METODI MATEMATICI PER L'INFORMATICA

D'ANGELO CARMINE

LOGICA PROPOSIZIONALE

Linguaggio comune

Nel linguaggio comune si utilizzano spesso frasi imprecise o ambigue: *Un americano muore di melanoma ogni ora*, questa affermazione è assurda perché significa che c'è un' americano che ogni ura muore di melanoma. È corretta invece: *Ogni ora, un americano muore di melanoma*. Un espressione ambigua può essere: *L'uomo vedeva la donna con il binocolo;* chi ha il binocolo? Non ci è dato saperlo.

Linguaggio matematico

Nel linguaggio matematico si richiede certezza in un'affermazione. Richiede soprattutto che sia possibile determinare se un'affermazione sia vera o falsa.

Esempio:
Dire quale delle seguenti affermazioni sono vere e quali sono false:

- 2 è un numero primo VERA
- non ci sono numeri primi al di fuori di 2 FALSA
- quando piove apro l'ombrello VERA

Proposizione

Una **proposizione** è una frase che dichiara un fatto e che può essere vera (T) o può essere falsa (F) ma non può essere entrambe.
Alcuni esempi:

- Come stai? : Una domanda non una proposizione
- x+5 =3 : x non è specificato => non è né T né F
- 2 è un numero primo : T
- Lei ha molto talento : Lei non è specificato => non è né T né F
- Ci sono altre forme di vita su altri pianeti dell'universo : Può essere T o F

Proposizione composte

Una proposizione più complessa può essere costruita attraverso proposizioni elementari connesse attraverso proposizioni elementari connesse attraverso connettivi logici:

- Negazione
- Congiunzione
- Disgiunzione
- Or esclusivo
- Implicazione
- Bicondizione (o Equivalenza)

Negazione

Sia p una proposizione. La frase "non è vero che p" è un'altra proposizione, chiamata la **negazione di p**. La negazione di p è denotata con **¬p** e si legge non p.
Esempio:

- Salerno è una città della Campania:
  - Non è vero che Salerno è una città della Campania.
  - Salerno non è una città della Campania.

Il valore della negazione di p cioè di ¬p è l'opposto del valore di p. La tabella di verità risultate è la seguente:

p	**¬p**
T	**F**
F	**T**

Congiunzione

Siano p e q proposizioni. La frase "p e q" è una proposizione detta congiunzione di p e q. La congiunzione di p e q è denotata con p ^ q. p ^ q è vera se entrambe p e q sono vere, altrimenti è falsa.
Esempi:

- Salerno è una città della Campania e 5 + 2 = 8
- Oggi piove e 2 + 5 ≠ 3.

Il valore della congiunzione p ^ q è vero se entrambe p e q sono vere, altrimenti è falso. La tabella della verità risultante sarà:

p	**q**	**p ^ q**
T	T	**T**
F	T	**F**
T	F	**F**
F	F	**F**

Disgiunzione

Siano p e q proposizioni. La frase "p o q" è detta disgiunzione di p e q. La disgiunzione di p e q è denotata con p v q. p v q è falsa se entrambe p e q sono false, altrimenti è vera.
Esempio:

- Salerno è una città della Campania o 5+2=8.
- Oggi piove o 2+5 ≠ 3.

Il valore della disgiunzione p v q è vero se p, q o entrambe sono vere:

p	**q**	**p v q**
T	T	**T**
F	T	**T**
T	F	**T**
F	F	**F**

Disgiunzione esclusiva (Or esclusivo)

Siano p e q proposizioni. L'or esclusivo di p e q è denotato con p⊕q. Dove p⊕q è vero quando esattamente uno tra p e q sono veri, altrimenti è falso.
Esempio:

- Nel menù a prezzo fisso di un ristorante: frutta o formaggio.

Il valore dell'or esclusivo $p \oplus q$ è vero se esattamente una tra p e q è vera.

p	**q**	**p⊕q**
T	T	**F**
F	T	**T**
T	F	**T**
F	F	**F**

Implicazione

Siano p e q proposizioni. La proposizione "p implica q" è chiamata implicazione. Essa è denotata con p q (talvolta anche con p => q) $p \rightarrow q$ è falsa quando p è vera e q è falsa, altrimenti è vera. p è chiamata ipotesi e q è chiamata conclusione.

La proposizione $p \rightarrow q$ può essere letta in molti modi equivalenti:

- se p allora q
- p solo se q
- p è sufficiente per q
- q è necessaria per p
- q ogniqualvolta p

condizione sufficiente → condizione necessaria

Il valore dell'implicazione $p \rightarrow q$ è falsa solamente se la verità di p implica la falsità di q. Quindi la tabella di verità risultante sarà:

p	**q**	**p→q**
T	T	**T**
F	T	**T**
T	F	**F**
F	F	**T**

Esercizio: Partendo da questa preposizione composta: Se ho la febbre allora sono ammalato, definire se tutte le situazioni che si possono presentare siano vere o false:

- Se ho la febbre allora sono ammalato **Vero**
- Se ho la febbre allora non sono ammalato **Falso**
- Se non ho la febbre allora sono ammalato **Vero**
- Se non ho la febbre allora non sono ammalato **Vero**

Esercizio: Supponete che abbia estratto una carta da un mazzo e vi dica: Se è una carta di cuori allora è una regina

In quali casi ho mentito?

- Se è una carta di cuori ed è una regina **Vero**
- Se è una carta di cuori ed è un re **Falso**
- Se è una carta di picche ed è una regina **Vero**
- Se è una carta di picche ed è un re **Vero**

Proposizioni condizionali derivanti dall'implicazione

L'inverso di p → q è q → p

Esempio: *se nevica allora le auto procedono lentamente*. p = nevica   q = le auto procedono lentamente, quindi p → q. L'inverso sarà : *se le auto procedono lentamente allora nevica*.
La tabella di verità risultante sarà:

p	**q**	**p→q**	**q**	**p**	**q → p**
T	T	**T**	T	T	**T**
F	T	**T**	F	T	**T**
T	F	**F**	T	F	**F**
F	F	**T**	F	F	**T**

L'opposto di p → q è ¬p → ¬q

Esempio: Esempio: *se nevica allora le auto procedono lentamente*. p = nevica   q = le auto procedono lentamente, quindi p → q. L'opposto sarà: *se non nevica allora le auto procedono velocemente*.
La tabella di verità risultante sarà:

p	**q**	**p→q**	**¬p**	**¬q**	**¬p → ¬q**
T	T	**T**	F	F	**T**
F	T	**T**	T	F	**F**
T	F	**F**	F	T	**T**
F	F	**T**	T	T	**T**

Il contronominale di p → q è ¬q → ¬p (opposto dell'inversa)

Esempio: Esempio: *se nevica allora le auto procedono lentamente*. p = nevica   q = le auto procedono lentamente, quindi p → q. Il contronominale sarà: se le auto procedono velocemente allora non nevica.
La tabella di verità risultante sarà:

p	**q**	**p→q**	**¬q**	**¬p**	**¬q → ¬p**
T	T	**T**	F	F	**T**
F	T	**T**	F	T	**T**
T	F	**F**	T	F	**F**
F	F	**T**	T	T	**T**

Bicondizone (o equivalenza)

Siano p e q proposizioni. La proposizione "p se e solo se q" è chiamata bicondizione (o equivalenza). Essa è denotata con p↔q (talvolta anche con p <=> q) p↔q è vera quando p e q hanno lo stesso valore di verità, altrimenti è falsa.
La proposizione p↔q può essere letta in molti modi diversa:

- Se p allora q, e viceversa
- p iff q
- p è necessaria e sufficiente per q

Esempio: *Puoi prendere l'aereo se e solo se hai comprato il biglietto*

- Vera se sono entrambe vere oppure entrambe false:
  - *Se puoi prendere l'aereo e hai comprato il biglietto*
  - *Se non puoi prendere l'aereo e non hai comprato il biglietto*
- Falsa se hanno valori opposti:
  - *Se puoi prendere l'aereo e non hai comprato il biglietto*
  - *Se non puoi prendere l'aereo e hai comprato il biglietto*

Il valore dell'equivalenza p↔q è vera solamente se I valori di verità di p e q coincidono.

p	**q**	**p↔q**
T	T	**T**
F	T	**F**
T	F	**F**
F	F	**T**

Possiamo notare che p↔q ha gli stessi valori di verità di (p → q)^(q → p)

p	**q**	**p→q**	**q → p**	**(p → q)^(q → p)**	**p↔q**
T	T	T	T	**T**	**T**
F	T	T	F	**F**	**F**
T	F	F	T	**F**	**F**
F	F	T	T	**T**	**T**

Esercizi: p = 2 è un numero primo = T e q = 6 è un numero primo = F, indicare il valore di verità delle seguenti proposizioni composte:

¬p = **F**; ¬q = **T**; p ^ q = **F**; p ^ ¬q = **T**; p v q = **T**;
p⊕q = **T**; p → q = **F**;q → p = **T**; p↔q = **F**

Esercizio: Costruire la tabella di verità per la seguente espressione: (p → q)^(¬p↔q)

p	**q**	**¬p**	**p → q**	**¬p↔q**	**(p → q)^(¬p↔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**

APPLICAZIONI DELLA LOGICA PROPOSIZIONALE

Rappresentazione di T e F in un computer

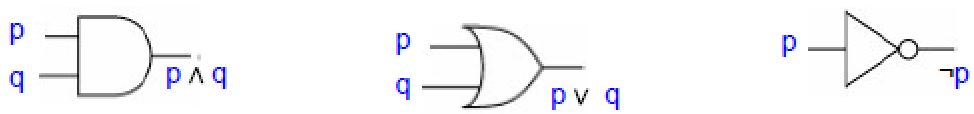
In un computer le informazioni sono memorizzate con 1 e 0, nella logica si utilizza invece vero e falso; per poter rappresentare quindi quest'ultimi è sufficiente un bit 1 (vero) e un bit 0 (falso). Quindi possiamo dire che una variabile booleana può corrispondere ad una proposizione.
Nelle operazione bit a bit T e F sono sostituite con 1 e 0, la tabella di verità risultante sarà:

p	**q**	**p^q**	**p v q**
1	0	0	1
1	1	1	1
0	0	1	0
0	1	0	1

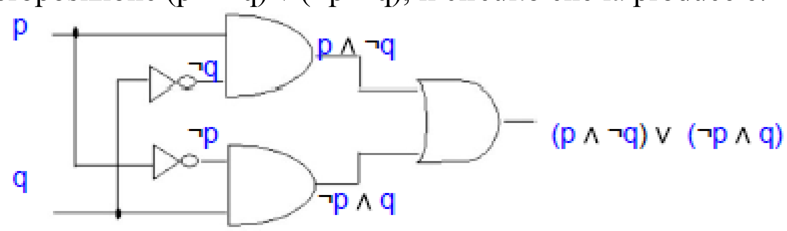
Logica proposizionale per la progettazione di circuiti logici

Porte:

AND **OR** **NOT**



Data la proposizione (p ^ ¬q) v (¬p ^ q), il circuito che la produce è:



Traduzione di frasi di un linguaggio comune in proposizioni logiche

Supponiamo di considerare la seguente frase: **Se hai più di 12 anni o sei accompagnato dai tuoi genitori allora puoi salire su quella giostra.**
Per trasformarla in una proposizione logica la prima cosa da fare è di analizzare la frase alla ricerca di un connettivo logico: Se (**hai più di 12 anni** o **sei accompagnato dai tuoi genitori**)
allora (**puoi salire su quella giostra**), a questo punto possiamo assegnare a delle variabili le proposizioni logiche trovate:

- a = hai più di 12 anni
- b = sei accompagnato dai tuoi genitori
- c = puoi salire su quella giostra

La sua traduzione logica sarà: (a v b) → c

Di seguito sarà descritta una regola generale per individuare questo processo:
Regola generale: Individua nella frase le parole chiave che corrispondono ai connettivi logici ed usa essi per identificare le proposizioni elementari.
Esempio: Puoi avere caffè gratis se sei maggiorenne ed è martedì
L'algoritmo da eseguire è il seguente:

1. individua i connettivi logici: Puoi avere caffè gratis ***se*** sei maggiorenne ***ed*** è martedì
2. identifica le preposizioni elementari: $\underbrace{\text{Puoi avere caffè gratis}}_{a}$ ***se*** $\underbrace{\text{sei maggiorenne}}_{b}$ ***ed*** $\underbrace{\text{è martedì}}_{c}$
3. riscrivi la frase come una proposizione logica: $(b \wedge c) \rightarrow a$.

Esercizio:
Si assuma di avere le seguenti proposizioni elementari:
p = Tu guidi a più di 130 km/h q = Prendi la multa
Tradurre ciascuna delle seguenti frasi:

- Tu non guidi a più di 130 km/h = **¬p**
- Tu guidi a più di 130 km/h, ma non prendi la multa = **p ^ ¬q**
- Se non guidi a più di 130 km/h allora non prendi la multa = **¬p → ¬q**
- Guidare a più di 130 km/h è sufficiente per prendere una multa = **p → q**
- Prendi la multa, ma non guidi a più di 130 km/h = **q ^ ¬p**

EQUIVALENZE PROPOSIZIONALI

Nel ragionamento matematico riveste un ruolo importante la possibilità di sostituire una asserzione (proposizione) con un'altra avente gli stessi valori di verità.

Alcuni tipi di proposizioni:

Alcune proposizioni sono interessanti poiché i loro valori nella tabella di verità sono sempre gli stessi.

- Tautologia

La **tautologia** è una proposizione composta che è sempre vera per tutti i possibili valori delle proposizioni elementari che la compongono:

p v ¬p è una tautologia =

p	**¬p**	**p v ¬p**
T	F	**T**
F	T	**T**

- Contraddizione

Una **contraddizione** è una proposizione composta che è sempre falsa per tutti i possibili valori delle proposizioni elementari che la compongono:

p ^ ¬p è una contraddizione =

p	**¬p**	**p ^ ¬p**
T	F	**F**
F	T	**F**

- Contingenza

Una contingenza è una proposizione composta che non è né una tautologia né una contraddizione.

Equivalenze logiche

Le proposizioni p e q sono dette logicamente equivalenti se hanno gli stessi valori di verità (o equivalentemente se $p \leftrightarrow q$ è una tautologia). La notazione $p \equiv q$ denota che p e q sono logicamente equivalenti.

Esempio: $p \rightarrow q$ è equivalente a $\neg q \rightarrow \neg p$

p	**q**	**¬q**	**¬p**	**p → q**	**¬q → ¬p**
T	T	F	F	**T**	**T**
T	F	T	F	**F**	**F**
F	T	F	T	**T**	**T**
F	F	T	T	**T**	**T**

Quindi le proposizioni composte logicamente e equivalenti hanno lo stesso valore di verità per tutti i possibili casi. È così possibile:

- Sostituire l'una con l'altra
- Utilizzare una qualunque di esse in un ragionamento logico
- Ottenere nuove proposizioni

Per verificare l'equivalenza si usa la tabella di verità.

Importanti equivalenze logiche

- Leggi di De Morgan

1) $\neg(p \vee q) \equiv \neg p \wedge \neg q$

dim:

p	**q**	**¬p**	**¬q**	**¬(p v q)**	**¬p ^ ¬q**
T	T	F	F	**F**	**F**
T	F	F	T	**F**	**F**
F	T	T	F	**F**	**F**
F	F	T	T	**T**	**T**

2) $\neg(p \wedge q) \equiv \neg p \vee \neg q$

dim:

p	**q**	**¬p**	**¬q**	**¬(p ^ q)**	**¬p v ¬q**
T	T	F	F	**F**	**F**
T	F	F	T	**T**	**T**
F	T	T	F	**T**	**T**
F	F	T	T	**T**	**T**

Un esempio di negazione utilizzando le leggi di De Morgan è il seguente:
Prendiamo in esame la frase: *L'estate in Messico è calda ed assolata.*
Notiamo subito che la frase è composta da due connettivi logici:
Usando De Morgan sulla frase abbiamo che:
L'estate in Messico non è calda o non è assolata.

Altre importanti equivalenze logiche

- Identità

- p ^ T ≡ p **dim:**

p	T	p ^ T
T	T	**T**
F	T	**F**

- p v F ≡ p **dim:**

p	F	p v F
T	F	**T**
F	F	**F**

- Idempotenza

- p v p ≡ p **dim:**

p	p	p v p
T	T	**T**
F	T	**F**

- p ^ p ≡ p **dim:**

p	p	p ^ p
T	T	**T**
F	T	**F**

- Doppia negazione

- ¬(¬p) ≡ p **dim:**

p	¬p	¬(¬p)
T	F	**T**
F	T	**F**

- Dominazione

- p v T ≡ T **dim:**

p	T	p v T
T	T	**T**
F	T	**T**

- p ^ F ≡ F **dim:**

p	F	p ^ F
T	F	**F**
F	F	**F**

- Commutativa

- p v q ≡ q v p **dim:**

p	q	p v q	q v p
T	T	**T**	**T**
T	F	**T**	**T**
F	T	**T**	**T**
F	F	**F**	**F**

- p ^ q ≡ q ^ p **dim:**

p	q	p ^ q	q ^ p
T	T	**T**	**T**
T	F	**F**	**F**
F	T	**F**	**F**
F	F	**F**	**F**

- Associativa

- (p v q) v r ≡ p v (q v r)

dim:

p	q	p v q	r	q v r	(p v q) v r	p v (q v r)
T	T	T	T	T	**T**	**T**
T	F	T	F	F	**T**	**T**
F	T	T	T	T	**T**	**T**
F	F	F	F	F	**F**	**F**

- (p ^ q) ^ r ≡ p ^ (q ^ r)

dim:

p	q	p ^ q	r	q ^ r	(p ^ q) ^ r	p ^ (q ^ r)
T	T	T	T	T	**T**	**T**
T	F	F	F	F	**F**	**F**
F	T	F	T	T	**F**	**F**
F	F	F	F	F	**F**	**F**

- Distributiva

- p ∨ (q ∧ r) ≡ (p ∨ q) ∧ (p ∨ r)

dim:

p	q	r	q ∧ r	p ∨ (q ∧ r)	p ∨ q	p ∨ r	(p ∨ q) ∧ (p ∨ r)
T	T	T	T	**T**	T	T	**T**
T	F	F	F	**T**	T	T	**T**
F	T	T	T	**T**	T	T	**T**
F	F	F	F	**F**	F	F	**F**

- p ∧ (q ∨ r) ≡ (p ∧ q) ∨ (p ∧ r)

dim:

p	q	r	q v r	p ^ (q v r)	p ^ q	p ^ r	(p ^ q) v (p ^ r)
T	T	T	T	**T**	T	T	**T**
T	F	F	F	**F**	F	F	**F**
F	T	T	T	**F**	F	F	**F**
F	F	F	F	**F**	F	F	**F**

- Altre utili equivalenze

- p ∨ ¬p ≡ T **dim:**

p	¬p	p v ¬p
T	F	**T**
F	T	**T**

- **p** ∧ ¬p ≡ F **dim:**

p	¬p	p ^ ¬p
T	F	**F**
F	T	**F**

- **p** → q ≡ (¬p ∨ q) **dim:**

p	q	¬p	p → q	¬p v q
T	T	F	**T**	**T**
T	F	F	**F**	**F**
F	T	T	**T**	**T**
F	F	T	**T**	**T**

- p ⊕ q ≡ (p ∧ ¬q) ∨ (¬p ∧ q) **dim:**

p	q	p ⊕ q	¬p	¬q	p ^ ¬q	¬p ^ q	(p ∧ ¬q) ∨ (¬p ∧ q)
T	T	**F**	F	F	F	F	**F**
T	F	**T**	F	T	T	F	**T**
F	T	**T**	T	F	F	T	**T**
F	F	**F**	T	T	F	F	**F**

- p ↔ q ≡ (p → q) ∧ (q → p) **dim:**

p	q	p ↔ q	(p → q)	(q → p)	(p → q) ∧ (q → p)
T	T	**T**	T	T	**T**
T	F	**F**	F	T	**F**
F	T	**F**	T	F	**F**
F	F	**T**	T	T	**T**

Esercizio:
Dimostrare che (p ^ q) → p è una tautologia.
Quindi abbiamo che dobbiamo dimostrare la proposizione: ((p ^ q) → p) ≡ T.
Svolgimento:
(p ^ q) → p ≡ ¬ (p ^ q) v p ← svolgimento dell'implicazione
≡(¬p v ¬q) v p ← De Morgan
≡(¬q v ¬p) v p ← commutatività
≡¬q v (¬p v p) ← associatività
≡¬q v T ← ¬p v p è uguale a T sia quando p = T, sia quando p = F
≡T
Dimostrazione via tavola della verità:

p	q	p ^ q	(p ^ q) → p
T	T	T	**T**
T	F	F	**T**
F	T	F	**T**
F	F	F	**T**

Regole di precedenza degli operatori

Abbiamo visto nelle espressioni composte l'uso di parentesi. Esse specificano l'ordine in cui gli operatori logici vanno applicati. Per esempio: (p v q) ^ (¬r) è la congiunzione di (p v q) e (¬r).
Per ridurre il numero di parentesi si stabilisce una convenzione sulla precedenza degli operatori.
Di seguito sono elencate le precedenze degli operatori:

Legenda : > = precede (priorità maggiore). **¬ > ^ > V > ⟶ > ⟷**
Esempio: (p v q) ^ (¬r) può essere scritta anche (p v q) ^ ¬r, ma può essere scritta anche senza ambiguità: p ^ q v ¬r.

