A$  (quelli usati per costituire altri nel Passo Ricorsivo), allora  $P$  è vero per tutti i nuovi elementi.

ES. Sia  $A$  l'insieme così definito:

P. B. :  $1 \in A$

P. R. :  $\forall x \in A$ , allora  $x+2 \in A$

Provare che  $A$  è costituito dagli int. disp. positivi.

Sia  $D = \{y \in \mathbb{N} \mid y = 2k+1, k \geq 0\}$  e proviamo che

$D = A$ , cioè  $D \subseteq A$  e  $A \subseteq D$

( $D \subseteq A$ ) procediamo per induzione, con  $P(k)$ :  $2k+1 \in A \forall k \geq 0$

P. B. : ( $k=0$ )  $2 \cdot 0 + 1 = 1 \in A$

Assumiamo per ipotesi che  $P(k)$  sia vera

P. I. : Proviamo  $P(k+1)$  vera:  $2(k+1)+1 = 2k+2+1 = (2k+1)+2 \in A$

( $A \subseteq D$ ) ind. str.

$P(x)$ :  $x = 2k+1$  per qualche  $k \geq 0$

P. B. : Dalla base della def. sappiamo che  $1 \in A \Rightarrow$

$P(1)$  è vera  $\Rightarrow 1 \in D$

P. R. : Assumiamo  $P(x)$  vera e dimostriamo  $P(x+2)$

$$x = 2k+1 \Rightarrow x+2 = 2k+1+2 = 2(k+1)+1 \in D$$

ES. Sia  $X$  l'insieme degli int. così def.:

•  $1 \in X \wedge 2 \in X$

•  $\forall x \in X$  allora anche  $x+3 \in X$

Dim.  $X=Y$ , con  $Y$  insieme degli int. pos. non multipli di 3

$$Y = \{y \in \mathbb{N} \mid y = 3k+h, k \geq 0 \text{ e } h \in \{1, 2\}\}$$

( $X \subseteq Y$ ) P. B. :  $1, 2 \in X$ .  $\nexists k, h \in \mathbb{N}$  tali che  $1 = 3k+2 = 3h$

P. I. :  $P(x)$  vera  $\Rightarrow x \in X \wedge x \in Y \Rightarrow P(x+3)$ .

Per assurdo  $x+3 \notin Y$ , ma quindi  $x+3$  è multiplo di 3  
e dunque  $x+3 = 3k$ , da cui  $x = 3(k-1)$  che implica  
 $x \notin Y$ , un assurdo.

$(Y \subset X)$  P. B. - Siamo  $l, 2 \in Y$  i più piccoli int. pos. men multipli di 3. Consideriamo  $l, 2 \in X$

P. I.: Supponiamo  $P(Y)$  vera, dunque  $y \in Y \Rightarrow y \in X$  e dim.  $P(y+3)$ , cioè  $y+3 \in X$ . Poiché per ipotesi induttiva  $y \in X$ , per def. di  $X$  anche  $y+3 \in X \in Y$

ES. Dim. per induzione che  $\forall m \in \mathbb{N}_0, 2^m \geq m+1$

$$\text{P.B. } (m=0) \text{ Si ha } 2^0 = 1 \geq 1 = 0+1 \quad \checkmark$$

P. I. Supponiamo  $P(m)$  vera per ipotesi induttiva e dimostriamo che  ~~$P(m+1)$~~   $\Rightarrow 2^{m+1} \geq (m+1)+1$  è vera

$$2^{m+1} = 2^m \cdot 2 \quad (m+1)+1 = m+2$$

$$2^m \cdot 2 \geq m+2 \Rightarrow 2^m \geq \frac{m+1}{2} = \frac{m+2}{2}$$

Sapendo per ip. che  $2^m \geq m+1$  e poiché  $m+1 > \frac{m+1}{2}$   
si ha  $2^m \geq m+1 > \frac{m+1}{2}$  dunque l'asserto è vero

ES. Dim. per induzione che  $\exists K \in \mathbb{N} : 3^m < m!$ ,  $\forall m \geq K$

$$\text{P.B. } (m=7) \text{ Si ha } 3^7 = 2187 < 5040 = 7!$$

P. I. Supponiamo per ipotesi induttiva  $P(m)$  vera e dim.  
che  $P(m+1)$  è vera, cioè  $3^{m+1} < (m+1)!$

$$3^{m+2} = 3^m \cdot 3 \quad (m+1)! = m! \cdot (m+1)$$

Poiché  $3^m < m!$  è vero, sceglio ~~una coppia~~ due valori  $x < y$  con  
 $x < y$  in modo che  $3^m \cdot x < m! \cdot y$  sia ancora vero.