Esercizi:
- mostrare che il contronominale di p → q è equivalente a p → q.
Quindi che: $(\neg q \rightarrow \neg p) \equiv (p \rightarrow q)$.
Dim:

$$
\begin{aligned}
(\neg q \rightarrow \neg p) &\equiv q \vee \neg p && \text{svolgo l'implicazione} \\
&\equiv \neg p \vee q && \text{commutatività} \\
&\equiv p \rightarrow q && \text{ritorno all'implicazione}
\end{aligned}
$$

- mostrare che $\neg (p \rightarrow q) \equiv (p \wedge \neg q)$.
Dim:

$$
\begin{aligned}
\neg (p \rightarrow q) &\equiv \neg(\neg p) \vee q && \text{doppia negazione} \\
&\equiv p \vee \neg q && \text{svolgo l'implicazione} \\
&\equiv \neg q \vee p && \text{commutatività} \\
&\equiv q \rightarrow p && \text{ritorno all'implicazione}
\end{aligned}
$$

- mostrare che l'opposto di p → q è equivalente all'inverso di p → q.
Quindi che $\neg p \rightarrow \neg q \equiv q \rightarrow p$.
Dim:

$$
\begin{aligned}
\neg p \rightarrow \neg q &\equiv \neg(p) \vee (\neg q) && \text{doppia negazione} \\
&\equiv p \vee \neg q && \\
&\equiv \neg q \vee \neg p && \text{commutatività} \\
&\equiv q \rightarrow p && \text{ritorno all'implicazione}
\end{aligned}
$$

PREDICATI E QUANTIFICATORI

Limiti della logica proposizionale

Logica proposizionale: il mondo è descritto attraverso proposizioni elementari e loro combinazioni logiche. I singoli oggetti cui si riferiscono le proposizioni o le proprietà di tali oggetti enunciati nelle proposizioni **non** hanno identificazione nella logica proposizionale.
Esempio: *Giovanni* è *uno studente dell'Università di Salerno*, non si può esprimere in logica proposizionale.

Infatti nella logica proposizionale ciascuna delle proposizioni deve essere ripetuta esaustivamente, cioè le asserzioni devono essere ripetute per oggetti diversi.
Un esempio è: *Se Giovanni è laureato in Informatica allora ha sostenuto l'esame di MMI.*
Tradotta sarebbe: Giovanni è laureato in informatica → ha sostenuto l'esame di MMI.
Questa frase può essere ripetuta infinite volte cambiando il nome Giovanni con un altro:

- Carmine è laureato in informatica → ha sostenuto l'esame di MMI
- Emanuele è laureato in informatica → ha sostenuto l'esame di MMI
- Francesco è laureato in informatica → ha sostenuto l'esame di MMI
- ecc.

Il problema è quindi di snellire la ripetizione esaustiva.
La soluzione la si ha costruendo le proposizioni con le variabili:
x *è laureato in Informatica →* ***x*** *ha sostenuto l'esame di MMI*

Le asserzioni definiscono una proprietà per un gruppo di oggetti.
Esempio:

- Tutte le auto nuove devono essere immatricolate
- Qualche laureato in Informatica si laurea con lode

Il problema è quindi come esprimere le proprietà di gruppo.
La soluzione è di usare i quantificatori:

- **Quantificatori universali:** la proprietà è soddisfatta per tutti i membri del gruppo.
- **Quantificatori esistenziali:** almeno un membro del gruppo soddisfa la proprietà.

Logica predicativa

Per rimediare alle limitazioni della logica proposizionale si usa la logica predicativa:

- Modella in maniera esplicita gli oggetti e le loro proprietà (chiamate predicati)
- Permette di costruire asserzioni con variabili e quantificatori.

La logica predicativa è composta da alcuni elementi fondamentali:

- **costante:** modella uno specifico oggetto (Giovanni, Salerno, 7, ecc.)
- **variabile:** rappresenta un oggetto di un tipo specificato. Il tipo è definito stabilendo un *universo del discorso*. (x, y possono essere persone, studenti, numeri)
- **predicato:** rappresenta la proprietà o le relazione tra gli oggetti.
  Esempio: x è più grande di 3
  P = è più grande di 3   è il predicato
  x è più grande di 3   sarà denotata con P(x)
  Il predicato può essere relativo anche a più di un oggetto (sposati(Giovanni, Maria)).

Predicati

Un predicato rappresenta la proprietà o le relazioni tra gli oggetti. Un predicato P(x) assume un valore Vero o Falso in dipendenza del fatto che la proprietà P vale o meno per x. La variabile x è un ogetto preso dall'universo del discorso.
Esempio: consideriamo il predicato Studenti(x) dove l' universo del discorso sono le persone:

- Studente(Giovanni) **T** se Giovanni è uno studente
- Studente(Anna) **T** se Anna è uno studente
- Studente(Nicola) **F** se Nicola non è uno studente

Esercizio: Sia P(x) un predicato che rappresenta l'asserzione: ***x è un numero primo***.
Quali soni i valori di verità per i seguenti valori di x: 2, 3, 4, 5, 6, 7.
P = è un numero primo.
P(2) = **T**, P(3) = **T**; P(4) = **F**; P(5) = **T**; P(6) = **F**; P(7) = **T**.
Posiamo dire che tutte le asserzioni P(2), P(3), P(4), P(5), P(6), P(7) sono proposizioni. Ma P(x) non lo è una proposizione perché P(x) è applicabile a più oggetti e quindi può assumere valori diversi.

Sappiamo anche che i predicati possono avere più argomenti, e che rappresenta la relazione tra gli argomenti (oggetti).

- Piu_vecchio(Giovanni, Pietro) - denota l'asserzione Giovanni è più vecchio di Pietro. È una proposizione perché è vera o falsa.
- ꝏ Piu_vecchio(x, y) - denota l'asserzione x è più vecchio di y. Non è una proposizione, ma la diventa dopo aver sostituto alle variabili i valori.

Asserzioni composte nella logica predicativa

Le asserzioni composte sono ottenute attraverso connettivi logici.
Esempio:

- $Studente(Giovanni) \wedge Studente(Anna)$
  - Traduzione: Sia Giovanni che Anna sono studenti
  - Proposizione: **SI**
- Città(Arno) Fiume(Arno)
  - Traduzione: L'Arno è un fiume o una città
  - Proposizione: **SI**
- $MMI(x) \rightarrow Matricola(x)$
  - Traduzione: Se x segue il corso di MMI allora x è una matricola
  - Proposizione: **NO**

Logica predicativa versus logica proposizionale

Logica proposizionale: utilizza asserzioni che descrivono proprietà di oggetti ben definiti (proposizioni)
Logica predicativa: consente di utilizzare asserzioni valide per più oggetti (predicati). Permette di *quantificare le asserzioni*, consente di fare asserzioni riguardanti gruppi di oggetti (quantificatori).

Asserzioni quantificate

La logica predicativa consente di fare asserzioni riguardanti gruppi di oggetti.
Per far questo vengono utilizzate asserzioni quantificate:

- **universale:** esempio: "Tutti gli studenti di MMI sono iscritti ad Informatica". L'asserzione è vera per tutti gli studenti di MMI.
- **Esistenziale:** esempio: "Alcuni studenti di Informatica si laureano con lode". L'asserzione è vera per alcuni studenti di Informatica.

Quantificatore universale

La quantificazione universale di P(x) è l'asserzione: P(x) è vera per tutti i valori di x nel dominio (universo del discorso).
La notazione $\forall x \, P(x)$ denota la quantificazione universale di P(x),
ed è espressa dicendo per ogni x P(x) è vera.
Esempio:
Supponiamo che P(x) denoti $x > x - 1$
Quale è il valore di verità di x P(x) se assumiamo che il dominio sia l'insieme di tutti i numeri reali R?
Risposta: poiché il numero reale x è più grande di se stesso diminuito di 1, abbiamo $\forall x \, P(x)$ è vera.

Esempio:

- $MMI(x) \rightarrow Matricola(x)$: traduzione: Se x segue il corso di MMI allora x è una matricola; non è una proposizione.
- $\forall x \, (MMI(x) \rightarrow Matricola(x))$:
  - Il dominio di x = persone
  - Traduzione: Se una persona segue il corso di MMI allora è una matricola
  - Proposizione: SI

La quantificazione converte una funzione proposizionale (predicato) $P(x)$ in una proposizione poiché fissa il valore di $P(x)$ per variabili prese da un insieme ben definito.

Esempio:
Supponiamo che $P(x)$ denoti ≥ 0.

- $P(x)$ è una proposizione? No perché può assumere molti valori diversi.
- $\forall x\ P(x)$ è una proposizione? Si perché il valore di $\forall x\ P(x)$ è ben definito:
  - è **vero** se $P(x)$ è vero per ogni x nel dominio
  - è **falso** se esiste un valore di x per cui $P(x)$ risultato falso.

Nell'utilizzo del quantificatore è importante definire esattamente il dominio (l'universo del discorso).
Esempio:
Supponiamo che $P(x)$ denoti ≥ 0.
Quale il valore di $\forall x\ P(x)$?

- Assumiamo che il dominio sia l'insieme dei numeri interi ($Z = \{ \ldots, -1, 0, 1, 2, \ldots \}$).
  $\forall\ x \in Z\ P(x)$ è falsa perché abbiamo che per $P(-1)$ abbiamo $x < 0$.
- Assumiamo invece che il dominio sia l'insieme dei numeri naturali ($N = \{0, 1, 2, \ldots\}$).
  $\forall\ x \in N\ P(x)$ è vera perché abbiamo $P(1) = T$, $P(2) = T$, ecc.

Un elemento x del dominio per il quale $P(x)$ è falsa è detto controesempio di $\forall x\ P(x)$. Per provare che un'asserzione che utilizza un quantificatore universale sia falsa basta individuare un controesempio.
Esempio: con $P(x)$ che denota $x \geq 0$ e con dominio l'insieme dei numeri interi Z, si ha che: $\forall\ x \in Z$ $P(x)$ = falsa.
La prova è data dell'esistenza di $x = -1$ per il quale abbiamo che $p(x)$ è falsa. Perché $-1 < 0$ e quindi è un controesempio per $\forall x\ P(x)$.

Quantificatore esistenziale
La quantificazione esistenziale di $P(x)$ è l'asserzione: Esiste un elemento x del dominio (universo del discorso) per il quale $P(x)$ è vera. La notazione $\exists x\ P(x)$ denota la quantificazione esistenziale di $P(x)$, ed è espressa dicendo esiste un x tale che $P(x)$ è vera.
Esempio 1:
Supponiamo che $P(x)$ denoti $x > 5$.
Il dominio utilizzato è l'insieme dei numeri reali R.
Quale è il valore di verità di $\exists x\ P(x)$?
Risposta: poiché è possibile trovare un numero reale maggiore di 5, per esempio $10 > 5$, abbiamo che $\exists x\ P(x)$ è vera.

Esempio 2:
Supponiamo che $Q(x)$ denoti $x = x+2$
Dominio: insieme dei numeri reali R
Quale è il valore di verità di $\exists x\ Q(x)$?
Risposta: poiché nessun numero reale è uguale a se stesso aumentato di 2, abbiamo che $\exists x\ P(x)$ è falsa.

Esempio 3:

- Laureato_Inf(x) Lode(x)
  - Traduzione: x è un laureato in Informatica e x si è laureato con lode
  - Proposizione: **NO**
- x Laureato_Inf(x) Lode(x)
  - Dominio: persone
  - Traduzione: C'è una persona che è un laureato in Informatica e che si è anche laureato con lode
  - Proposizione: **SI**

Sintesi delle asserzioni quantificate:

Asserzione	**Quando è vera?**	**Quando è falsa?**
$\forall x\ P(x)$	P(x) è vera per tutti gli x	C'è qualche x per il quale P(x) è falsa
$\exists x\ P(x)$	C'è qualche x per il quale P(x) è vera	P(x) è falsa per tutti gli x

Supponiamo che gli elementi del dominio possano essere enumerati, cioè essi siano $x_1, x_2, \ldots, x_n$ allora:

- $\forall x\ P(x)$ è vera se $P(x_1) \wedge P(x_2) \wedge \ldots \wedge P(x_n)$ è vera.
- $\exists x\ P(x)$ è vera se $P(x_1) \vee P(x_2) \vee \ldots \vee P(x_n)$ è vera.

Esercizi:

- Supponiamo che P(x) denoti $x^2 > 10$, il dominio è {1, 2, 3, 4}. Quale è il valore di verità di $\exists x\ P(x)$?
Risposta: $\exists x\ P(x)$ ha valore vero perché esiste una valore di P(x) il quale valore è vero ed è:
P(4) = 16 > 10. La disgiunzione è P(1) = F, P(2) = F, P(3) = F, P(4) = T. Quindi abbiamo P(1) v P(2) v P(3) v P(4) = F v F v F v T quindi è T.

Lo stesso esercizio ma usando il per ogni ($\forall x\ P(x)$) risulta falsa perché abbiamo P(1) come cotro esempio visto che P(1) = 1 > 10, che è falso.
La disgiunzione è P(1) = F, P(2) = F, P(3) = F, P(4) = T. Quindi abbiamo P(1) ^ P(2) ^ P(3) ^ P(4) = F ^ F ^ F ^ T quindi è F.

Traduzioni di frasi utilizzando i quantificatori

La formulazione di un asserzione nella logica predicativa dipende dal dominio:
Esempio 1: *Tutti gli studenti di Informatica sono simpatici*

- Dominio: studenti di Informatica
  simpatici = sono simpatici
  Traduzione : $\forall x$ simpatici(x)
- Dominio: studenti
  inf = di informatica, simpatici = sono simpatici
  $\forall x$ (inf(x) → simpatici(x))
- Dominio: persone
  stud = studente, inf = di informatica, simpatici = sono simpatici
  $\forall x$ (stud(x) ^ (inf(x) → simpatici(x))

Esempio 2: *Qualche studente di ingegneria è simpatico*

- Dominio: studenti di Ingegneria
  simpatico = è simpatico
  Traduzione: ∃x simpatico(x)
- Dominio: studenti
  ing = di ingegneria, simpatico = è simpatico
  Traduzione: x (ing(x) ^ simpatico(x))

Tipicamente, date due qualunque predicati S(x) e P(x):
Le asserzioni esistenziali infatti sono legate alle congiunzioni:

- Qualche S(x) è P(x): ∃x (S(x) ^ P(x))
- Qualche S(x) non è P(x) : ∃x (S(x) ^ ¬P(x))

Esempio: *Qualche italiano è vegano*

- Dominio: italiani
  Traduzione :∃x Vegano(x)
- Dominio: persone
  Traduzione: ∃x (Italiano(x) ^ Vegano(x))

Asserzioni matematica quantificate

La maggioranza dei teoremi ed asserzioni matematiche esprimono l'esistenza di un oggetto con una qualche proprietà o una proprietà valida per tutti gli oggetti.

Esempio 1:
$x^2+2x+1=0$ ha una radice reale
La natura esistenziale di questa asserzione è più esplicita se la si esprime come: esiste un numero reale x tale che $x^2+2x+1=0$. Considerando l'insieme dei numeri reali R come dominio, simbolicamente può essere espressa come: $\exists x\ (x^2+2x+1=0)$.

Esempio 2:
$\sqrt{2}$è un numero irrazionale
La natura esistenziale di questa asserzione è più esplicita se la si esprime come:
Non esistono due interi p e q tale che $\sqrt{2}=\frac{p}{q}$
Simbolicamente può essere espressa come: $\neg\left(\exists p\in Z,\ \exists q\in Z\left(\sqrt{2}=\frac{p}{q}\right)\right)$.

Esempio 3:
Il quadrato di un qualunque numero reale è maggiore o uguale a zero.
La natura universale di questa asserzione è più esplicita se la si esprime come
Ogni numero reale ha il quadrato maggiore o uguale a zero
Considerando l'insieme dei numeri reali R come dominio, simbolicamente può essere espressa come:
$\forall x\ (x^2 \geq 0\ )$.

Quantificatori innestati
Più di un quantificatore può essere necessario per rappresentare una qualche asserzione.
Esempio 1:
Ogni numero reale ha un corrispondente negativo.
Assumiamo che:
- il dominio sia l'insieme dei numeri reali R
- P(x, y) sia $x + y = 0$

Traduzione: $\forall x\ \exists y\ P(x, y)$

Esempio 2:
C'è una persona che ama tutti gli altri.
Assumiamo che:
- il domino sia l'insieme delle persone
- Ama(x, y) sia x ama y

Traduzione: $\exists x\ \forall y\ Ama(x, y)$

L'ordine dei quantificatori innestati è importante perché invertendoli il significato potrebbe essere completamente differente.
Esempio:
Un americano muore di melanoma ogni ora.
Muore(x, h) sia x muore nell'ora h, allora così come è scritta l'asserzione precedente è:
$\exists x\ \forall h\ Muore(x, h)$.
Mentre noi avevamo in mente: $\forall h\ \exists x\ Muore(x, h)$

Negazione di quantificatori
Niente è perfetto diventa: $\neg(\exists x\ Perfetto(x))$. Un altro modo per esprimere l'asserzione precedente è:
Ogni cosa è imperfetta: $\forall x\ \neg(Perfetto(x))$.
In conclusione possiamo dire che: $\neg(\exists x\ Perfetto(x))$ è equivalente a $\forall x\ \neg(Perfetto(x))$.

Negazione di asserzioni quantificate (Leggi di De Morgan per quantificatori)

Negazione	Asserzione equivalente
$\neg\forall x\ P(x)$	$\exists x\ \neg P(x)$
$\neg\exists x\ P(x)$	$\forall x\ \neg P(x)$

Proviamo che $\neg\forall x\ P(x)$ è equivalente a $\exists x\ \neg P(x)$.
Dim:
Dobbiamo provare che $\neg\forall x\ P(x) \rightarrow \exists x\ \neg P(x)$.
1. Cominciamo col provare che $\neg\forall x\ P(x) \rightarrow \exists x\ \neg P(x)$.
   Se $\neg(\forall x\ P(x))$ è vera $\rightarrow$ $\forall x\ P(x)$ è falsa $\rightarrow$ $\exists x$ per il quale P(x) è falsa $\rightarrow$
   $\rightarrow$ $\exists x$ per il quale $\neg P(x)$ è vera $\rightarrow$ $\exists x\ \neg P(x)$.
2. Ci rimane da provare che $\exists x\ \neg P(x) \rightarrow \neg\forall x\ P(x)$.
   Se $\exists x\ \neg P(x)$ è vera $\rightarrow$ $\exists x$ per cui P(x) è falsa $\rightarrow$ non è vero che $\forall x\ P(x)$ è vera $\rightarrow$
   $\rightarrow \neg(\forall x\ P(x))$

Negazione di quantificatori innestati

Per negare asserzioni con quantificatori innestati, si applica la negazione al quantificatore più a sinistra ed utilizzando le regole:

- $\neg\forall x\ P(x)$ è equivalente a $\exists x\ \neg P(x)$
- $\neg\exists x\ P(x)$ è equivalente a $\forall x\ \neg P(x)$

Si procede applicando la negazione al quantificatore immediatamente successivo, e così via.
Esempio:
Non c'è una persona che ama tutti gli altri.
Traduzione: $\neg\exists x\ \forall y\ Ama(x, y)$
$\neg\exists x\ (\ \forall y\ Ama(x, y)) \equiv \forall x\ \neg(\forall y\ Ama(x, y)) \equiv\ \forall x\ \exists y\ \neg Ama(x, y)$.

Rapporti tra quantificatori e connettivi logici

Nota 1: può accadere che $\exists x\ [\ P(x) \wedge D(x)]$ non è lo stesso di $\exists x\ P(x) \wedge \exists x\ D(x)$.
Esempio: consideriamo come dominio N:
$P(x)$ = x è pari $D(x)$ = x è dispari
Abbiamo che:

- $\exists x\ [\ P(x) \wedge D(x)]$ è **falsa** perché x non può essere sia pari che dispari.
- $\exists x\ P(x) \wedge \exists x\ D(x)$ è **vera** perché esiste un x pari e esiste un x dispari.

Nota 2: Che cosa possiamo dire di : $\forall x\ [\ P(x) \vee D(x)]$ e $\forall x\ P(x) \vee \forall x\ D(x)$
Considerando sempre N come dominio abbiamo che:

- $\forall x\ [\ P(x) \vee D(x)]$ è **vera** perché per ogni valore di $x \in N$ abbiamo che può essere o pari o dispari la x presa in considerazione in quel momento.
- $\forall x\ P(x) \vee \forall x\ D(x)$ è **falsa** perché non esistono in N numeri che siano solo pari o solo dispari; infatti abbiamo che come proposizione F v F che è uguale ad F.

Nota 3: Se in una espressione logica compaiono due espressioni logiche con quantificatori connesse con connettivi logici, è possibile muovere un quantificatore solo se la variabile legata al connettivo logico non appare nell'altra espressione logica.
Esempio:
$\forall x\ [\ F(x) \vee P(x) \rightarrow \exists y\ E(x, y)]$ è equivalente a $\forall x\ \exists y\ [\ F(x) \vee P(x) \rightarrow E(x, y)]$

INSIEMI ED OPERAZIONI SU INSIEMI

Insieme

L'insieme è una struttura discreta utilizzata per rappresentare oggetti discreti.
Molte strutture discrete sono costruite a partire dagli insiemi:

- Combinazioni (insiemi usati nel conteggio)
- Relazioni (insiemi che rappresentano le relazioni tra gli oggetti)
- Grafi (insiemi di vertici e archi)

Un insieme si può definire anche come una collezione non ordinata di oggetti, chiamati elementi dell'insieme.
Esempi:

- Insieme delle vocali: V = {a, e, i, o, u}
- Insieme dei primi 7 numeri primi: P = {1, 2, 3, 5, 7, 11, 13, 17}

Un insieme può essere rappresentato attraverso:

1. La lista (l'enumerazione) degli elementi che lo costituiscono (E= {50, 52, 54, 56, 58, 60, 62}).

2. La definizione della proprietà che caratterizza i suoi elementi (E= { x | x è un intero pari e $50 \leq x \leq 63$ }).

Se gli elementi dell'insieme sono molti si utilizza l'ellissi (…) nella rappresentazione dell'insieme attraverso l'enumerazione (A = {1, 2, …, 100}).

Alcuni insiemi importanti:

- Numeri naturali: N = {0,1,2,3, …}
- Interi: Z = {…, −2,−1,0,1,2, …}
- Interi positivi: - Z+ = {1,2, 3.…}
- Numeri razionali: Q = {p/q | p Z, q Z, q 0}
- Numeri reali: R

Esempio:
L' insieme dei numeri pari è { 0, 2, 4, 6, 8, 10, … }= { 2n | n N }
L' insieme dei numeri dispari è { 1, 3, 5, 7, 9, 11, … }= { 2n+1 | n N }
Quindi se P = { 2n | n N } allora $4 \in P$, ma $5 \notin P$.

Uguaglianza tra insiemi

Due insiemi sono uguali se e solo se sono costituiti dagli stessi elementi. Scriveremo $a \in A$ per indicare che a è un elemento di A.
Esempio:
I seguenti insiemi: {1, 2, 3}, {1, 2, 2, 3}, {3, 1, 2}. Questi tre insiemi sono uguali perché:

- Avere elementi duplicati in un insieme non dice nulla di più sull'insieme.
- Avere elementi in un ordine diverso non dice nulla di più sull'insieme.

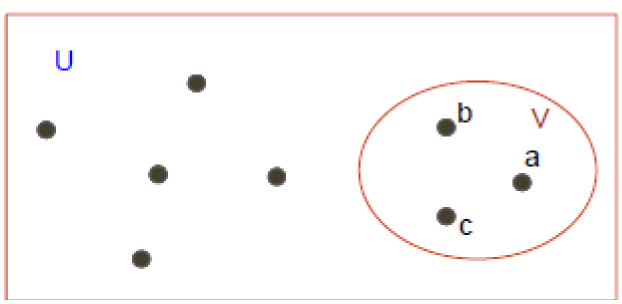
Mentre {1, 2, 3, 4} e {1, 2, 2, 3} non sono uguali perché 4 non appartiene ad entrambi gli insiemi.
Un modo alternativo per dire che A = B è: $\forall$**x (x $\in$ A)** $\leftrightarrow$ **(x $\in$ B)**.

Insiemi speciali

- L'**insieme universale** è denotato con U; è l'insieme costituito da tutti gli elementi che si stanno considerando.
- L'**insieme vuoto** è denotato con $\emptyset$; non contiene alcun elemento.

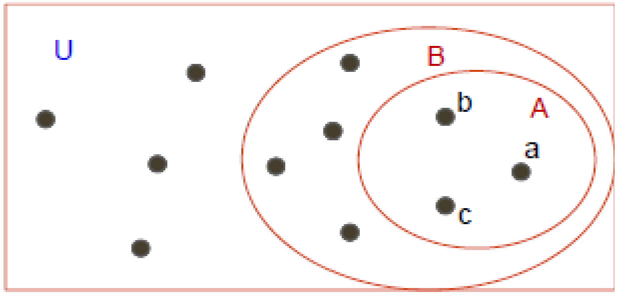
Diagrammi di Venn

Un insieme può essere rappresentato visivamente usando i diagrammi di Venn: V = {a, b, c}



Sottoinsiemi

Un insieme A è detto un sottoinsieme di un insieme B se e solo se ogni elemento di A è anche un elemento di B. Usiamo $A \subseteq B$ per indicare che A è un sottoinsieme di B.



Un modo alternativo per dire che $A \subseteq B$ è: $\forall \mathbf{x}\ (\mathbf{x} \in \mathbf{A}) \rightarrow (\mathbf{x} \in \mathbf{B})$.

Proprietà dei sottoinsiemi

TEOREMA:

$\emptyset \subseteq S$ cioè l'insieme vuoto è sottoinsieme di qualunque insieme.

Dim:

Dobbiamo far vedere che $\forall x\ (x \in \emptyset) \rightarrow (x \in S)$.

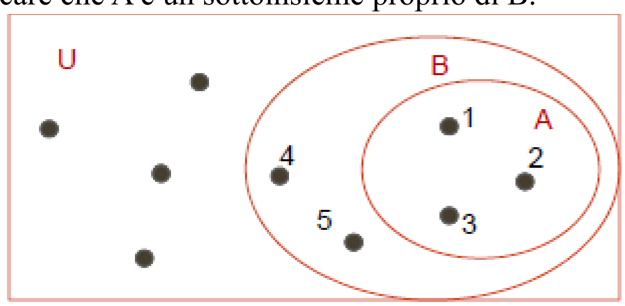
Poiché $\emptyset$ non contiene alcun elemento allora $x \in \emptyset$ è sempre **falsa**.

Ma una implicazione $\rightarrow$ è sempre vera se l'ipotesi è falsa, quindi $\forall x\ (x \in \emptyset) \rightarrow (x \in S)$ è vera.

Sottoinsiemi propri

Un insieme A è detto un sottoinsieme proprio di un insieme B se e solo se $A \subseteq B$ e $A \neq B$.

Usiamo $A \subset B$ per indicare che A è un sottoinsieme proprio di B.



Esempio: A={1,2,3} B ={1,2,3,4,5} $A \subset B$? Si.

Cardinalità

Sia S un insieme e sia n un intero non negativo. Se ci sono esattamente n distinti elementi in S, diciamo che n è la cardinalità di S. La cardinalità di S è denotata con $|S|$.

Esempi:

- $A = \{1, 2, 3\}$ quindi $|A| = 3$
- $B = \{1, 2, 3, \dots, 20\}$ quindi $|B| = 20$
- $|\emptyset| = 0$

Un insieme infinito è un insieme non finito.

Esempi: L'insieme dei numeri naturali è infinito perché $N = \{0, 1, 2, \dots, +\infty\}$, anche l'insieme dei numeri reali R è infinito.

Insieme potenza

Dato un insieme S. L'insieme potenza di S è l'insieme di tutti i sottoinsiemi di S. L'insieme potenza di S è denotato con P(S).

Esempio 1:

Consideriamo l'insieme vuoto: Ø. Quale è l'insieme potenza di Ø? P(Ø) = {Ø}. Invece quale è la cardinalità di P(Ø)? |P(Ø)| = 1.

Esempio 2:

Consideriamo l'insieme: {1} . Quale è l'insieme potenza di {1}? P({1}) = {Ø, {1}}. Invece quale è la cardinalità di P({1})? |P({1})| = 2.

Esempio 3:

Consideriamo l'insieme: {2} . Quale è l'insieme potenza di {2}? P({2}) = {Ø, {1}, {2}, {1,2}}. Invece quale è la cardinalità di P({2})? |P({2})| = 4.

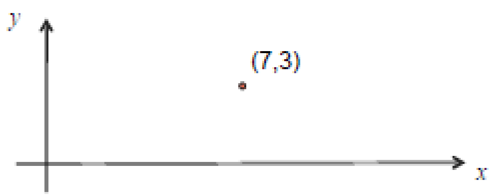
Quindi se S è un insieme con |S| = n allora $|P(S)| = 2^n$

n-ple

Un insieme è usato per rappresentare una collezione non ordinata di oggetti. Una n-pla è usata per rappresentare una collezione ordinata di oggetti.

Una n-pla ordinata $(x_1, x_2, \ldots, x_n)$ è una collezione ordinata che ha x_1 come primo elemento, x_2 come secondo elemento, …, x_n come n-simo elemento, con $n \geq 2$.

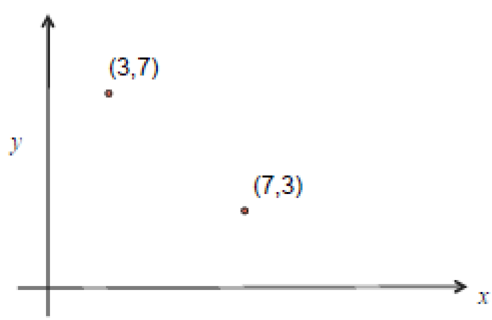
Esempio:



Coordinate di un punto nel piano

In una n-pla l'ordine della collezione è importante:

Esempio:

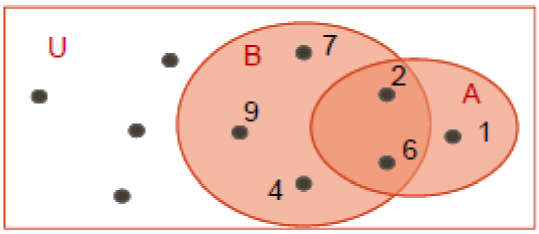


Coordinate di un punto nel piano

Prodotto cartesiano
Siano S e T due insiemi. Il prodotto cartesiano di S e T denotato con S x T, è l'insieme di tutte le coppie ordinate (s,t) dove $s \in S$ e $t \in T$. Quindi, $S \times T = \{ (s, t) \mid s \in S \text{ e } t \in T\}$.
Esempi:
Prendiamo in considerazione i due insiemi S = {1,2} e T = {a,b,c}, il loro prodotto cartesiano sarà
S x T = { (1,a), (1,b), (1,c), (2,a), (2,b), (2,c) } o T x S = { (a,1), (a, 2), (b,1), (b,2), (c,1), (c,2) }.
Nota: $S \times T \neq T \times S$.

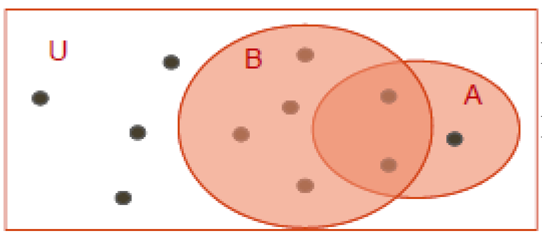
La cardinalità di S x T è uguale a |S x T| = |S| * |T|.

Operazioni sugli insiemi
Unione:
Siano A e B due insiemi. L'unione di A e B, denotata con A U B, è l'insieme che contiene gli elementi in A o quelli in B. Quindi **A U B = { x | x ∈ A v x ∈ B }**.



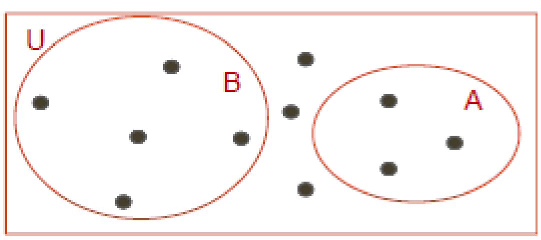
Esempio: A = {1, 2, 6}   B = {2, 4, 6, 7, 9}
A U B = {1, 2, 4, 6, 7, 9}

La cardinalità dell'insieme unione è | A U B | = |A| + |B| - | A ∩ B|.



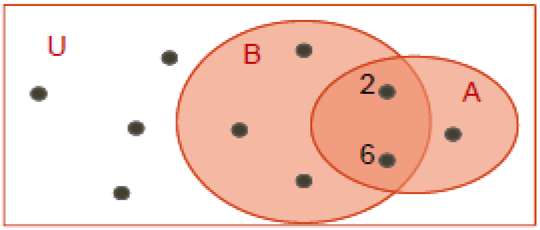
Perché funziona? Se si considera |A| + |B| allora si conta |A ∩ B| due volte.
Più in generale vale il **principio di inclusione ed esclusione.**

Se A e B sono disgiunti allora la cardinalità dell'insieme unione è |A U B| = |A| + |B| perché l'intersezione ha valore Ø.



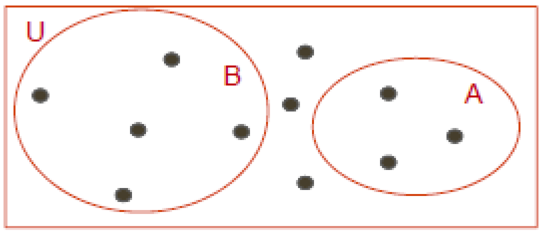
Intersezione:

Siano A e B due insiemi. L'intersezione di A e B, è denotata con $A \cap B$, è l'insieme che contiene gli elementi in A e quelli in B. Quindi $\mathbf{A \cap B = \{ x | x \in A \wedge x \in B\}}$.



Esempio: A = {1, 2, 6}   B = {2, 4, 6, 7, 9)
$A \cap B = \{2, 6\}$

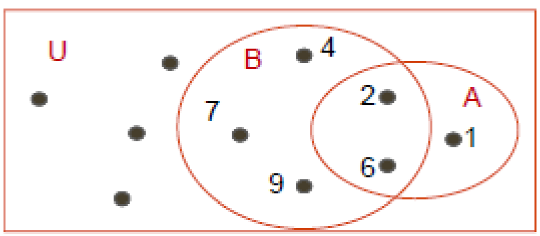
Due insiemi si dicono **disgiunti** se la loro intersezione è vuota, cioè $A \cap B = \emptyset$.



Esempio: A = {1, 2, 6}   B = {0, 5, 3, 8}
$A \cap B = \emptyset$

Differenza:

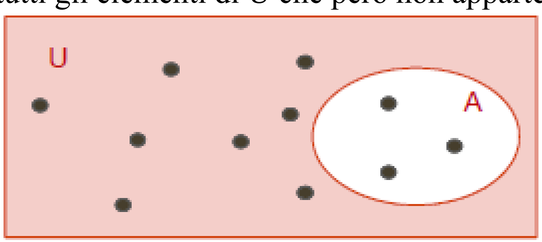
Siano A e B due insiemi. La differenza tra A e B, denotata con A – B, è l'insieme che contiene quegli elementi che sono in A ma non sono in B. Quindi $\mathbf{A - B = \{ x | x \in A \wedge x \notin B\}}$.



Esempio: A = {1, 2, 6}   B = {2, 4, 6, 7, 9)
A – B = {1}

Complemento di A:

Sia U l'insieme universale ed A un insieme. Il complemento di A, denotato con $\overline{A}$, è l'insieme di tutti gli elementi di U che però non appartengono ad A. Quindi $\overline{A} = \{ x | x \in U \wedge x \notin A\}$.



Esempio 1: U = {1, 2, 3, 4, 5, 6, 7, 8,}   A = {1, 3, 5, 7}
$\overline{A}$ = {2, 4, 6, 8}
Esempio 2: U = N   A = {2n | n ∈ N}
$\overline{A} = \{2n + 1 | n \in N\}$ = insieme dei numeri dispari

Insiemi: operazioni ed identità

Operazioni:

$A = B$ abbiamo $\forall x (x \in A) \Leftrightarrow (x \in B)$	$A \cap B = \{x | x \in A \wedge x \in B\}$
$A \subseteq B$ abbiamo $\forall x (x \in A) \Rightarrow (x \in B)$	$A - B = \{x | x \in A \wedge x \notin B\}$
$A \cup B = \{x | x \in A \vee x \in B\}$	$\overline{A} = \{x | x \in U \wedge x \notin A\}$

Identità tra gli insiemi:

Identità: $A\cup\emptyset=A$ $A\cap U=A$ **Dominazione:** $A\cap U=U$ $A\cup\emptyset=\emptyset$ **Idempotenza:** $A\cup A=A$ $A\cap A=A$	**Doppio complemento:** $\overline{\overline{A}}=A$ **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: $\overline{(A\cup B)}=\overline{A}\cap\overline{B}$ $\overline{(A\cap B)}=\overline{A}\cup\overline{B}$ **Leggi dell'assorbimento:** $A\cup(A\cap B)=A$ $A\cap(A\cup B)=A$	**Leggi del complemento:** $A\cup(\overline{A})=U$ $A\cap(\overline{A})=\emptyset$

Le identità tra gli insiemi possono essere provate utilizzando le tavole di appartenenza seguendo i seguenti punti:

- Elencare gli insiemi che costituiscono l'identità.
- Elencare le diverse combinazioni di appartenenza degli elementi agli insiemi.
- Assegna 1 se un elemento appartiene all'insieme, 0 altrimenti.

Provare che $\overline{(A\cap B)}=\overline{A}\cup\overline{B}$:

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

Le identità tra gli insiemi possono essere provate utilizzando le equivalenze logiche.

Provare che $\overline{(A\cap B)}=\overline{A}\cup\overline{B}$:

$\overline{(A\cap B)}=\{x \mid x\notin A\cap B\}$	definizione di complemento
$=\{x \mid \neg(x\in A\cap B)\}$	definizione di non appartenenza
$=\{x \mid \neg(x\in A \wedge x\in B)\}$	definizione di intersezione
$=\{x \mid \neg(x\in A) \vee (x\in B)\}$	dalla Legge di De Morgan
$=\{x \mid x\notin A \vee x\notin B\}$	definizione di non appartenenza
$=\{x \mid x\in \overline{A}\cup\overline{B}\}$	definizione di complemento
$=\overline{A}\cup\overline{B}$	definizione di unione

Esercizi:

L'insieme dei numeri naturali dispari è: $\{1, 3, 5, 6, 9, 11, \ldots\} = \{2n + 1 \mid n \in N\}$

Dare una descrizione formale dell'insieme X degli interi non negativi che verificano la seguente proprietà: Se $n \geq 5$ allora n è dispari.

$X = \{n \mid (n \geq 5) \rightarrow (n \text{ è dispari})\}$

$X = \{n \mid (n \geq 5) \rightarrow (\exists\, k \in N \mid n = 2k + 1)\}$

$X = \{ n \mid n = 2k +1, k \in N, k \geq 2\} \cup \{0, 1, 2, 3, 4\}$

Come rappresentare gli insiemi in un computer?

Stringa di bit

La stringa di bit deve prevedere tanti bit quanti sono gli elementi dell'insieme universale U. U = $\{a_1, a_2, \ldots, a_n\}$ allora $\forall A \subseteq U$ la stringa che rappresenta A ha n bit. Ogni elemento U corrisponde ad una posizione precisa nella stringa. Dato un insieme A, la stringa di n bit A avrà nella posizione i, per $1 \leq i \leq n$, un:

- 1 se l'elemento $a_i \in A$
- 0 se l'elemento $a_i \notin A$

Esempio:

Prendendo inconsiderazione l'insieme universale U = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10} e l'insieme A = {1, 3, 5, 6, 9}, lo si rappresenti sotto formato di stringa binaria: 1010110010.

Con la stringa di bit è molto più efficiente effettuare la ricerca. Infatti basta fare un AND tra la stringa che rappresenta l'insieme ed una stringa con tutti 0 ed un 1 in corrispondenza dell'elemento da cercare. Se il risultato è 0 allora l'elemento non è nell'insieme, altrimenti si.

Esempio:

Prendendo inconsiderazione l'insieme universale U = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10} e l'insieme A = {1, 3, 5, 6, 9}, si vuole verificare che $3 \in A$:

1010110010 ^
0010000000 = 0010000000. La stringa risultante è diversa da 0 quindi l'elemento è presente.

Con la stringa di bit è molto più semplice effettuare operazioni tra insiemi. Infatti se si vuole fare l'unione di due insiemi A e B, basta fare un OR tra le stringhe che rappresentano i due insiemi. La stringa ottenuta come risultato rappresenta l'insieme A U B.