In particolare, con  $x=3$  e  $y=m+2$  ho dal passo base  
che  $3 < m+1$ ,  $\forall m \geq 7$  e quindi  $3^m \cdot 3 < m! \cdot (m+1)$

è vero  $\forall m \geq 7$

# RICORSIONE

Le definizioni ricorsive sono definizioni che sfruttano il fatto che degli oggetti (funzioni, algoritmi, insiemi, ecc.) possono essere definiti in termini di se stessi, ma di più piccole dimensioni.

Esempio: La sequenza delle potenze di 3: 1, 3, 9, 27, 81, ...  
 $b_m = 3^m$ ,  $m \in \mathbb{N}$  può essere scritta ricorsivamente.

$$b_0 = 1$$

$$b_m = 3 \cdot b_{m-1}, m \geq 1$$

Def. u.c. progressione aritmetica  $b_m = b_{m-1} + d$ ,  $m \geq 1$

$$b_0 = a$$

Def. u.c. progressione geometrica  $b_m = b_{m-1} \cdot r$ ,  $m \geq 1$

$$b_0 = a$$

Per definire una funzione ricorsiva sull'insieme degli interi non negativi

Passo base: Specificare  $f(0)$

Passo ricorsivo: Fornire la regola per calcolare  $f(m)$  in termini di  $f(m-1)$

Fattoriale:  $0! = 1$

$$m! = m \cdot (m-1)!, m \geq 1$$

Esempio: Def. u.c.  $f(m) = 2m+1$

$$f(0) = 1 \quad f(1) = 3 = 1+2 = f(0)+2$$

$$f(2) = 5 = 3+2 = f(1)+2$$

$$f(0) = 1$$

$$f(m) = f(m-1)+2, m \geq 1$$

Es: Def. n.c.  $f(m) = m^2$ ,  $m \geq 1$

$$f(1) = 1$$

Sviluppo  $f(m-1)$  per arrivare ad  $f(m)$ :

$$f(m-1) = (m-1)^2 = m^2 - 2m + 1 = f(m) - 2m + 1$$

$$f(2) = 1$$

$$f(m) = f(m-1) + 2m - 1, m \geq 2$$

Es.: Data  $f$  definita come:

$$f(0) = 3$$

$$f(m) = 2 \cdot f(m-1) + 3, m \geq 1$$

$$f(0) = ? \Rightarrow f(0) = 3$$

$$f(1) = 2 \cdot 3 + 3 = 9$$

$$f(2) = 2 \cdot 9 + 3 = 21$$

$$f(3) = 2 \cdot 21 + 3 = 45$$

Es.: Sia  $f$  la funzione fattoriale

$$4! = ?$$

$$4! = 4 \cdot 3!$$

$$3! = 3 \cdot 2!$$

$$2! = 2 \cdot 1!$$

$$1! = 1 \cdot 0! \quad 0! = 1$$

$$1! = 1 \quad 2! = 2 \cdot 1 = 2$$

$$3! = 3 \cdot 2 = 6$$

$$4! = 4 \cdot 6 = 24$$

PROVARE LA CORRETTEZZA DI UN ALGORITMO

$\begin{cases} f(0) = 3 \\ f(m) = 2 \cdot f(m-1) + 3 \end{cases} \rightarrow$  procedura funz(m) {  
if ( $m == 0$ ) return 3;  
return  $2 \cdot \text{funz}(m-1) + 3$ ;  
}

Dimostriamo che il valore restituito da funz(m) coincide con  $f(m)$

P.B.:  $\text{funz}(0) = 3 = f(0)$  ✓      Ip.  $\text{funz}(m) = f(m)$

P.I.:  $\text{funz}(m+1) = 2 \cdot \text{funz}(m) + 3 = 2 \cdot f(m) + 3 = f(m+1)$  ✓

```

int Fib(m) {
    if (m <= 2) return m;
    return Fib(m-1) + Fib(m-2);
}

```

$$\begin{aligned}
 f(0) &= 0 \\
 f(1) &= 1 \\
 f(m) &= f(m-1) + f(m-2) \quad m \geq 2
 \end{aligned}$$

P.B.:  $\text{Fib}(0) = 0 \Rightarrow f(0) \quad \text{e} \quad \text{Fib}(1) = 1 = f(1)$

P.I.: Per ip. si ha  $\text{Fib}(m) = f(m) \quad \text{e} \quad \text{Fib}(m-1) = f(m-1)$   
 $\text{Fib}(m+1) = \text{Fib}(m) + \text{Fib}(m-1) = f(m) + f(m-1) = f(m+1)$  ✓

## STRINGHE

Possono essere descritti ricorsivamente insiemi di stringhe.