Esempio:

Prendendo inconsiderazione l'insieme universale U = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}, l'insieme A = {1, 3, 5, 6, 9} e l'insieme B = {1, 2, 9}, si effettui l'unione di A e di B.

1010110010 v
1100000010 = 1110110010. Quindi dalla stringa risultante ricaviamo che A U B = {1, 2, 3, 5, 6, 9}.

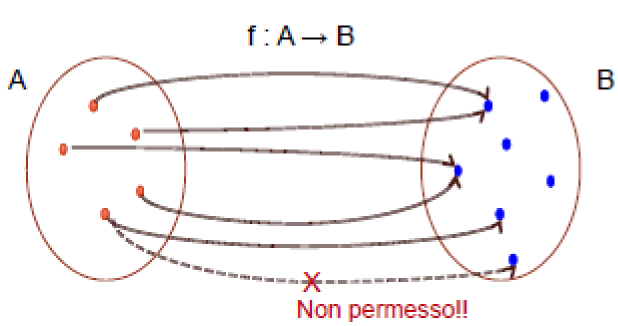
CARDINALITÀ DEGLI INSIEMI

Richiami

Un insieme è una struttura discreta utilizzata per rappresentare oggetti discreti. Una funzione mette in relazione oggetti appartenenti ad un insieme con appartenenti ad un altro insieme (non necessariamente diverso dal primo).

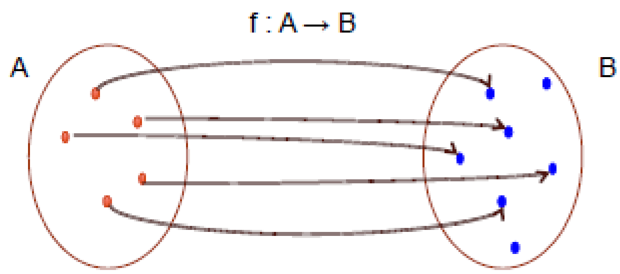
Sappiamo anche che un insieme è una collezione non ordinata di oggetti, chiamati elementi dell'insieme.

Funzioni

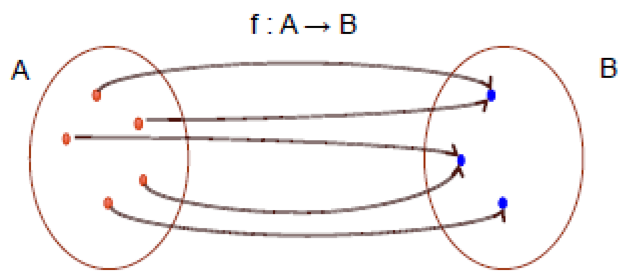


Siano A e B due insiemi. Una funzione da A in B, denotata **f: A → B**, associa ciascun elemento di A ad esattamente un elemento di B.

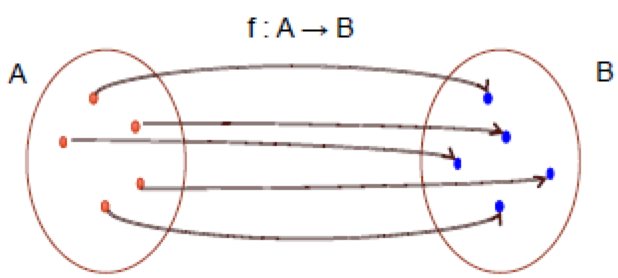
Iniettiva: una funzione è detta iniettiva se e solo se $f(x)=f(y) \Rightarrow \forall x, y \in f(x)$.
Alternativamente, x ≠ y → f(x) ≠ f(y).



Suriettiva: una funzione da A e B è detta suriettiva se e solo se $\forall b \in B \exists a \in A : f(a)=b$.
Alternativamente, f(A) = B.



Biettiva: una funzione è detta biettiva se è sia iniettiva che suriettiva.



Cardinalità

La definizione di cardinalità che sappiamo è la seguente: *Sia S un insieme e sia n un intero non negativo. Se ci sono esattamente n distinti elementi in S, diciamo che n è la cardinalità di S. La cardinalità di S è denotata con* **|*S*|**.
Ora verrà data una definizione alternativa di cardinalità di un insieme:
Due insiemi A e B hanno la stessa cardinalità se esiste una corrispondenza uno-a-uno tra gli elementi di A e quelli di B. Alternativamente se esiste una biezione tra A e B.
Esempio:
Prendiamo in considerazioni i seguenti insiemi: A = {a, b, c}   B = {α, β, γ}
Consideriamo la funzione f definita come:

- a → α
- b → β
- c → γ

f definisce una biezione, quindi A e B hanno la stessa cardinalità, cioè |A| = |B| = 3.

Insiemi numerabili

Un insieme che è finito o ha la stessa cardinalità di Z^+ è detto numerabile. Cioè i suoi elementi possono essere enumerati.

Esempio:

Prendiamo A = {0, 2, 4, 6, …} cioè A è l'insieme dei numeri pari.

A è numerabile? Dimostriamolo.

dim:

Dalla definizione dovremmo far vedere che c'è una funzione biettiva f: $Z^+ \rightarrow A$, ricordiamo che $Z^+ = \{1, 2, 3, 4, \ldots\}$.

Definiamo ora la funzione $f: x \in Z^+ \rightarrow 2x-2 \in A$

- $1 \rightarrow 2 * 1 - 2 = 0$
- $2 \rightarrow 2 * 2 - 2 = 2$
- $3 \rightarrow 2 * 3 - 2 = 4$
- …

f è una biezione ?

- f è iniettiva perché: $f(x) = f(y) \rightarrow 2x - 2 = 2y - 2 \rightarrow x = y$
- f è suriettiva perché $\forall a \in A \exists x \in Z^+, a = 2x - 2 \rightarrow (a+2)/2$ è un intero positivo

Perciò $|A| = |Z^+|$

Teorema

L'insieme degli interi Z è numerabile.

dim:

Dalla definizione dovremmo far vedere che c'è una funzione biettiva f: $Z^+ \rightarrow Z$, ricordiamo che $Z^+ = \{1, 2, 3, 4, \ldots\}$.

Definiamo la funzione:

$$f: x \in Z^+ \rightarrow \begin{cases} \dfrac{x}{2} & se\ x\ è\ pari \\ \dfrac{-(x-1)}{2} & se\ x\ è\ dispari \end{cases}$$

f è iniettiva perché:

$$-f(x) = f(y) \Rightarrow \frac{x}{2} = \frac{y}{2} \Rightarrow x = y\ (se\ x\ e\ y\ sono\ pari)$$

$$-f(x) = f(y) \Rightarrow -\frac{(x-1)}{2} = \frac{-(y-1)}{2} \Rightarrow x = y\ (se\ x\ e\ y\ sono\ dispari)$$

f è suriettiva perché:

$$-\forall z \in Z \quad \begin{matrix} 2z\ è\ un\ intero\ pari\ positivo\ se\ z = positivo \\ -2z+1\ è\ un\ intero\ dispari\ positivo\ se\ z = negativo \end{matrix}$$

Perciò $|Z| = |Z^+|$

Un numero razionale può essere espresso come il rapporto p/q di due interi p e q, con q ≠ 0.

Teorema

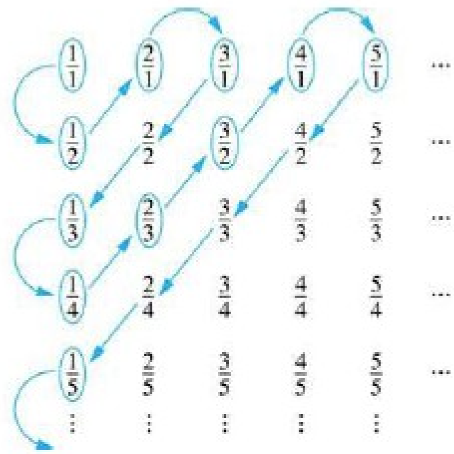
I numeri razionali positivi sono numerabili.

dim:

Vedremo che è possibile formare una sequenza con tutti i p/q.
Disponiamo p/q per riga:

- nella 1ª riga i p/q con q=1
- nella 2ª i p/q con q= 2, etc.

Notate che tutti i p/q lungo la medesima "diagonale" hanno p+q dello stesso valore.



Mettiamo quindi in una lista i p/q:

- prima i p/q con p+q = 2 (cioè il solo 1/1)
- poi i p/q con p+q = 3 (cioè ½ e 2/1)
- etc.

Ogni volta che si incontra un P/q già incontrato non lo si inserisce (per esempio 2/2 = 1/1, 2/4 = ½, …)
Siccome:

- ogni numero razionale è stato inserito esattamente una volta nella lista e
- gli elementi di una lista possono essere contati

questo implica che i numeri razionali positivi sono numerabili.

Teorema

l'insieme dei numeri reali R non è numerabile.

dim:

Procediamo per contraddizione.
Supponiamo che R sia numerabile (arriveremo ad una contraddizione).
Poiché un sottoinsieme di un insieme numerabile è numerabile, abbiamo che:

- i numeri reali tra 0 e 1 sono numerabili, cioè c'è una corrispondenza biunivoca tra $Z^+ = \{1, 2, 3, \dots\}$ ed i numeri in[0, 1].
- Possiamo perciò creare una sequenza di tutti i numeri reali [0, 1]: $r_1, r_2, r_3, \dots$

Dove:

- $r_1 = 0, d_{11}\, d_{12}\, d_{13} \dots$
- $r_2 = 0, d_{21}\, d_{22}\, d_{23} \dots$
- $r_3 = 0, d_{31}\, d_{32}\, d_{33} \dots$
- …

dove $d_{ij} \in \{0, 1, 2, \dots, 9\}$

$r_1 = 0, 23794 \dots$
$r_2 = 0, 54781 \dots$
$r_3 = 0, 62314 \dots$
….

consideriamo un numero reale $r = 0, b_1\, b_2\, b_3 \dots$ $b_i = \begin{cases} 4 & se\ d_{ij} \neq 4 \\ 5 & se\ d_{ij} = 4 \end{cases}$ quindi r = 0,454…

Si noti che stiamo considerando rappresentazioni decimali uniche di numeri reali (cioè si evitano rappresentazioni che finiscono con una lista infinita di 9).
Invece di avere $r_i = 0, 23799999 \dots$ consideriamo $r_i = 0, 2380000 \dots$

Quindi infine:
Poiché tutti i numeri reali in [0, 1] sono nella lista $r_1, r_2, r_3, \dots$ allora $\exists i : r = r_i$
Ricordando che $r_i = 0, d_{i1}\, d_{i2} \dots d_{ij} \quad \dots$ $\qquad b_i = \begin{cases} 4 & se\ d_{ij} \neq 4 \\ 5 & se\ d_{ij} = 4 \end{cases}$
$r = 0, d_1\, d_2 \ \dots\ d_i \quad \dots$

Si ha una contraddizione poiché dovrebbe essere $b_i = b_{ij}$ ed invece:
- $b_i = 4$ se $d_{ij} = 5$
- $b_i = 5$ se $d_{ij} = 4$

DIMOSTRAZIONI

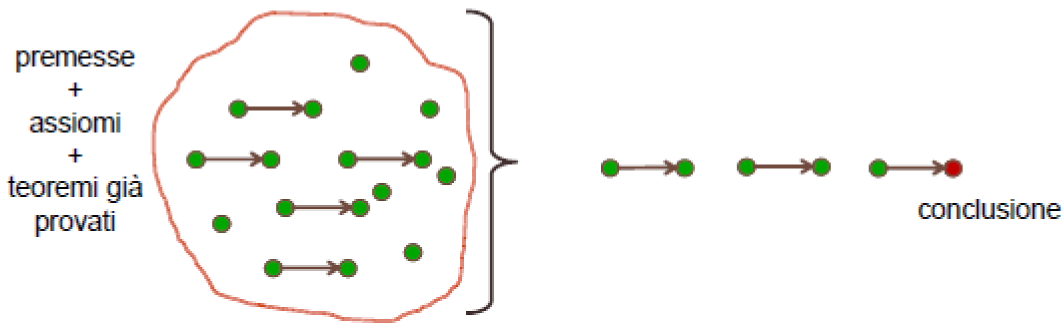
Una dimostrazione è un ragionamento che stabilisce la verità di un asserzione matematica attraverso l'uso di altre asserzioni vere:
- ipotesi del teorema
- assiomi che si assumono essere veri
- teoremi dimostrati precedentemente

Teoremi

Un teorema è una asserzione che si può dimostrare essere vera. Tipicamente un teorema lo si può vedere in questo modo: $\underbrace{(p_1 \wedge p_2 \wedge p_3 \wedge \dots \wedge p_n)}_{\text{premesse (ipotesi)}} \rightarrow \underbrace{q}_{\text{conclusione}}$.

Esempio: *Teorema di Fermat*
Se *p è un primo ed a è un numero non divisibile per p* (premessa o ipotesi) allora $a^{p-1} \equiv 1 \bmod p$ (conclusione).

In una dimostrazione si usano: assiomi, definizioni di termini, risultati ottenuti precedentemente e strumenti della logica proposizionale per completare la dimostrazione.



Di seguito analizzeremo i diversi metodi usati per provare che p → q è T. È bene ricordare che p → q è T in tutti i casi tranne quando p = T e q = F. Quindi:
- Se p è F allora indipendentemente dal valore di q abbiamo p → q è T.
- Se p è T allora dobbiamo provare anche che q è T per avere p → q è T.

Per provare che p → q è T dovremmo dimostrare che: *se p è T allora q è T.*

Metodi per provare teoremi:

Metodi di base:

- Dimostrazione diretta
- Dimostrazione per contrapposizione
- Dimostrazione per contraddizione (assurdo)
- Dimostrazione di equivalenza
- Dimostrazione banale
- Dimostrazione vuota
- Dimostrazione per analisi dei casi
- Dimostrazione con quantificatori

Nota: non tutti i metodi di dimostrazione vanno bene in tutti i casi; infatti può accadere che un metodo dimostrativo si rivela più semplice di altri. Può essere perciò necessario tentare più di un approccio. o Inoltre, alcune dimostrazioni possono richiedere l'utilizzo di più di un tipo di dimostrazione.

Dimostrazione diretta

$p \rightarrow q$ viene dimostrata mostrando che "se p è T allora q è T", in maniera diretta:

- si parte dal fatto che p è T
- si fanno una serie di deduzioni, usando assiomi, definizioni e teoremi precedentemente provati per arrivare a dire che anche q è T.

Esempio 1: Sia n un intero. Provare che "Se **n è dispari**, allora **n^2 è dispari**".

dim:

Assumiamo che l'ipotesi sia vera, cioè n è dispari, allora $n = 2k + 1$, dove k è un qualsiasi intero. Quindi:

$$n^2 = (2k +1)^2 =$$
$$= 4k^2 + 4k + 1 =$$
$$= 2(2k^2 + 2k) + 1$$

Perciò n^2 è dispari.

Esempio 2: Siano n ed m interi. Provare che "Se **ne ed m sono dispari**, allora **n + m è pari**".

dim:

Assumiamo che l'ipotesi sia vera, cioè n ed m siano dispari, allora $n = 2k + 1$ e $m = 2h + 1$ dove k ed h sono due qualunque interi. Quindi:

$n + m = (2k +1) + (2h + 1) =$

$=2k + 2 h + 2$

Perciò n + m è pari.

Dimostrazione per contrapposizione

$p \rightarrow q$ viene dimostrata mostrando che "se ($\neg q$ è T) allora (p è F)" o con "se ($\neg q$ è T) allora ($\neg p$ è T)" .

Nota: Ciò che si dimostra è che " se "se ($\neg q$ è T) allora ($\neg p$ è T)", quindi si ricordi che $\neg q \rightarrow \neg p \equiv p \rightarrow q$ (contronominale).

Esempio: Provare che "Se **3n + 2 è dispari**, allora **n è dispari**"

dim:

Assumiamo al contrario che n è pari, cioè $n = 2k$, Quindi:

$3n + 2 = 3(2k) + 2 = 6k + 2$, Abbiamo quindi che $3n + 2$ è pari. Quindi $3n + 2$ è dispari $\equiv$ F.

Dimostrazione per contraddizione (assurdo)

$p \rightarrow q$ viene dimostrata mostrando che " se [(p è T) e ($\neg q$ è T)] allora è F". Cioè si parte dal fatto che:

- $\neg q$ è T
- p è T

Quindi si fanno una serie di deduzioni, usando assiomi definizioni e teoremi precedentemente provati per arrivare ad un'asserzione F.
L'approccio è corretto perché:

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

Esempio 1: Provare che "Se **3n + 2 è dispari**, allora **n è dispari**".
dim:
Assumiamo al contrario che n è pari, cioè $n = 2k$, dove k è un intero.
Per ipotesi sappiamo che $3n + 2$ è dispari, cioè $3n + 2 = 2h +1$, dove h è un intero.
$2h + 1 = 3n + 2 = 3(2k) + 2 = 6k + 2$ che è ovviamente pari.
Ma questo è F(è assurdo) poiché $2h + 1$ è dispari.

Esempio 2: Siano x e y due numeri reali. Provare che "Se **5x + 25y = 1723**, allora **x o y non sono interi**".
dim:
Assumiamo al contrario che x e y siano interi:
$5x + 25y = 1723$
$5(x +5y) = 1723$
$x + 5y = 1723 / 5$
ma essendo che 1723 non è divisibile per 5 $\rightarrow$ che $x + 5y$ non è un intero.
Ma questo è F(è assurdo) poiché sappiamo che x e y sono interi.

Dimostrazione di equivalenza

$p \rightarrow q$ è dimostrata con $(p \rightarrow q) \wedge (q \rightarrow p)$. Dobbiamo provare quindi che $p \leftrightarrow q$, che è equivalente a p se e solo se q. Entrambe le implicazione devono essere vere.

Esempio 1: **n è dispari** se e solo se **n^2 è dispari**.
dim: di $p \rightarrow q$:
Dobbiamo provare che: Se n è dispari allora n^2 è dispari.
Usiamo la dimostrazione diretta. Supponiamo che n sia dispari. Allora $n = 2k + 1$, dove k è un intero, quindi $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Perciò n^2 è dispari.
dim: di $q \rightarrow p$:
Dobbiamo provare che: Se n^2 è dispari allora n è dispari.
Usiamo la dimostrazione indiretta, cioè proviamo $(\neg p \rightarrow \neg q)$. Supponiamo che n sia pari. Allora $n = 2k$, dove k è un intero, quindi $n^2 = (2k)^2 = 4k^2$. Perciò n^2 è pari.
Poiché entrambe $(p \rightarrow q)$ e $(q \rightarrow p)$ sono vere, l'equivalenza è vera.

A volte i teoremi affermano che più proposizioni sono equivalenti:

- Vogliamo provare che: $p_1 \leftrightarrow p_2 \leftrightarrow \ldots\ldots \leftrightarrow p_n$
- Tutte le proposizioni p_1 , p_2 , …… , p_n hanno lo stesso valore di verità
- Un modo per provarlo è provare la seguente proposizione equivalente:

$(p_1 \to p_2)\wedge (p_2 \to p_3) \wedge \ldots\ldots \wedge (p_n \to p_1)$ che è uguale ad :

$p_1 \to p_2 \to \ldots\ldots \to p_n \to p_1$

Mostrate che le seguenti asserzioni sono equivalenti:

- p_1: n è pari
- p_2: n-1 è dispari
- p_3: n^2 è pari

dim: proveremo che $p_1 \to p_2$,, $p_2 \to p_3$, $p_3 \to p_1$

- proviamo che $p_1 \to p_2$:
  Se n è pari, allora n = 2k, dove k è un intero. Quindi $n - 1 = 2k - 1 = 2(k - 1) + 1$ che è un intero dispari.
- Proviamo che $p_2 \to p_3$:
  Se n – 1 è dispari, allora $n - 1 = 2k + 1$, dove k è un intero. Quindi $n^2 = (2k + 2)^2 = 4k^2 + 8k + 4 = 2(2k^2 + 4k + 2)$ che è un intero pari.
- Proviamo che $p_3 \to p_1$:
  Per contrapposizione supponiamo che n sia dispari, cioè $n = 2k + 1$, dove k è un intero. Quindi $n^2 = (2k + 1)^2 = 4k^2 +4k + 1 = 2(2k^2 + 2k) + 1$ che è un intero dispari.

Dimostrazione banale

$p \to q$ viene dimostrata mostrando che se la conclusione q è sempre vere allora $p \to$ è banalmente vera.

Esempio 1: Sia P(n): " se $\geq b$ allora $a^n \geq b^n$", Mostrare che $P(n) \to P(0)$.

dim:

$a^0 \geq b^0$ è 1 = 1 che è banalmente vera indipendentemente da n.

Esempio 2: Proviamo che " Se $x > 0$ allora $(x + 1)^2 - 2x \geq x^2$.

dim:

$(x + 1)^2 - 2x = (x^2 + 2x + 1) - 2x = x^2 + 1 \geq x^2$

Dimostrazione vuote

Vogliamo provare che $p \to q$. Se l'ipotesi p è sempre falsa allora $p \to q$ è banalmente vera.

Esempio: Sia P(n): se $n \geq 1$ allora $n^2 \geq 1$. Mostrare che (se $n = 0$) $\to$ p(0)).

dim:

Per $n = 0$ l'ipotesi di P(n) è falsa. Così P(0) è sempre vera.

Dimostrazione per analisi dei casi

Vogliamo provare che $(p_1 \vee p_2 \vee \dots \vee p_n) \rightarrow q$, che è equivalente a $(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \dots \wedge (p_n \rightarrow q)$

Perché vale?

$(p_1 \vee p_2 \vee \dots \vee p_n) \rightarrow q \equiv$

$\neg (p_1 \vee p_2 \vee \dots \vee p_n) \vee q \equiv$ (applichiamo De Morgan)

$(\neg p_1 \wedge \neg p_2 \wedge \dots \wedge \neg p_n) \wedge q \equiv$ (applichiamo distributiva)

$(\neg p_1 \vee q) \wedge (\neg p_2 \vee q) \wedge \dots \wedge (\neg p_n \vee q) \equiv$

$(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \dots \wedge (p_n \rightarrow q)$

Infatti alla fine di tutti si deve provare la verità di tutti i casi uno per uno.

Esempio 1: Mostrare che $|x||y| = |xy|$ per x ed y reali

dim:

Consideriamo i possibili valori di x e y. I casi possibili sono 4:

1. $x \geq 0, y \geq 0 \Rightarrow xy \geq 0$ e $|xy| = xy = |x||y|$
2. $x \geq 0, y < 0 \Rightarrow xy \leq 0$ e $|xy| = -xy = x(-y) = |x||y|$
3. $x < 0, y \geq 0 \Rightarrow xy \leq 0$ e $|xy| = -xy = (-x)y = |x||y|$
4. $x < 0, , y < 0 \Rightarrow xy > 0$ e $|xy| = (-x)(-y) = |x||y|$

Tutti i casi sono provati.

Esempio 2: Sia $n \in Z$. Provare che $9n^2 + 3n - 2$ è pari.

dim:

Per prima cosa consideriamo che: $9n^2 + 3n - 2 = (3n + 1)(3n - 1)$. Poiché n è un intero, allora $(3n + 2)(3n - 1)$ è il prodotto di due interi.

Consideriamo 2 casi:

1. Assumiamo $3n + 2$ = pari: $9n^2 + 3n - 2$ è banalmente pari perché è il prodotto di due interi di cui uno paro.
2. Assumiamo $3n + 2$ = dispari: $3n + 2 - 3$ è pari $\rightarrow$ $3n - 1$ è pari $\rightarrow$ $9n^2 + 3n - 2$ è pari perché uno dei suoi fattori è pari.

Tutti i casi sono provati.

Analisi dei casi - dimostrazioni esaustive

Alcuni teoremi possono essere provati esaminando un numero relativamente piccolo di esempi. Questo modo di fare è un tipo speciale di dimostrazione per casi. Ogni caso consiste nel controllare un singolo esempio.

Esempio: $(n + 1)^3 \geq 3^n$ se n è un intero positivo con $n \leq 4$.

dim:

Bisogna verificare $(n + 1)^3 \geq 3^n$ solo nei casi n = 1, 2, 3, 4

- $n = 1$ $(n + 1)^3 = (1 + 1)^3 = 8 \geq 3^n = 3^1 = 3$
- $n = 2$ $(n + 1)^3 = (2 + 1)^3 = 27 \geq 3^n = 3^2 = 9$
- $n = 3$ $(n + 1)^3 = (3 + 1)^3 = 64 \geq 3^n = 3^3 = 27$
- $n = 4$ $(n + 1)^3 = (4 + 1)^3 = 125 \geq 3^n = 3^4 = 81$

Dimostrazioni con quantificatori

Asserzioni espresse con un quantificatore.

Esistenziale: dimostrazioni di esistenza, vogliamo provare che $\exists x\, P(x)$.

Si può risolvere in due modi:

- *Costruttiva*: in cui dobbiamo trovare un esempio che mostri che l'asserzione vale.
  Esempio: esiste un intero che può essere scritto in due diversi modi come la somma di cubi di interi positivi.
  Dim: $1729 = 10^3 + 9^3 = 12^3 + 1^3$
- *Non-costruttiva*: se non si trova un esempio calzante, si opta per una dimostrazione per assurdo in cui si nega l'asserzione esistenziale e si mostra che ciò implica una contraddizione:
  Si assume che vale $\neg\exists x\, P(x) \equiv \forall x\, \neg P(x)$.
  Poi si arriva ad una contraddizione.

Esempio: (Pigeon Hole Principle)

Se n + 1 oggetti sono distribuiti in n scatole allora qualche scatola deve contenere almeno 2 oggetti.

dim:

- Assumiamo di avere n + 1 oggetti, e n scatole identificate con $B_1, B_2, \dots, B_n$.
- Per contrapposizione supponiamo che nessuna scatola contiene più di 1 oggetto.

k_i = il numero di oggetti posti nella scatola B_i, per i = 1, …, n e $k_i \leq$ allora:

$k_1 + k_2 + \dots + k_n \leq 1 + 1 + \dots + 1 = n$.

Ma questo contraddice l'ipotesi $k_1 + k_2 + \dots + k_n = n + 1$.

Negazione quantificatore esistenziale: vogliamo provare che $\neg\exists x\, P(x) \equiv \forall x\, \neg P(x)$.

Lo si prova rapportandolo al quantificatore universale, oppure si procede per assurdo ipotizzando l'esistenza di un elemento x che soddisfa P(x) e arrivando ad una contraddizione.

Esempio: Il numero $\sqrt{2}$ è un irrazionale.

Si ricordi che l'asserzione *il numero* $\sqrt{2}$ *è un irrazionale* è equivalente a:

non esistono due interi p e q : $\sqrt{2}$ *= p/q*, simbolicamente può essere espressa come:

$$\neg(\exists p, q \in Z(\sqrt{2} = \frac{p}{q}))$$

In questo caso l'ipotesi non è specificata; abbiamo solo la tesi.

dim:

Assumiamo per contraddizione che $\sqrt{2}$ è un razionale, cioè $\sqrt{2}$ = p/q, dove p e q sono due numeri naturali che non hanno fattori comuni.

$2 = p^2/q^2$ =>

=> $2q^2 = p^2$ =>

=> p è pari (infatti dispari^2 = dispari), c'è un intero r : p = 2r =>

=> $2q^2 = p^2 = 4r^2$ =>

=> $q^2 = 2r^2$ =>

=> q è pari =>

=> p e q hanno il fattore 2 in comune

Questa è una contraddizione. Perciò $\sqrt{2}$ è un irrazionale.

Universale: vogliamo provare che $\forall x P(x)$. Dobbiamo provare che la proprietà vale per tutti i valori nel domino. Questa dimostrazione può essere complicata. Si può richiede l'analisi dei casi (con suddivisione della dimostrazione per sottogruppi) per avere un aiuto in più.

Esempio: Se n ed m sono dispari, allora n + m è pari.
dim:
Assumiamo che l'ipotesi sia vera, cioè n ed m siano dispari, Allora n = 2k + 1 e n = 2h + 1 dove k ed h sono due qualunque interi. Quindi n + m = (2k + 1) + (2h + 1) = 2k + 2h + 2. Perciò n + m è pari.

In questa dimostrazione non viene fatta alcuna restrizione sugli interi n ed m se non l'ipotesi dell'implicazione: n ed m sono interi arbitrari. Quindi la dimostrazione precedente prova anche:
$\forall n, m \in Z(\text{se n ed me sono dispari, allora n +m è pari})$.

Negazione quantificatore universale: vogliamo provare che $\neg\forall x P(x) \equiv \exists x \neg P(x)$. I controesempi sono simili alla dimostrazione costruttiva di esistenzialità.

Errori
Le dimostrazioni sbagliate spesso nascono da operazioni matematiche sbagliate. Consideriamo la seguente dimostrazione sbagliata che dice: 2 = 1.
Sia a = b
$a^2 = ab$ (moltiplichiamo per entrambi i lati)
$a^2 + a^2 – 2ab = ab + a^2 – 2ab$ (aggiungiamo $a^2 – 2ab$ ad entrambi i lati)
$2(a^2 – ab) = (a^2 – ab)$ (dividiamo entrambi i lati per $(a^2 – ab)$)
2 = 1
Che cosa c'è di sbagliato? L'errore si trova nel momento che dividiamo, perché è come se dividessimo per 0.

INDUZIONE MATEMATICA

Dimostrazioni

Metodi dimostrativi di base: diretto, indiretto (per assurdo), equivalenza, analisi dei casi.
Dimostrazioni di asserzioni quantificate:

- Esiste un x con una qualche proprietà P(x), in questo caso è sufficiente trovare un elemento per il quale la proprietà vale.
- Per tutte le x vale la proprietà P(x), in questo caso la dimostrazione è in genere più complessa, e deve valere per tutte le x.

Induzione matematica: è una tecnica che può essere applicata per provare asserzioni generali per insiemi di interi positivi, per sequenze associate ad interi.

Induzione matematica

L'induzione matematica è usata per provare asserzioni con dominio Z^+ della forma $\forall n\, P(n)$.
L'induzione matematica consiste in due passi:

- **Base:** la proposizione P(1) è vera.
- **Passo di induzione:** fissato un intero positivo n, l'implicazione $P(n) \rightarrow P(n + 1)$ è vera. L'assunzione P(n) è chiamata **ipotesi induttiva**. Si conclude perciò che $\forall n\, P(n)$.

Nota che:

- dalla Base so che P(1) è vera
- dal Passo di induzione so che $P(1) \rightarrow P(2)$ è vera (perché P(1) è vera)
- dal Passo di induzione so che $P(2) \rightarrow P(3)$ è vera (perché P(2) è vera)
- …
- Quindi P(n) è vera $\forall n \in Z^+$

Esempio: Provare che la somma dei primi n interi positivi dispari è n^2
cioè $1 + 3 + 5 + 7 + \ldots + (2n - 1) = n^2$

dim:
$P(n) : 1 + 3 + 5 + 7 + \ldots + (2n - 1) = n^2$
Base: Mostrare che P(1) è vera, è banale infatti: $1 = 1^2$
Passo di induzione: Mostrare che se *P(n) è vera* allora *P(n + 1)* è vera per un qualunque fissato n.

- Supponiamo che P(n) è vera: $1 + 3 + 5 + 7 + \ldots + 2(n - 1) = n^2$
- Mostriamo che P(n + 1) è vera:
  $1 + 3 + 5 + 7 + \ldots + 2(n - 1) + [2 (n+ 1) - 1] = (n + 1)^2$
  per ipotesi induttiva sappiamo che $1 + 3 + 5 + 7 + \ldots + 2(n - 1) = n^2$ quindi:
  $n^2 + [2 (n+ 1) - 1] = (n + 1)^2$
  $n^2 + [2n + 2 - 1] = (n + 1)^2$
  $n^2 + 2n - 1 = (n + 1)^2$
  $(n + 1)^2 = (n + 1)^2$
  Quindi anche per P(n + 1) la proposizione vale.

Correttezza dell’induzione matematica

Supponiamo che:

- $P(1)$ è vera
- $P(n) \rightarrow P(n + 1)$ è vera per tutti gli interi positivi

vogliamo quindi provare che $\forall n\ P(n)$ è vera.

dim:

Per contraddizione, assumiamo che c’è almeno un intero positivo **m** : **P(m) è falsa**.

S = insieme di tutti gli interi positivi n per i quali P(n) è falsa

Così $S \neq \emptyset$

Proprietà del buon-ordinamento: ogni insieme non vuoto di interi positivi ha almeno un elemento.

S ha almeno un elemento, diciamo k, con $k > 1$, **nota:** $k \neq 1$ poiché P(1) è vera.

Sia poi k il più piccolo intero in S : P(k) è falsa.

Questo implica che $k – 1 > 0$ e $P(k – 1)$ è vera.

Ma $P(k – 1) \rightarrow P(k)$ è vera per ipotesi. Siamo arrivati quindi ad una contraddizione $\rightarrow \forall n\ P(n)$ è vera.

Esempio 1: Proviamo che $n < 2^2$ per tutti gli interi positivi n.

dim: P(n): $n < 2^n$ per ogni intero $n \geq 1$

Base: P(1): $1 < 2^1$ (ovvio)1

Passo di induzione: mostrare che se P(n) è vera allora P(n + 1) è vera per tutti gli n

- Supponiamo P(n): $n < 2^n$ è vera
- Mostriamo che P(n + 1): $n + 1 < 2^{n+1}$ è vera
- $n + 1 < 2^n + 1$ sappiamo per ipotesi induttiva che $n < 2^n$ quindi:

  $2^n + 1 < 2^n + 2^n$ ($2^n + 1$ è sicuramente minore di $2^n + 2^n$)

  $= 2\ 2^n = 2^{n+1}$

  Quindi anche per P(n + 1) la proposizione vale.

Esempio 2: Proviamo che $n^3 – n$ è divisibile per 3, per ogni intero positivo n.

dim: P(n): $n^3 – n$ è divisibile per 3 per ogni intero $n \geq 1$

Base: P(1): $1^3 – 1 = 0$ è divisibile per 3 (ovvio)

Passo di induzione: mostrate che se se P(n) è vera allora P(n + 1) è vera per tutti gli n

- Supponiamo P(n) : $n^3 – n$ è divisibile per 3 (ipotesi induttiva)
- Mostriamo che P(n + 1): $(n + 1)^3 – (n + 1)$ è divisibile per 3
- $(n + 1)^3 – (n + 1) = n^3 + 3n^2 +3n + {}^1 - n – 1 =$

$(n^3 – n) + 3n^2 + 3n =$ $\underbrace{(n^3 - n)}_{divisibile\ per\ 3\ (ipotesi\ induttiva)} + 3\underbrace{(n^2 + n)}_{divisibile\ per\ 3}$.

Quindi anche per P(n + 1) la proposizione vale.

Induzione matematica (generalizzazioni)

Si può usare l’induzione matematica anche quando si vuole provare che:

P(n) è vera con n = b, b + 1, b + 2, …   dove b è un intero

I due passi dell’induzione diventano:

- **Base:** la proposizione P(b) è vera
- **Passo di induzione:** fissato un intero $n \geq b$, l’implicazione $P(n) \rightarrow P(n + 1)$ è vera.

Nota: b può essere negativo, zero o positivo.

Esercizio 1: Proviamo che $n^2 < 2^n$ per tutti gli interi $n \geq 5$.
dim: P(n): $n^2 < 2^n$ per tutti gli interi $n \geq 5$
Base: P(5) è vera, infatti $5^2 < 2^5 = 25 < 32$ (ovvio)
Passo di induzione:mostrate che se P(n) è vera allora P(n + 1) è vera per $n \geq 5$.

- Supponiamo $n^2 < 2^n$ è vera, ipotesi induttiva
- Mostriamo che P(n + 1): $(n + 1)^2 < 2^{n+1}$ è vera quindi:
- $(n + 1)^2 = n^2 + 2n + 1 < n^2 + 2n + n$ (perché $n \geq 5 > 1$)

$= n^2 + \mathbf{3}n < n^2 + n*n = n^{2+} n^2$ (perché $n \geq 5 > 3$)
$= 2\ n^2 < 2\ 2^n = 2^{n+1}$ (per ipotesi induttiva $n^2 < 2^n$)
Quindi anche per P(n + 1) la proposizione vale.

Esercizio 2: provare per induzione che per gli interi non negativi $1 + 2 + 2^2 + \ldots + 2^n = 2^{n+1} - 1$
dim: P(n): $1 + 2 + 2^2 + \ldots + 2^n = 2^{n+1} - 1$ per ogni intero $n \geq 0$.
Base: P(0): $2^0 = 1 = 2^1 - 1$
Passo di induzione:

- Supponiamo che P(n) è vera (ipotesi induttiva)
- Mostriamo che P(n + 1): $1 + 2 + 2^2 + \ldots + 2^n\ 2^{n+1} = 2^{(n+1)+1} - 1$ è vera:

$1 + 2 + 2^2 + \ldots + 2^n\ 2^{n+1} = 2^{n+2} - 1$
per ipotesi induttiva $1 + 2 + 2^2 + \ldots + 2^n = 2^{n+1-}\ 1$ quindi abbiamo:

- $2^{n+1} - 1 + 2^{n+1} = 2^{n+2} - 1$

uso la proprietà commutativa e ho:
$2^{n+1} + 2^{n+1-}\ 1 = 2^{n+2} - 1$ ripeto 2 volte 2^{n+1} quindi ho:
$2\ 2^{n+1} - 1 = 2^{n+2} - 1$
$2^{n+1+1} - 1 = 2^{n+2} - 1$
$2^{n+2} - 1 = 2^{n+2} - 1$
Quindi anche per P(n + 1) la proposizione vale.

Esercizio 3: Provare per induzione che un insieme con n elementi ha 2^n sottoinsiemi.
Dim: P(n): un insieme con n elementi ha 2^n sottoinsiemi
Base: proviamo P(0)
Se un insieme ha 0 elementi allora esso è l'insieme vuoto. L'insieme vuoto $1 = 2^0$ sottoinsiemi (solo se stesso).
Passo di induzione:

- Supponiamo che P(n) è vera (ipotesi induttiva).
- Mostriamo che P(n + 1) è vera: sia T un insieme con n + 1 elementi, sia a un qualunque elemento di T → T = S U {a} dove |S| = n
- I sottoinsiemi di T possono essere ottenuti in questo modo:
  - per ogni sottoinsieme X di S, ci sono 2 sottoinsiemi di T, cioè X e X U {A}
  - tali insiemi sono tutti distinti
  - Quindi ci sono 2 sottoinsiemi di T per ogni sottoinsiemi di S
  - Il numero di sottoinsiemi di T = 2 (numero di sottoinsiemi di S) = $2\ 2^n = 2^{n+1}$

Induzione forte

L'induzione regolare usa:

- il passo base: P(1)
- il passo di induzione $P(n) \rightarrow P(n + 1)$

L'induzione forte usa:

- il passo base: P(1)
- il passo di induzione $[P(1) \wedge P(2) \wedge \ldots \wedge P(n)] \rightarrow P(n + 1)$

Esempio 1: mostriamo che un intero positivo più grande di 1 è un primo o può essere scritto come il prodotto di primi.
P(n): un intero positivo $n > 1$ o è primo o può essere scritto come il prodotto di primi.
dim:
Base: P(2) è vera, infatti 2 = 2 (ovvio)
Passo di induzione: Assumiamo vere P(2), … , P(n); dimostriamo che P(n + 1) è anch'essa vera (ipotesi induttiva)
Distinguiamo 2 casi:

1. Se n + 1 è esso stesso un numero primo allora P(n + 1) è banalmente vera.
2. Se n + 1 è un numero composto allora $n + 1 = a * b$. Dall'ipotesi induttiva P(a) e P(b) sono vere. Così n + 1 può scritto come il prodotto di primi.

Esempio 2: Consideriamo il gioco seguente: abbiamo 2 scatole ciascuna contenente n cerini e 2 giocatori; a turno, ciascun giocatore può eliminare da una delle scatole quanti cerini vuole; vince chi elimina l'ultimo cerino.
P(n): con n cerini per scatola, il giocatore che gioca per secondo può vincere.
Proviamo che P(n) è vera, per ogni intero positivo n.

dim:
Base: n = 1 abbiamo:

- il primo giocatore ha una sola scelta: togliere l0unico cerino da una delle due scatole.
- Il secondo giocatore togliendo l'unico ed ultimo cerino della seconda scatola.

Passo di induzione: Assumiamo che P(j) è vera $\forall j$ con $1 \leq j \leq n$. Dimostriamo che P(n + 1) è anch'essa vera.

- Supponiamo allora che ci sono n + 1 cerini in ciascuna delle due scatole all'inizio del gioco.
  Sia c il numero di cerini che il *primo giocatore* elimina da una delle due scatole → che in tale scatola *rimangono $n + 1 - x$* cerini.
  Se il *secondo giocatore* elimina esattamente *x* cerini dall'altra scatola → nell'altra scatola *rimangono $n + 1 - x$* cerini.

Queste due affermazioni → che ci ritroviamo con due scatole ciascuna avente $n + 1 - x$ cerini. Per ipotesi induttiva $P(n +1 - x)$ è vera, cioè il giocatore che gioca per secondo può vincere → P(n + 1) vera.