Un alfabeto è un insieme finito di lettere e simboli, detti elementi. (Alf. delle cifre arabe - Alf. binario - ...)

L'insieme di stringhe  $\Sigma^*$  sull'alfabeto  $\Sigma$  è definito così:

P.B.: la stringa vuota  $\lambda \in \Sigma^*$

P.R.: Se  $w \in \Sigma^*$  e  $x \in \Sigma$  allora  $wx \in \Sigma^*$  (concatenazione)

La lunghezza di una parola in  $\Sigma^*$  sull'alfabeto  $\Sigma$  è:

P.B.:  $\ell(\lambda) = |\lambda| = 0$

P.R.: Se  $w \in \Sigma^*$  e  $x \in \Sigma$  allora  $|wx| = |w| + 1$

E.S.: L'insieme delle parole palindromi su  $\Sigma = \{a, b\}$

P.B.:  $a, b, \lambda$  sono palindromi

P.R.: Se  $w$  è palindromo, allora  $awa$  e  $bwb$  sono pal.

Un albero radicato è un albero contenente una radice:

P.B.: Un singolo vertice  $\tau$  è un albero radicato

P.R.: Supponiamo che  $T_1, T_2, \dots, T_m$  siano alberi radicati disgiunti con radice  $\tau_1, \tau_2, \dots, \tau_m$ . Allora il grafo formato dalla radice  $\tau$  ottenuto connettendo con un arco  $\tau$  a ciascun  $\tau_1, \dots, \tau_m$  è anch'esso un albero radicato

Un albero binario pieno è un albero radicato in cui  
ciascun vertice ha 2 oppure 0 figli, detti figlio dx e sx.

P.B.: Un singolo vertice è un all. bin. pieno

P.R.: Se  $T_1$  e  $T_2$  sono all. bin. pieni allora l'albero  $T$   
ottenuto connettendo la radice  $z$  alle radici  $c_1$  e  $c_2$   
tramite un arco è a sua volta un all. bin. pieno

E.S.

Def. ric.  $L$ , insieme delle stringhe su  $\Sigma = \{a, b\}$  che iniziano  
per  $a$

P.B.:  $a \in L$

P.R.: Se  $w \in L$ , allora  $wa \in wb \in L$

Def. ric.  $L$ , insieme delle stringhe su  $\Sigma = \{a, b\} =$

~~se~~  $w = aw'$ ,  $w' \in \{a, b\}^*$ ,  $|w'| = 2h$ ,  $h \geq 0$

"Stringhe di lunghezza pari che iniziano per a"

P.B.:  $aa, ab \in L$

P.R.: Se  $w \in L$ , allora  $waa, wab, wba, wbb \in L$

Def. ric.  $L := \{a^{m+2}b^{2m+2} \in \Sigma^* \mid m \in \mathbb{N}\}$ ,  $\Sigma = \{a, b\}$

P.B. ( $m=0$ ):  $aab \in L$

P.R.: Se  $w \in L$ , allora  $awb \in L$

E.S.

P.B.:  $(1, 1, 1) \in S$

P.R.: Se  $(x, y, z) \in S$ , allora  $(x+1, y+1, z+1) \in S$

Tramite ind. str. dim. che  $V(x, y, z) \in S$  mi ha  $x+y+z$  mult. di 3

P.B.:  $(x, y, z) = (1, 1, 1) \Rightarrow x+y+z = 1+1+1 = 3 \quad \checkmark$

P.I.: Supp. per ip. che  $P((x, y, z))$  sia vera

$$P((x+1, y+1, z+1)) \Rightarrow x+1+y+1+z+1 = (x+y+z)+3 =$$

$$= 3k+3 = 3(k+1)$$

$\checkmark$

Relazione di ricorrenza = def. ric. di una sequenza

Data una sequenza  $a_0, a_1, \dots, a_m$  una relazione di ricorrenza esprime  $a_m$  in termini di uno o più dei termini precedenti della sequenza.

ES.: La sequenza geometrica  $b, bz, bz^2, bz^3, \dots, bz^n, \dots$   
 $a_0 = b$  (condizione iniziale)  
 $a_m = a_{m-1} \cdot z$  (relazione)

Problema: data la relazione e la cond. iniz., si risolva una relazione quando si trova una formula chiusa per l' $m$ -esimo termine (non dipende più da precedenti)

Precedente esercizio:  $a_m = b z^m$

In informatica, si cercano le soluzioni quando già effettuata l'analisi degli algoritmi recursive, infatti queste relazioni esprimono la complessità asintotica

ES.: int fattoriale (n)

```
if (n == 1) return 1;  
return n * fattoriale (n-1);
```

$$T(n) = T(n-1) + a \quad b = \text{costo di return 1}$$

$$T(1) = b \quad a = \text{costo operazione per effettuare } n \cdot \text{fatt}(n)$$

Ci sono 2 metodi per giungere ad una soluzione / sostituzione ed iterazione / con cui determinare soluzioni esatte e limiti.

Iterazione (esplicitare fino al caso base)

$$T(n) = T(n-1) + a \quad T(1) = b$$

$$T(n) = T(n-1) + a$$

$$= T(n-2) + a + a$$

$$= T(n-1) + \underbrace{a+a+\dots+a}_K$$

$$= T(1) + \underbrace{a+a+\dots+a}_{n-1} \rightarrow b + (n-1) \cdot a$$

Le iterazioni si fermano quando arriva alla cond. iniz.

$$Es.: Sia m paro \quad T(m) = 2T(m-2) + 3 \quad T(6) = ?$$

$$T(m) = 2T(m-2) + 3$$

$$= 2(2T(m-4) + 3) + 3$$

$$= 2^2 T(m-4) + 2 \cdot 3 + 3$$

$$= 2^2 (2T(m-6) + 3) + 2 \cdot 3 + 3$$

$$= 2^3 T(m-6) + 2^2 \cdot 3 + 2 \cdot 3 + 3$$

$$= 2^K T(m-2K) + 2^{K-1} \cdot 3 + 2^{K-2} \cdot 3 + \dots + 3$$

$$= 2^{m/2} T(0) + 2^{\frac{m}{2}-1} \cdot 3 + 2^{\frac{m}{2}-2} \cdot 3 + \dots + 3$$

$$= 2^{m/2} + 3 \sum_{i=0}^{\frac{m}{2}-1} 2^i$$

$$= 2^{m/2} + 3(2^{m/2-1+1} - 1) = 4 \cdot 2^{m/2} - 3$$

$$Es.: Sia 2^K = m \quad T(m) = T(m/2) + 1 \quad T(2) = ?$$

$$T(m) = T(m/2) + 1$$

$$= (T(m/2^2) + 1) + 1$$

$$= T(m/2^2) + 2$$

$$= T(m/2^3) + 3$$

$$= T(m/2^K) + K$$

$$= T(1) + K = 1 + K = 1 + \log_2 m$$

Es.: Poiché rischierere la relazione su Fibonacci, studiamo 2 diseguaglianze per limitarla:

$$\text{I } T(m) \leq 2(T(m-1))$$

$$\left[ T(2) = 1 \quad \wedge \quad T(1) = 2 \right]$$

$$\leq 2 \cdot 2T(m-2)$$

$$\leq 2 \cdot 2 \cdot 2T(m-3) = 2^3 T(m-3)$$

$$\leq 2^K \cdot T(m-K)$$

$$\leq 2^{m-2} (T(1)) = 2^{m-1}$$

$$T(m) \leq 2^{m-1}$$

Stop quando

$$m-K=1 \Rightarrow K=m-2$$

$$\text{II } T(m) \geq 2T(m-2)$$

$$\geq 2 \cdot 2 T(m-2-2)$$

Stop quando

$$\geq 2^3 T(m-3 \cdot 2)$$

$$m-K-2=2 \Rightarrow K=(m-2)/2$$

$$\geq 2^K T(m-K \cdot 2)$$

$$\geq 2^{\frac{m-2}{2}} T(2) = 2^{\frac{m-2}{2}}$$

$$T(m) \geq 2^{\frac{m-2}{2}}$$