Schema per le dimostrazioni per induzione

- Formula un predicato che descrive il problema in funzione di un intero n e individua P(n).
- Esprimi ciò che deve essere provato come **∀n ≥ b**, P(n); bisogna individuare sempre il **b** più adatto al problema.

Suddividere poi la dimostrazione in: *passo base*, *ipotesi induttiva* e *passo di induzione*:

- **Base:** mostrare che P(b) è vera.
- **Ipotesi induttiva:** Esprimi in modo chiaro la proposizione "Assumiamo che P(n) è vera per un arbitrario n ≥ b".
- **Passo di induzione:** Affermare ciò che si deve provare (Scrivere in maniera esplicita che cosa dice P(n + 1). Provare P(n + 1) facendo uso dell'ipotesi induttiva P(n).

Nota su dimostrazioni per induzione

Le dimostrazioni per induzione nascono spesso da situazioni che non riflettono esattamente lo schema dato precedentemente.
2 cose sono sicure:

- P(n+1) deve essere provata vera, usando il fatto che P(m) è vera per un qualunque insieme di interi m ≤ n
- La base deve provare la veridicità di P(*) per il più piccolo (talvolta più di uno) valore consentito ad n.

RICORSIONE

Dato un oggetto si pensi a funzioni, insiemi, algoritmi, … in alcuni casi esso può essere definito in termini di se stesso, ma di più piccole dimensioni. A volte è difficile definire un oggetto in maniera esplicita, mentre è più semplice definirlo in maniera ricorsiva.

Definizioni ricorsive

Esempio 1: consideriamo la sequenza di interi 1, 3, 9, 27, 81, …
È evidente che è la sequenza di potenze di 3, cioè:

- 1, 2, 9, 27, 81, … , 3^n
- $3^0, 3^1, 3^2, 3^3, 3^4, \dots, 3^n$
- impostiamo una variabile $b_n = 3^n$ (n-esimo termine della sequenza), n ∈ N.

Definiamo ricorsivamente la sequenza di potenze di 3: $b_n = 3 * 3^{n-1}$

Quindi abbiamo: $\begin{cases} b_n = 3 * b_{n-1} & per\, n \geq 1 \\ b_0 = 1 & per\, n = 0 \end{cases}$

Esempio 2: consideriamo la sequenza aritmetica (progressione aritmetica)
a, a +d, a + 2d, a + 3d, …, a + nd con a = -1 e d = 4 abbiamo:
-1, 3, 7, 11, …, -1 + n4
impostiamo una variabile $b_n = a + nd$ (n-esimo termine della sequenza), n ∈ N.
Definiamo ricorsivamente la sequenza: $b_n = a + (n - 1)d + d$

Quindi abbiamo: $\begin{cases} b_n = b_{n-1} + d & per\, n \geq 1 \\ b_0 = a & per\, n = 0 \end{cases}$

Esempio 3: consideriamo la sequenza geometrica (progressione geometrica)
a, ar, ar^2, ar^3, …, ar^n con a = 6 e r = 1/3 abbiamo:
6, 2, 2/3, 2/9, …, $6(1/3)^n$
impostiamo una variabile $b_n = ar^n = a\, r^{n-1}$(n-esimo termine della sequenza), n ∈ N.
Definiamo ricorsivamente la sequenza: $b_n = ar^n = a\, r^{n-1} * r$

Quindi abbiamo: $\begin{cases} b_n = b_{n-1} + r & per\, n \geq 1 \\ b_0 = a & per\, n = 0 \end{cases}$

In alcuni casi la definizione ricorsiva di un oggetto può essere molto facile da scrivere:
Per esempio il fattoriale:

$n! = \begin{cases} n*(n-1)! & per\, n \geq 1 \\ 1 & per\, n = 0 \end{cases}$ infatti 0! = 1.

Mentre in altri casi la definizione ricorsiva di un oggetto è l'unico modo per descriverlo:
Per esempio i numeri di Fibonacci:

$Fib(n) = \begin{cases} Fib(n-1) + Fib(n-2) & per\, n \geq 2 \\ 1 & per\, n = 1 \\ 0 & per\, n = 0 \end{cases}$ si può scrivere anche come: $F_n = F_{n-1} + F_{n-2}$ per $n \geq 2$, $F_1 = 1$, $F_0 = 0$

Definire funzioni ricorsive

Per definire una funzione ricorsiva sull'insieme degli interi non negativi si devono seguire due passi:

- **Passo base:** Specificare il valore della funzione in 0
- **Passo ricorsivo:** Dare una regola per determinare il valore della funzione in n in termini del valore della funzione in interi n-1

Un esempio ne è il fattoriale: $n! = \begin{cases} n*(n-1)! & per\, n \geq 1 \\ 1 & per\, n = 0 \end{cases}$

Esercizio 1: definire ricorsivamente la funzione: f(n) = 2 n + 1
f(0) = 1
f(1) = 2 • 1+ 1= 3 = 1 + 2 = f(0) + 2
f(2) = 2 • 2+ 1= 5 = 3 + 2 = f(1) + 2
f(3) = 2 • 3+ 1= 7 = 5 + 2 = f(2) + 2
…
f(n) = 2n + 1 = dai risultati precedenti notiamo che si può scrivere come 2 (n – 1 + 1) +1 =
= 2(n – 1) + 1 + 2 = f(n – 1) + 2
Quindi:
il caso base è f(0) = 1 e il passo ricorsivo è f(n) = f(n – 1) + 2 per n 1.

Esercizio 2:
definire ricorsivamente la funzione che somma i primi n interi positivi f(n) = 1 + 2 + 3 + …. + n per n ≥ 1
Abbiamo che:
f(1) = 1
f(2) = 1 + 2 = 3 = 1 + 2 = f(1) + 2
f(3) = 1 + 2 + 3 = 6 = 3 + 3 = f(2) + 3
…
f(n) = 1 + 2 + 3 + … + n - 1 + n = f(n – 1) + n
Quindi:
Caso base : f(1) = 1, passo ricorsivo: f(n) = f(n – 1) + n per n ≥ 2

Esercizio 3: definire ricorsivamente la funzione $f(n) = n^2$ per $n \geq 1$
Abbiamo che:
$f(1) = 1$
$f(2) = 2^2 = 4 = 1 + (2 * 2) – 1 = f(1) + 2 * 2 - 1$
$f(3) = 3^2 = 9 = 4 + (2 * 3) – 1 = f(2) + 2 * 3 - 1$
…
$f(n) = n^2 = (n – 1) + (2 * n) – 1 = f(n – 1) + 2n – 1$
Quindi:
Caso base : $f(1) = 1$, passo ricorsivo: $f(n) = f(n – 1) + 2n – 1$ per $n \geq 2$

Calcolo di funzioni ricorsive

Esempio 1: sia f una funzione ricorsiva definita come:

1. **Passo base:** $f(0) = 3$
2. **Passo ricorsivo:** $f(n) = 2 f(n – 1) + 3$ per $n \geq 1$

Qual è il valore di $f(3) = ?$

- $f(3) = 2 f(2) + 3$ Passo ricorsivo
- $f(2) = 2 f(1) + 3$ Passo ricorsivo
- $f(1) = 2 f(0) + 3$ Passo ricorsivo
- $f(0) = 3$ Passo base
- $f(1) = 2 * 3 + 3 = 9$
- $f(2) = 2 * 9 + 3 = 21$
- $f(3) = 2 * 21 + 3 = 45$

Esempio 2: Funzione fattoriale

1. **Passo base:** $0! = 1$
2. **Passo ricorsivo:** $n! = n(n – 1)!$ per $n \geq 1$

Calcolare 4!:

- $4! = 4 * 3!$ Passo ricorsivo
- $3! = 3 * 2!$ Passo ricorsivo
- $2! = 2 * 1!$ Passo ricorsivo
- $1! = 1 * 0!$ Passo ricorsivo
- $0! = 1$ Passo base
- $1! = 1$
- $2! = 2$
- $3! = 6$
- $4! = 24$

Esempio 3:

1. **Passo base:** $f(1) = 1$
2. **Passo ricorsivo:** $f(n)= f(n-1) +2n-1$ per $n \geq 2$

Qual è il valore f(4)?

- $f(4) = f(3) + 2 * 4 – 1$ Passo ricorsivo
- $f(3) = f(2) + 2 * 3 – 1$ Passo ricorsivo
- $f(2) = f(1) + 2 * 2 – 1$ Passo ricorsivo
- $f(1) = 1$ Passo base
- $f(2) = 4$
- $f(3) = 9$
- $f(4) = 16$

Uso della ricorsione

Un ***algoritmo*** è detto ***ricorsivo*** se risolve un problema riducendo esso ad una istanza dello stesso problema ma con un input più piccolo.

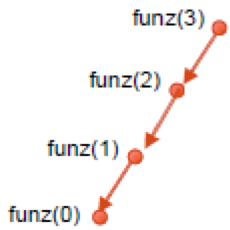
```
procedure funz(n)
        if n = 0 then return 3
        else return 2 * funz(n – 1) + 3
```

Esempio:

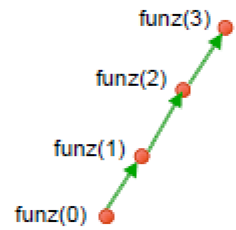
- **Caso base:** f(0) = 3
- **Passo ricorsivo:** f(n) = 2 * f(n – 1) + 3   per n ≥ 1

Calcolo di funz(3):

f(3) = 2 * f(2) + 3
f(2) = 2 * f(1) + 3
f(1) = 2 * f(0) + 3
f(0) = 3



f(0) = 3
f(1) = 2 * 3 + 3 = 9
f(2) = 2 * 9 + 3 = 21
f(3) = 2 * 21 + 3 = 45



Algoritmi ricorsivi

Correttezza: produce un output corretto per ogni possibile input.

Esempio 1: Proviamo la correttezza dell'algoritmo descritto dalla procedura funz(n).
Dimostriamo che il valore restituito dalla procedura *funz(n)* coincide con *f(n)*.
dim: Usiamo l'induzione matematica su n.

- **Passo base:** se n = 0, il primo passo dell'algoritmo dice che il valore restituito da funz(0) è 3. Corretto perché f(0) = 3.
- **Ipotesi induttiva:** per un n intero positivo arbitrario, l'algoritmo computa correttamente f(n), cioè funz(n) restituisce f(n).
- **Passo di induzione:** Ora mostriamo che la procedura funz(n + 1) computa correttamente anche f(n + 1):

La procedura funz(n + 1) restituisce 2 funz(n) + 3. Per ipotesi induttiva funz(n) coincide con f(n), quindi abbiamo:

2 funz (n – 1) + 3 = 2 f(n – 1) + 3 coincide con 2 funz(n) + 3 = 2 f(n) + 3 che è uguale a f(n + 1)

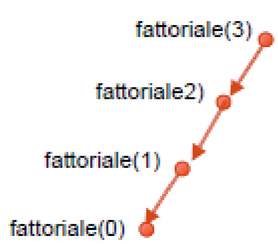
Esempio 2: funzione fattoriale

```
procedure fattoriale(n)
        if n=0 then return 1
        else return n * fattoriale(n–1)
```

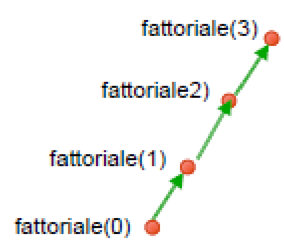
- **Caso base:** 0! = 1
- **Passo ricorsivo:** n! = n (n – 1)!   per n ≥ 1

Calcolo di fattoriale(3):

fattoriale(3) = 3 * fattoriale(2)
fattoriale(2) = 2 * fattoriale(1)
fattoriale(1) = 1 * fattoriale(0)
fattoriale(0) = 1



fattoriale(0) = 1
fattoriale(1) = 1 * 1 = 1
fattoriale(2) = 2 * 1 = 2
fattoriale(3) = 3 * 2 = 6



Dimostriamo che il valore restituito dalla procedura fattoriale(n) coincide con n!.
dim: Usiamo l'induzione matematica su n.

- **Passo base:** se n = 0, il primo passo dell'algoritmo dice che il valore restituito da fattoriale(0) è 1. Corretto perché 0! = 1.
- **Ipotesi induttiva:** per un n intero positivo arbitrario, l'algoritmo computa correttamente n!, cioè fattoriale(n) restituisce n!.
- **Passo di induzione:** Ora mostriamo che la procedura fattoriale(n + 1) computa correttamente anche (n + 1)!:

La procedura fattoriale(n + 1) restituisce (n + 1) * fattoriale(n) .
Per ipotesi induttiva (n + 1) * fattoriale(n) coincide con (n + 1)!

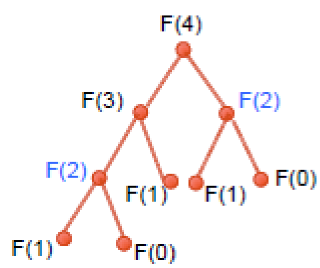
Esempio 3: Numeri di Fibonacci

- **Casi base:** F(0) = 0, F(1) = 1
- **Passo ricorsivo:** F(n) = F(n – 1) + F(n – 2) per $n \geq 2$

```
procedure Fibonacci(n)
        if n = 0 then return 0
        else if n = 1 then return 1
                else return Fibonacci(n − 1) + Fibonacci(n − 2)
```

Calcolo di Fibonacci(4):
Fibonacci(4) = **Fibonacci(3)** + *Fibonacci(2)*
Fibonacci(3) = Fibonacci(2) + Fibonacci(1)
Fibonacci(2) = Fibonacci(1) + Fibonacci(0)
Fibonacci(1) = 1 Fibonacci(0) = 0

Fibonacci(2) = Fibonacci(1) + Fibonacci(0)
Fibonacci(1) = 1 Fibonacci(0) = 0



Nota: non sempre gli algoritmi ricorsivi sono efficienti, essi però sono semplici da progettare.
Nel calcolo di Fibonacci(4) con l'algoritmo ricorsivo valutiamo due volte Fibonacci(2). Infatti:
Fibonacci(4)= Fibonacci(3) + *Fibonacci(2)*= (Fibonacci (2) + Fibonacci(1)) + *Fibonacci(2)*.

Consideriamo ora una procedura iterativa per il calcolo dei numeri di Fibonacci:

- **Casi base:** F(0) = 0, F(1) = 1
- **Passo ricorsivo:** F(n) = F(n – 1) + F(n – 2) per $n \geq 2$

```
Procedure Fibonacci-iterativa(n)
        if n=0 then return 0
        else if n=1 then return 1
                else x=0, y=1
                        for i=2 to n do
                                z= x+y
                                x=y
                                y=z
        return y
```

x e y conterranno sempre x = F(n - 2) y = F(n - 1)
F(n) = z = x + y = F(n - 2) + F(n - 1)
Per prepararsi alla prossima iterazione (calcolare F(n+1)), dobbiamo aggiornare x e y: x dovrà contenere F(n-1) e y dovrà contenere F(n).

Ciascun numero di Fibonacci viene calcolato esattamente una volta.

Uso di definizioni ricorsive - insiemi

Le definizioni ricorsive possono essere usate nelle dimostrazioni.

Esempio: sia f(n) n-simo termine della sequenza dei numeri di Fibonacci. Provare che per $n \geq 3$:

$$F(n) > a^{n-2} \text{ dove } a = (1+\sqrt{5})/2$$

dim: usiamo l'induzione forte

- **Passo base:**
  - $F(3) = F(2) + F(1) = 1+1 = 2 > (1+\sqrt{5})/2 = \alpha$
  - $F(4) = F(3) + F(2) = 2+1 = 3 > [(1+\sqrt{5})/2]^2 = \alpha^2$
- **Ipotesi induttiva:** Assumiamo che per $3 \leq j \leq n$ con $n \geq 3$ si ha $F(j) > a^{j-2}$
- **Passo di induzione:** consideriamo ira $F(n + 1)$ e la sua definizione, poi applichiamo l'ipotesi induttiva, quindi: $F(n + 1) = F(n - 1) + F(n) > a^{n-3} + a^{n-2} = a^{n-3}(1 + a) = a^{n-3}\, a^2 = a^{n-1}$

Ricorda: un insieme può essere definito:

- Elencando i suoi elementi: {a, b, c} ha elementi a, b, c
- specificando le proprietà caratteristiche di suoi elementi: A = { w | w ha la proprietà P}

Un altro modo per descrivere insiemi è attraverso una definizioni ricorsiva.

Un insieme A è definito ricorsivamente nel modo seguente:
Passo base: Si definiscono uno o più oggetti elementari.
Passo ricorsivo: definisce la regola che permette di costruire oggetti più complessi in termini di quelli già definiti dell'insieme.

Nota: gli elementi dell'insieme sono definiti esclusivamente dalle regole date.

Esempio: sia A un sottoinsieme di interi definito ricorsivamente come segue:

- **Passo base:** $1 \in A$
- **Passo ricorsivo:** se $x \in A$ allora $x+2 \in A$

Quali sono gli elementi di A?

- $1 \in A$ **passo base**
- Applico il **passo ricorsivo**: $x = 1 \in A$ allora $x+2 = 1+2 = 3 \in A$
- Applico il **passo ricorsivo**: $x = 3 \in A$ allora $x+2 = 3+2 = 5 \in A$
- $1, 3, 5, 7, 9, \ldots \in A$

Più avanti questa regola sarà provata con l'induzione strutturale, in cui diremo che l'insieme A è l'insieme degli interi dispari positivi.

Uso di definizioni ricorsive - insiemi di stringhe

Le definizioni ricorsive possono essere usate per descrivere insiemi di stringhe. Un **alfabeto** è un insieme finito di elementi (chiamati lettere o simboli). Esempi:

- L'alfabeto delle lettere romane minuscole è: $\Sigma = \{a,b,\ldots,z\}$.
- L'alfabeto delle cifre arabe è: $\Sigma = \{0,1,\ldots,9\}$.
- L'alfabeto binario è: $\Sigma = \{0,1\}$.
-

Nota: Σ = sigma, λ = lambda, w = word (parola), **l**(w) = lunghezza di una parola

L'insieme di stringhe Σ^* sull'alfabeto Σ è definito ricorsivamente nel seguente modo:
Passo base: la stringa vuota $\lambda \in \Sigma^*$
Passo ricorsivo: se $w \in \Sigma^*$ e $x \in \Sigma$ allora $wx \in \Sigma^*$

Esempio: Sia $\Sigma = \{0, 1\}$. Σ^* è l'insieme di tutte le stringhe binarie.
Infatti, $\lambda \in \Sigma^*$ applicando il passo base
0 e $1 \in \Sigma^*$ applicando la prima volta il passo ricorsivo
$00, 01, 10, 11 \in \Sigma^*$ con la seconda applicazione.

Le definizioni ricorsive possono essere usate *per ottenere nuove definizioni ricorsive*.
La lunghezza **l**(w) di una parola **w** è definita come il numero di caratteri di cui **w** è costituita.
Es: $\Sigma = \{a, b, \ldots, z\}$ zaino $\in \Sigma^*$ **l**(zaino) = 5

La sua definizione ricorsiva è:

La lunghezza di una parola in Σ^* sull'alfabeto Σ è definito ricorsivamente nel seguente modo:
Passo base: **l**(λ) = 0
Passo ricorsivo: se $w \in \Sigma^*$ e $x \in \Sigma$ allora **l**(wx) = **l**(w) + 1

Le definizioni ricorsive possono essere usate *per descrivere parole palindrome*. Una stringa è palindroma se letta da sinistra a destra o da destra a sinistra da luogo alla stessa sequenza.
Esempio: alla, otto, ingegni, Anna, ottetto, etc.

Per semplicità daremo ora una definizione ricorsiva per un piccolo alfabeto $\Sigma = \{a, b\}$:

L'insieme delle parole palindrome $\Sigma = \{a, b\}$ è definito ricorsivamente nel seguente modo:
Passo base: a, b, λ sono parole palindrome
Passo ricorsivo: se w è una parola palindroma allora anche a**w**a e b**w**b sono parole palindrome

Esempio:

- λ è una parola palindroma **passo base**
- bλb = bb è una parola palindroma **passo ricorsivo**
- a bb a è una parola palindroma **passo ricorsivo**

Uso di definizioni ricorsive – espressioni aritmetiche

Le definizioni ricorsive possono essere usate per descrivere espressioni aritmetiche.

Un'espressione aritmetica è definita ricorsivamente nel seguente modo:
Passo base: i *numeri* (interi o reali) e le *variabili* sono espressioni aritmetiche
Passo ricorsivo: se E_1 ed E_2 sono espressioni aritmetiche allora $(E_1 + E_2)$, $(E_1 – E_2)$, $(E_1 \times E_2)$, $(E_1 \setminus E_2)$ sono espressioni aritmetiche. Se E è un'espressione aritmetica allora (- (E)) e un'espressione aritmetica.

Uso di definizioni ricorsive – strutture dati

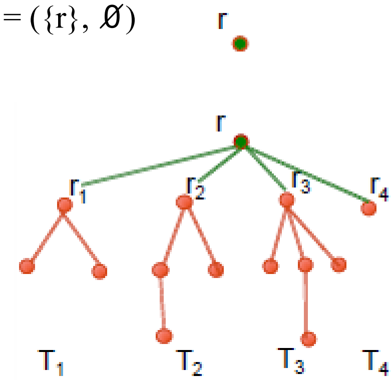
Le definizioni ricorsive possono essere usate per descrivere strutture dati. Un *albero radicato* è un albero contenente un vertice particolare detto **radice**.

Un albero radicato può essere descritto ricorsivamente nel modo seguente:
Passo base: un singolo vertice *r* è un albero radicato
Passo ricorsivo: supponiamo che $T_1, T_2, \ldots, T_n$ sono alberi radicati disgiunti con radici $r_1, r_2, \ldots r_n$, allora il grafo formato dalla radice *r*, che non è in nessuno degli alberi radicati $T_1, T_2, \ldots, T_n$, ottenuto connettendo con un arco *r* a ciascun $r_1, r_2, \ldots, r_n$ è anch'esso un albero radicato.

Più formalmente, un albero radicato T = (V, E) è definito:

Passo base: un singolo vertice r è un albero radicato T = ({r}, ∅)

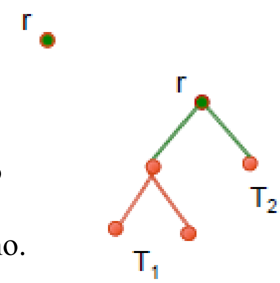
Passo ricorsivo: supponiamo che:
$T_1 = (V_1, E_1)$ $T_2 = (V_2, E_2)$ … $T_n = (V_n, E_n)$
sono alberi radicati disgiunti
$V_i \cap V_j = \emptyset$ per $1 \leq i \neq j \leq n$
con radici $r_1, r_2, \dots, r_n : r_1 \in V_1, r_2 \in V_2, \dots, r_n \in V_n$
Allora, il grafo T = (V, E) con:
$V = \{r\}, \cup V_1 \cup V_2 \cup \dots \cup V_n$ e
$E = \{(r, r_1), (r, r_2), \dots, (r, r_n)\} \cup E_1 \cup E_2 \cup \dots \cup E_n$
è formato dalla radice r che non è in nessuno degli alberi radicati $T_1, T_2, \dots, T_n$.
Quindi $r \in V$ e $r \notin V_1 \cup V_2 \cup \dots \cup V_n$ è ottenuto connettendo con un arco r a ciascun r_1, $r_2, \dots, r_n$ dove $(r, r_1) \in E, (r, r_2) \in E, \dots, (r, r_n) \in E$ è anch'esso un albero radicato.



Un **albero binario pieno** è un albero radicato dove ciascun vertice ha 0 o due figli; se tali figli esistono, essi sono chiamati figlio destro e figlio sinistro.

Un albero binario pieno è descritto ricorsivamente nel seguente modo:
Passo base: un singolo vertice r è un albero binario pieno

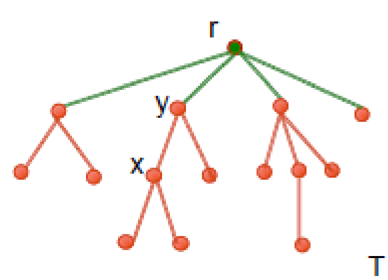
Passo ricorsivo: Se T_1 e T_2 sono alberi binari pieni, allora l'albero T formato connettendo la radice r con un arco alla radice del sottoalbero sinistro T_1 e con un altro arco alla radice del sottoalbero destro T_2 p un albero binario pieno.



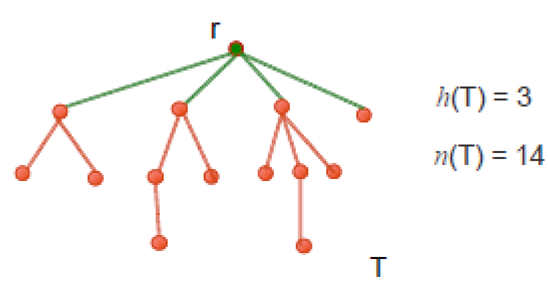
Terminologia su alberi radicati

Dato un albero radicato T con radice r si ha che:

- il **padre di un vertice x** è il primo vertice y che si incontra sul cammino da x a r
- x è detto **figlio di y**
- un vertice che non ha figli è detto **foglia**
- un vertice che non è una foglia è detto **nodo interno**



- la **profondità (o livello)** di un vertice x di T è la lunghezza del cammino che va dalla radice r a x
- **l'altezza h(T)** di T è definita la più grande profondità di un vertice in T
- il **numero di vertici n(T)** di T è n**(T) =|V|**



Definiamo ricorsivamente l'altezza di un albero radicato T.

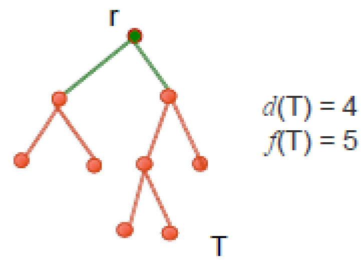
L'altezza h(T) di un albero radicato T è definito ricorsivamente come: **Passo base:** $h(T) = 0$ se T consiste della sola radice r **Passo ricorsivo:** $h(T) = 1 + \max\{h(T_1), \ldots, h(T_n)\}$ se $T_1, \ldots, T_n$ sono i sottoalberi di T

Definiamo ricorsivamente il numero di vertici di un albero radicato T.

Il numero di vertici n(T) di un albero radicato T è definito ricorsivamente come: **Passo base:** $n(T) = 1$ se T consiste della sola radice r **Passo ricorsivo:** $n(T) = 1 + n(T_1) + , \ldots, + n(T_n)\}$ se $T_1, \ldots, T_n$ sono i sottoalberi di T

Dato un albero binario pieno T = (V, E) indichiamo con:

- ***d*(T)** = il numero di vertici di T con due figli
- ***f*(T)** = il numero di foglie di T



Definiamo ricorsivamente il numero di vertici con due figli di un albero binario pieno T.

Il numero di vertici con due figli d(T) di un albero binario pieno T è definito ricorsivamente come: **Passo base:** $d(T) = 0$ se T consiste della sola radice r **Passo ricorsivo:** $d(T) = 1 + d(T_1) + d(T_2)\}$ se T_1 e T_2 sono i sottoalberi di T

Definiamo ricorsivamente il numero di foglie di un albero binario pieno T.

Il numero di foglie f(T) di un albero binario pieno T è definito ricorsivamente come: **Passo base:** $f(T) = 1$ se T consiste della sola radice r **Passo ricorsivo:** $f(T) = f(T_1) + f(T_2)\}$ se T_1 e T_2 sono i sottoalberi di T

GRAFI

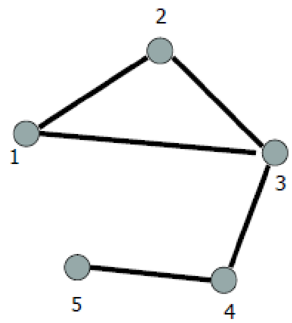
Che cosa è una rete?

Una rete è una collezione di entità che sono interconnesse attraverso dei collegamenti (link). In matematica le reti sono modellate attraverso i grafi, le **entità** sono i *nodi (vertici)*, i **link** sono gli *archi*. un ***grafo*** è un modello matematico che serve per modellare le relazioni fra oggetti. La teoria dei grafi è nata nel 18° secolo, grazie a Leonhard Euler, per risolvere il problema dei ponti di Königsberg.

Grafi non orientati

È un modello matematico definito come una coppia di insiemi (G = (V, E)) dove **V** è un insieme finito di elementi chiamati vertici, invece **E** è un insieme finito di elementi chiamati archi (edge). Un'arco $e \in E$ è una coppia di vertici (e = (u, v) $u \neq v$). ***(Questo tipo di grafo è una relazione simmetrica).***

V = {1, 2, 3, 4, 5}
E={(1,2),(1,3),(2,3),(3,4),(4,5)}



Neighborhood N(i) del nodo i, è l'insieme dei nodi adiacenti ad i:

- N(1)={2,3} N(2)={1,3} N(3)={1,2,4} N(4)={3,5} N(5)={4}

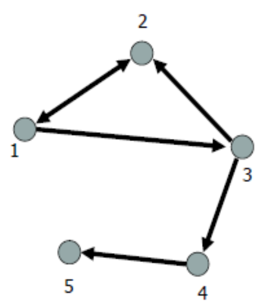
Degree (grado) d(i) del nodo i, è la size di N(i) e rappresenta il numero di archi incidenti su i:

- [d(1), d(2), d(3), d(4), d(5)] = [2,2,3,2,1]

Grafi orientati

G = (V, E) si dice orientato o diretto quando abbiamo una coppia ordinata cioè ha importanza chi sia il primo e chi sia il secondo. Possiamo dire che avnedo $e=(u,v)$ abbiamo che $u \rightarrow v$ è diversa da $v \rightarrow u$, quindi possiamo dire che abbiamo una relazione da u a v ma non è detto il viceversa. ***(Questo tipo di grafo è una relazione asimmetrica)***.

V = {1, 2, 3, 4, 5}
E={‹1,2›, ‹2,1› ‹1,3›, ‹3,2›, ‹3,4›, ‹4,5›}



in-degree $d_{in}(i)$ del nodo i, sono il numero degli archi che entrano in i:

- $[d_{in}(1), d_{in}(2), d_{in}(3), d_{in}(4), d_{in}(5)]$ = [1,2,1,1,1]

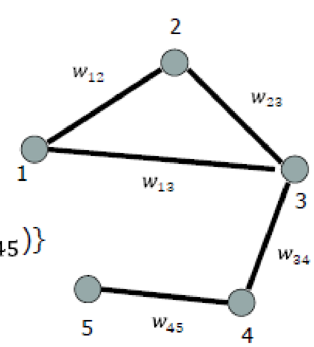
out-degree $d_{out}(i)$ del nodo i, sono il numero di archi che escono da i:

- $[d_{out}(1), d_{out}(2), d_{out}(3), d_{out}(4), d_{out}(5)]$ = [1,1,2,1,0]

Grafi pesati

G = (V, E) è un grafo avente dei pesi sugli archi che rappresentano le distanze tra un vertice x e un vertice y.

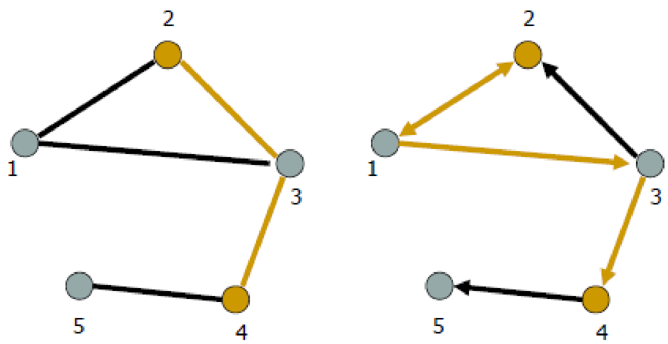
V = {1, 2, 3, 4, 5}
E={(1,2,w_{12}),(1,3, w_{13}),(2,3, w_{23}),(3,4, w_{34}),(4,5, w_{45})}



Cammini (path)

Un cammino da un nodo *i* ad un nodo *j* è una sequenza di archi (direzionati o non direzionati) dal nodo *i* al nodo *j*. Ha le seguenti caratteristiche:

- La lunghezza di un cammino è il numero di archi che fanno parte di quest'ultimo
- I nodi i e j sono connessi se esiste una path tra loro
- Un ciclo è un cammino che parte e finisce nello stesso nodo



Shortest Path

Shortest Path dal nodo i al nodo j è il cammino più corto tra tutti i cammini che congiungono i e j.

Diametro

È il più lungo shortest path nel grafo.

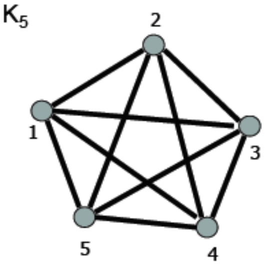
Grafo completo

Ogni nodo è connesso a tutti gli altri nodi del grafo, è chiamato clique K_n (cricca).

$$K_n = \begin{cases} V = \{v_1, v_2, \ldots, v_n\} \\ E = \{(v_i, v_j) \mid 1 \le i, j \le n \quad \text{con}\, i \ne j\} \end{cases}$$

Preso un Grafo G = (V, E) con V = {1, 2, 3, 4, 5} e E = {(1, 2), (1, 3), (1, 4), (1, 5), (2, 3), (2, 4), (2, 5), (3, 4), (3, 5), (4, 5)}

K_5

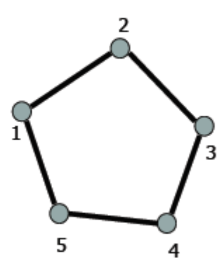


Grafo ciclico

Un grafo che consiste di un unico ciclo o in altre parole, di un certo numero di vertici connessi in una catena chiusa, si indica con C_n.

$$C_n = \begin{cases} V = \{v_1, v_2, \ldots, v_n\} \\ E = \{(v_1, v_2), (v_2, v_3), \ldots, (v_{n-1}, v_n), (v_n, v_1)\} \end{cases}$$

C_5

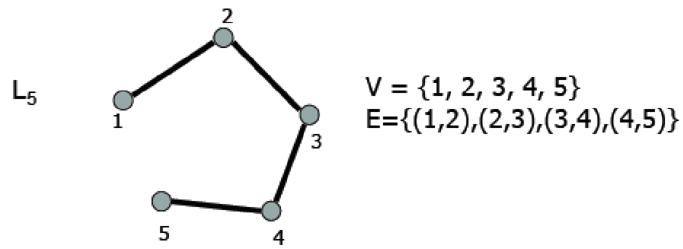


V = {1, 2, 3, 4, 5}
E={(1,2),(2,3),(3,4),(4,5),(5,1)}

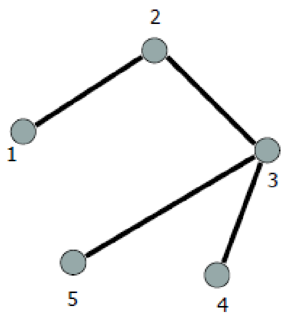
Grafo linea

Un grafo che consiste di un indica path, si indica con L_n.

$$L_n = \begin{cases} V = \{v_1, v_2, \ldots, v_n\} \\ E = \{(v_1, v_2), (v_2, v_3), \ldots, (v_{n-1}, v_n)\} \end{cases}$$



Albero

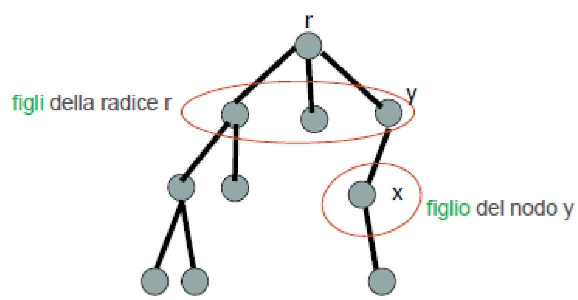


Un grafo è un albero(libero) se è connesso, non direzionato e non contiene un ciclo.

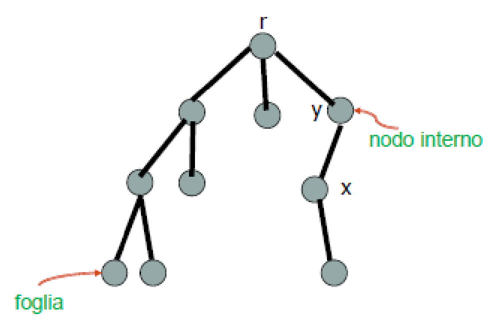
Albero radicato

Un albero con un nodo particolare chiamato radice *r*.

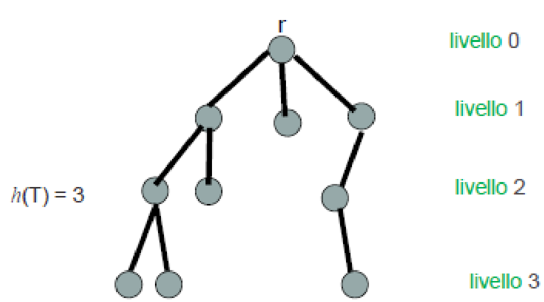
- Il padre di un vertice x è il primo vertice y che si incontra sul cammino da x a r, x è detto figlio di y.



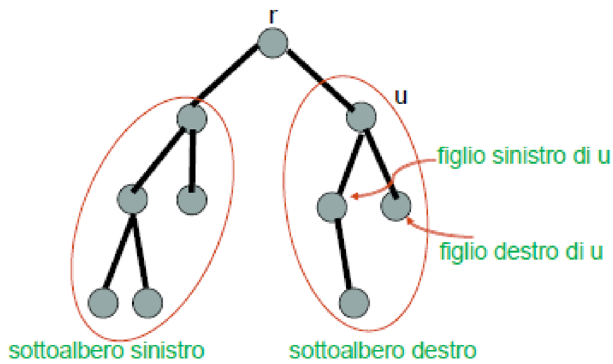
- un vertice che non ha figli è detto foglia, un vertice che non è una foglia è detto nodo interno



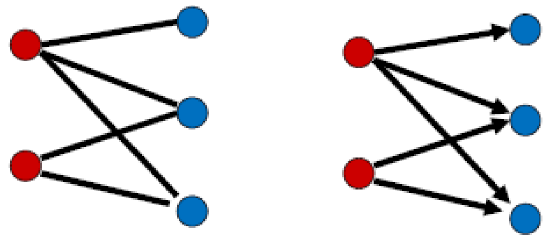
- la profondità (o livello) di un vertice x di T è la lunghezza del cammino che va dalla radice r a x
- o l'altezza h(T) di T è definita la più grande profondità di un vertice in T



Albero binario
Un albero con un nodo particolare chiamato radice, in cui ogni nodo ha soltanto due figli.



Grafo bipartito
Grafo in cui l’insieme dei vertici V può essere partizionato in due insiemi **R** e **B**, tali che ci sono archi solo tra i nodi in R e B, e non ci sono archi all’interno di **R** né all’interno di **B**.



INDUZIONE STRUTTURALE

Definizioni ricorsive ed induzione strutturale

Dovendo provare proprietà di oggetti definiti ricorsivamente può essere utile l' induzione strutturale.
Sia A = un insieme di elementi definiti ricorsivamente, e P = proprietà avente come oggetto gli elementi di A, si vuole provare che $\forall x \in A \quad P(X)$.
Con l'induzione strutturale basta provare che:

- **Passo base:** mostrare che l'enunciato P è vero per tutti gli elementi nell'insieme specificati dal passo Base della definizione ricorsiva di A.
- **Passo ricorsivo:** Mostrare che:
  se l'enunciato P è vero per ciascuno degli elementi già in A, cioè gli elementi usati per costruire nuovi elementi del passo ricorsivo della definizione di A, allora l'enunciato P è vero per questi nuovi elementi.

Esempio 1: Sia A l'insieme costituito dagli elementi definiti ricorsivamente come segue:

- **Passo base:** $1 \in A$
- **Passo ricorsivo:** se $x \in A$ allora $x+2 \in A$

Provare che A è costituito dagli interi dispari positivi.
dim:
Sia D l'insieme di tutti gli interi dispari positivi cioè: $D = \{\, y \in Z^{+} : \exists k\,(k \geq 0 \wedge y = 2k+1)\}$
Dobbiamo provare che D = A, proveremo quindi che D ⊆ A e A ⊆ D

1) Proviamo prima che D ⊆ A: procediamo usando l'induzione matematica: P(k) : 2k + 1 ∈ A ∀k ≥ 0

- **Passo base:** proviamo che P(0) è vera, 2 * 0 + 1 = 1 ∈ A
- **Ipotesi induttiva:** assumiamo che P(k) è vera
- **Passo di induzione:** proviamo che P(k + 1) è vera allora:
  $$2*(k+1)+1 = 2*(k+1+1)+1 = \underbrace{(2*k+1)}_{\text{ipotesi induttiva}} + \underbrace{2 \in A}_{\text{definizione ricorsiva}}$$

2) Ora proviamo che A ⊆ D: procediamo usando l'induzione strutturale:
P(x): x = 2k +1 per qualche intero k ≥ 0 ∀x ∈ A

- **Passo di ricorsione:** usiamo la seconda parte della definizione ricorsiva di A, e consideriamo un x + 2 ∈ A: Assumiamo che P(x) è vera, quindi proviamo che P(x + 2) è vera.
  x = 2k + 1 per qualche intero k ≥ 0
  x + 2 = 2k + 1 + 2= 2 (k +1) + 1 ∈ D

Esempio 2: Sia A un insieme definito nel modo seguente:

- **Passo base:** $3 \in A$
- **Passo ricorsivo:** se $x \in A$ e $y \in A$ allora $x + y \in A$

Provare che A è costituito dagli interi positivi multipli di 3.

dim: Sia M l'insieme di tutti i multipli di 3, cioè $M = \{ y \in Z^{+} : \exists k (k \in Z^{+} \wedge y = 3k) \}$

Dobbiamo provare che M = A, quindi proveremo $M \subseteq A$ e $A \subseteq M$

1) Proviamo prima che $M \subseteq A$: procediamo usando l'induzione matematica: P(k) : $3k \in A \quad \forall k \geq 1$

- **Passo base:** proviamo che P(1) è vera, $3 * 1 = 3 \in A$
- **Ipotesi induttiva:** assumiamo che P(k) è vera
- **Passo di induzione:** proviamo che P(k + 1) è vera allora: $3 * k + 1 = \underbrace{3 * k}_{\text{ipotesi induttiva}} + \underbrace{3 \in A}_{\text{definizione ricorsiva}}$

2) Ora proviamo che $A \subseteq M$: procediamo usando l'induzione strutturale:

P(x): x = 3k per qualche intero $k \geq 1 \quad \forall x \in A$

Usiamo la definizione ricorsiva di A:

- **Passo base:** dalla base della definizione ricorsiva sappiamo che $3 \in A$ poiché $3 = 3 * 1 \rightarrow P(3)$ è vera.
- **Passo di ricorsione:** usiamo la seconda parte della definizione ricorsiva di A, e consideriamo un $x + y \in A$: Assumiamo che P(x) è vera, quindi proviamo che P(x + y) è vera.
  $x = 3k$ e $y = 3h$ per qualche intero $k \geq 1$ e $h \geq 1$
  $x + y = 3k + 3h = 3 (k + h) \in M$

Esempio 3: siano u e w due stringhe appartenenti a Σ^{*}. Provare che $\ell(u\, w) = \ell(u) + \ell(w)$

dim:

Costruiamo la dimostrazione sulla definizione ricorsiva della stringa $w \in \Sigma^{*}$

- **Passo base:** $\lambda \in \Sigma^{*}$
- **Passo ricorsivo:** Se $w \in \Sigma^{*}$ e $x \in \Sigma^{*}$ $wx \in \Sigma$

Dobbiamo provare che $\forall w \in \Sigma^{*}$ P(w) dove P(w): $\ell(u\, w) = \ell(u) + \ell(w) \quad \forall u \in \Sigma^{*}$

- **Passo base:** dobbiamo mostrare che P(λ) è vera: $\ell(u\, \lambda) = \ell(u) + \ell(\lambda) + 0 = \ell(u) + \ell(\lambda)$
- **Passo di ricorsione:** assumiamo che P(w) sia vera, proviamo che P(wx) è vera $\forall x \in \Sigma^{*}$

$$l(uwx) \underbrace{=}_{\text{def. ricorsiva di } l} l(uw) + 1 = \underbrace{l(u) + l(w) + 1}_{\text{ipotesi indutttiva}} = \underbrace{l(u) + l(wx)}_{\text{def. ricorsiva di } l}$$

Induzione strutturale

Ricordiamo alcune definizioni ricorsive date per gli alberi. Per semplicità limitiamoci a considerare gli alberi binari pieni.

Il numero di nodi con due figli d(T) di un albero binario pieno T è definito:

- **passo base:** $d(T) = 0$ se T consiste della sola radice r
- **passo ricorsivo:** $d(T) = 1 + d(T_1) + d(T_2)$ se T_1 e T_2 sono i sottoalberi destro e sinistro di T

Il numero di foglie f(T) di un albero binario pieno T è definito:

- **passo base:** $f(T) = 1$ se T consiste della sola radice r
- **passo ricorsivo:** $f(T) = 1 + f(T_1) + f(T_2)$ se T_1 e T_2 sono i sottoalberi destro e sinistro di T

Esempio 4: Se T è un albero binario pieno, sia d(T) = il numero di vertici di T con due figli e f(T) = il numero di foglie di T allora $f(T) \le d(T) + 1$

dim: Usiamo l'induzione strutturale (definizione ricorsiva di T)

P(T) : $f(T) \le d(T) + 1$ per ogni albero binario pieno T

- **Base:** dobbiamo mostrare che se T è l'albero costituito dalla sola radice allora P(T) è vera. Sia T l'albero costituito dalla sola radice: dalla definizione di d e di f si ha: $d(T) = 0$ e $f(T) = 1$. Quindi $f(T) = 1 = 0 + 1 = d(T) + 1$

dim: Sia T un albero binario pieno costituito da più di un vertice, siano T_1 e T_2 i sottoalberi destro e sinistro di T.

- **Passo di ricorsione:** assumiamo che $P(T_1)$ e che $P(T_2)$ siano vere:

$f(T_1) \le d(T_1) + 1$ e $f(T_2) \le d(T_2) + 1$.

proviamo che P(T) è vera: $f(T) \le d(T) + 1$

Ricordando che: $f(T) = f(T_1) + f(T_2)$ e $d(T) = 1 + d(T_1) + d(T_2)$.

Quindi $f(T) = f(T_1) + f(T_2)$ **def. ricorsiva di *f***

$\le (d(T_1) + 1) + (1 + d(T_2))$ **ipotesi induttiva su T_1 e T_2**

$= (1 + d(T_1) + d(T_2)) + 1 = d(T) + 1$ **def. ricorsiva di *d***

Ricordiamo alcune definizioni ricorsive date per gli alberi. Per semplicità limitiamoci a considerare gli alberi binari pieni.

Il numero di nodi con due figli h(T) di un albero binario pieno T è definito:

- **passo base:** $h(T) = 0$ se T consiste della sola radice r
- **passo ricorsivo:** $h(T) = 1 + \max \{h(T_1), h(T_2)\}$ se T_1 e T_2 sono i sottoalberi destro e sinistro di T

Il numero di foglie n(T) di un albero binario pieno T è definito:

- **passo base:** $n(T) = 1$ se T consiste della sola radice r
- **passo ricorsivo:** $n(T) = 1 + n(T_1) + n(T_2)$ se T_1 e T_2 sono i sottoalberi destro e sinistro di T

Esempio 5: se T è un albero binario pieno, allora $n(T) \le 2^{h(T) + 1} - 1$

dim: usiamo l'induzione strutturale (definizione ricorsiva di T)

P(T): $n(T) \le 2^{h(T) + 1} - 1$ per ogni albero binario pieno T

- **passo base:** dobbiamo mostrare che se T è l'albero costituito dalla sola radice allora P(T) è vera
  Sia T è l'albero costituito dalla sola radice.
  Dalla definizione di h si ha $h(T) = 0$.
  Dalla definizione di n si ha $n(T) = 1$.
  Quindi $n(T) = 1 = 2^{0 + 1} - 1 = 2^{h(T) + 1} - 1$

dim: Sia T un albero binario pieno costituito da più di un vertice. Siano T_1 e T_2 i sottoalberi destro e sinistro di T.

- **Passo di ricorsione:** assumiamo che $P(T_1)$ e che $P(T_2)$ siano vere:

$n(T_1) \le 2^{h(T1) + 1} - 1$

$n(T_1) \le 2^{h(T2) + 1} - 1$

proviamo che P(T) è vera: $n(T) \le 2^{h(T) + 1} - 1$

$n(T) = 1 + n(T_1) + n(T_2)$ **def. ricorsiva di *n***

$\le 1 + (2^{h(T1) + 1} - 1) + (2^{h(T2) + 1} - 1)$ **ipotesi induttiva**

$= 2^{h(T1) + 1} + 2^{h(T2) + 1} - 1 \le$

$\le 2 \max\{ 2^{h(T1)+1}, 2^{h(T2)+1}\} - 1 \le 2\ 2^{\max\{ h(T1), h(T2)\} + 1} - 1 \le 2\ 2^{h(T)} - 1 = 2^{h(T) + 1} - 1$ **def. ricorsiva di *h***

RELAZIONI DI RICORRENZA

Una definizione ricorsiva di una sequenza è = a una relazione di ricorrenza.

> Data una sequenza $a_0, a_1, \ldots, a_n$, *una relazione di ricorrenza* esprime a_n in termini di uno o più dei termini precedenti della sequenza, cioè di $a_0, a_1, \ldots, a_{n-1}$, per tutti gli interi non negativi $n \geq 0$.

Affinché la relazione di ricorrenza definisca univocamente la sequenza devono essere definite le *condizioni iniziali*.

Esempio: consideriamo la sequenza geometrica: $b, br, br^2, br^3, \ldots, br^n, \ldots$
Definizione ricorsiva della sequenza:

$$\begin{cases} a_n = a_{n-1} r \quad n \geq 1 & (\textit{relazione di ricorrenza}) \\ a_0 = b & (\textit{condizione iniziale}) \end{cases}$$

Data una relazione di ricorrenza, unitamente alle condizioni iniziali, l'obiettivo è di risolvere la relazione di ricorrenza cioè trovare una formula chiusa per l'n-simo termine della sequenza (formula esplicita in n che non dipende più dai termini precedenti).
Esempio: data la relazione di ricorrenza e la sua condizione iniziale:

- $a_n = a_{n-1}\, r$ (relazione di ricorrenza)
- $a_0 = b$ (condizione iniziale)

La sua soluzione è: $a_n = br^n$

D'ora in avanti useremo T(n) per indicare l'n-simo termine a_n della sequenza.

In informatica, l'interesse per le soluzioni delle relazioni di ricorrenza risiede nel fatto che esse nascono dall'analisi di algoritmi ricorsivi. Gli algoritmi ricorsivi hanno un passo base e un passo ricorsivo.

Esempio: calcolo del fattoriale

```
procedure fattoriale(n)
        if n=1 then return 1
        else return n * fattoriale(n−1)
```

La complessità asintotica di un algoritmo ricorsivo si esprime attraverso una relazione di ricorrenza.
complessità asintotica della procedure fattoriale(n) può essere descritta dalla relazione di ricorrenza.

$$\begin{cases} T(n) = T(n-1) + b \\ T(1) = a \end{cases}$$

dove a = costo per effettuare *return 1*, e b = costo per effettuare il prodotto n * fattoriale(n - 1)

Metodi per la risoluzione di relazioni di ricorrenza

Esistono alcuni metodi utili per risolvere le equazioni di ricorrenza. Noi analizzeremo:

- Metodo di sostituzione
- Metodo di iterazione

Illustreremo tali metodi, utilizzandoli per determinare:

- soluzioni esatte
- limiti superiori
- limiti inferiori

alle relazioni di ricorrenza.

Metodo di sostituzione

Idea: indovinare una soluzione, e verificare che essa funziona.

Il metodo consiste nei seguenti passi:

- si ipotizza una soluzione per l'equazione di ricorrenza data
- si usa l'induzione (matematica i forte) per provare che la soluzione dell'equazione di ricorrenza è effettivamente quella intuita.

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

1) ipotizziamo che la soluzione sia $T(n) \leq c\, n$, per un costante c opportuna (che deve essere ancora determinata), verifichiamolo con l'induzione:

- **Passo base:** $T(1) = b \leq c * 1$ per ogni $c \geq b$
- **Ipotesi induttiva:** supponiamo che $T(n-1) \leq c\,(n-1)$
- **Passo induttivo:** $T(n) = T(n-1) + a \leq c\,(n-1) + a = cn + (a-c)$ ma $cn + (a-c) \leq cn$ per $a - c \leq 0$, quindi $T(n) \leq cn$ per $c \geq a$ e $c \geq b$

Abbiamo determinato quindi un limite superiore per T(n): $T(n) \leq cn$ per $c \geq a$ e $c \geq b$

Possiamo però volere anche un limite inferiore per T(n):
ipotizziamo che $T(n) \geq h\, n$, dove h è una costante opportuna (che deve essere ancora determinata), verifichiamolo con l'induzione.

- **Passo base:** $T(1) = b \geq h * 1$ per ogni $h \leq b$
- **Ipotesi induttiva:** supponiamo che $T(n-1) \geq h\,(n-1)$
- **Passo induttivo:** $T(n) = T(n-1) + a \geq h\,(n-1) + a = hn - h$ ma $hn + (a-h) \geq hn$ per $a - h \geq 0$, quindi $T(n) \geq hn$ per $h \leq a$ e $h \leq b$

Abbiamo determinato un limite inferiore per T(n): $T(n) \geq hn$ per $h \leq a$ e $h \leq b$

Ricapitoliamo quindi:

$$T(n) = \begin{cases} T(1) = b \\ T(n-1) + a \end{cases}$$

- Abbiamo determinato quindi un limite superiore per T(n): **$T(n) \leq cn$ per $c \geq a$ e $c \geq b$**
- Abbiamo determinato un limite inferiore per T(n): **$T(n) \geq hn$ per $h \leq a$ e $h \leq b$**

Possiamo però essere più precisi:

2) ipotizziamo che la soluzione sia $T(n) = a\,(n-1) + b$, verifichiamolo con l'induzione:

- **Passo base:** $T(1) = b = a * 0 + b$
- **Ipotesi induttiva:** supponiamo che $T(n-1) = a\,(n-2) + b$
- **Passo induttivo:** $T(n) = T(n-1) + a = (a\,(n-2) + b) + a = a\,(n-1) + b$ quindi $T(n) = a\,(n-1) + b$

Esempio 2: $n = 2^k$ $T(n) = n + T(n/2)$ $T(1) = 1$

1) ipotizziamo che la soluzione sia $T(n) \le c\, n$ per una costante c opportuna, verifichiamolo con l'induzione:

- **Passo base:** $T(1) = 1 \le c * 1$ per ogni $c \ge 1$
- **Ipotesi induttiva:** supponiamo che $T(n/2) \le c\,(n/2)$
- **Passo induttivo:** $T(n) = n + T(n/2) \le n + c\,(n/2) = (c/2 + 1)\, n$ ma $(c/2 + 1)\, n \le cn$ per $c \ge 2$ quindi $T(n) \le cn$ per $c \ge 2$

2) ipotizziamo che la soluzione sia $T(n) \le c \log_2 n$ per una costante c opportuna, verifichiamolo con l'induzione:

- **Passo base:** $T(2) = 1 \le c * 1 = c \log_2 2$ per ogni $c \ge 1$
- **Ipotesi induttiva:** supponiamo che $T(n/2) \le c \log_2(n/2)$
- **Passo induttivo:** $T(n) = 1 + T(n/2) \le 1 + c \log_2(n/2) = 1 + c\,(\log_2 n - 1) = 1 - c + \log_2 n$
  ma $1 - c + c \log_2 n \le c \log_2 n$ per $c \ge 1$ quindi $T(n) \le c \log_2 n$ per $c \ge 1$

3) ipotizziamo che la soluzione sia $T(n) \le c\,(\log_2 n + 1)$ per una costante c opportuna, verifichiamolo con l'induzione:

- **Passo base:** $T(2) = 1 \le c * 1 = c\,(\log_2 1 + 1)$ per ogni $c \ge 1$
- **Ipotesi induttiva:** supponiamo che $T(n/2) \le c\,(\log_2(n/2) + 1)$
- **Passo induttivo:** $T(n) = 1 + T(n/2) \le 1 + c\,(\log_2(n/2) + 1) = 1 + c\,(\log_2 n - 1 + 1) = 1 + c \log_2 n$
  ma $1 - c + c \log_2 n \le c\,(\log_2 n + 1)$ per $c \ge 1$ quindi $T(n) \le c\,(\log_2 n + 1)$ per $c \ge 1$

Esempio 3: $T(n) = T(\lfloor n/2 \rfloor) + T(\lfloor 2n/3 \rfloor) + n^2$ $T(1) = 1$

1) ipotizziamo che la soluzione sia $T(n) \le c\, n^2$ per una costante c opportuna, verifichiamolo con l'induzione:

- **Passo base:** $T(1) = 1 \le c * 1$ per ogni $c \ge 1$
- **Ipotesi induttiva:** supponiamo che $T(n/2) \le c\,(n/2)^2$ e $T(2n/3) \le c\,(2n/3)^2$
- **Passo induttivo:**
$$\begin{aligned} &T(n) = T(\lfloor n/2 \rfloor) + T(\lfloor 2n/3 \rfloor) + n^2 \\ &\le c(\lfloor n/2 \rfloor)^2 + c(\lfloor 2n/3 \rfloor)^2 + n^2 \\ &< c(n/2)^2 + c(2n/3)^2 + n^2 \\ &= n^2(c/4 + 4c/9 + 1) \end{aligned}$$
  ma $n^2(c/4 + 4c/9 + 1) \le c\, n^2$ per $c \ge c/4 + 4c/9 + 1$ quindi $T(n) \le cn^2$ per $c \ge 11/36$

Metodo di iterazione

Idea: “srotolare” l’equazione di ricorrenza ed esprimerla come **somma di termini dipendenti da n** e **dalla condizione iniziale.**

Esempio 1: T(n) = T(n – 1) + a   T(1) = b

T(n) = T(n – 1) + a   **ma T(n – 1) = T(n – 2) + a**

= T(n – 2) + a + a   **ma T(n – 2) = T(n – 3) + a**

= T(n – 3) + a + a + a

…

$= T(n-k) \underbrace{+a+a+\ldots+a}_{k}$ **proseguendo in questo modo dopo k iterazioni avremo**

…

$= T(1) \underbrace{+a+a+\ldots+a}_{n-1}$ **le iterazioni si fermano quando si arriva alla condizione iniziale n – k = 1**

= b + (n – 1) a   **T(1) = b**

Esempio 2: T(n – 2) + 3   T(0) = 1

T(n) = 2 T(n – 2) + 3   **ma T(n – 2) = 2T(n – 4) + 3**

= 2 (2 T(n – 4) + 3) +3

= 2^2 T(n – 4) + 2 * 3 + 3   **ma T(n – 4) = 2t(n – 6) + 3**

= 2^2 (2T(n – 6) + 3) + 2 * 3 + 3

= 2^3 T(n – 6) + 2^2 * 3 + 2 *3 +3

…   **proseguendo in questo modo dopo k iterazioni avremo**

= 2^k T(n – 2 * k) + 2^{k-1} * 3 + 2^{k-2} *3 + … + 3

…

= $2^{n/2}$ T(0) + $2^{n/2-1}$ * 3 + $2^{n/2-2}$ * 3 + … + 3 **le iterazioni si fermano quando si arriva alla condizione iniziale n- 2k = 0 → k = n/2**

= $2^{n/2} + 3\ \Sigma_{i=0,\ldots,n/2-1} 2^i$

= $2^{n/2} + 3\ (2^{n/2-1+1} - 1) = 4 * 2^{n/2} - 3$ **quindi T(n) = 4 * $2^{n/2}$ – 3**

Esempio 3: sia n = 2^k T(n) = T(n /2) + 1   T(1) = 1

T(n) = T(n/2) + 1   **ma T(n/2) = T(n/2^2) + 1**

= (T(n/2^2) +1) + 1

= T(n/2^2) + 2   **ma T(n/2^2) = T(n/2^3) + 1**

= (T(n/2^3) +1) + 2

= T(n/2^3) + 3

= …   **proseguendo in questo modo dopo k iterazioni avremo**

= T(n/2^k) + k

= T(1) + k   **ma T(1) = 1 e k = $\log_2$ n**

= 1 + k = $\log_2$ n + 1   **Quindi T(n) = $\log_2$ n + 1**

Esempio 4: sia n = 2^k T(n) = 8 T(n /2) + n   T(1) = 2

$T(n) = 8T(n/2) + n$ **ma $T(n/2) = T(n/2^2) + 1$**
$= 8^2(8\ T(n/2^2) + n/2\ ) + n$
$= 8^2\ T(n/2^2) + 8 * n/2 + n$
$= 8^2T(n/2^2 + 4 * n + n$ **ma $T(n/2^2) = 8T(n/2^3) + n/2^2$**
$= 8^{2\ (}T(n/2^3) + n/2^2) + 4 * n + n$
$= 8^3\ (8T(n/2^3) + n/2^2) + 4 * n + n$
$= 8^3\ T(n/2^3) + 8^{2\ *}\ n/2^2 + 4 * n + n$
$= 8^3\ T(n/2^3) + 4^2 * n + 4 * n + n$
$=$ … **proseguendo in questo modo dopo k iterazioni avremo**
$= 8^k\ T(n/2^k) + 4^{k-1} * n + 4^{k-2} * n + \ldots + n$
$= 8^k\ T(n/2^k) + n * \Sigma_{i = 0, \ldots, k-1} 4^i$
$= 8^k\ T(n/2^k) + n\ (4^{k-1+1} - 1)/3$
$= 8^k\ T(n/2^k) + n\ (4^k - 1)/3$
$= (2^k)^3 * T(n/2^k) + n * ((2^k)^2 - 1)/3$ **ma $T(1) = 2$ e $n = 2^k$**
$= n^3 * T(1) + n * (n^2 - 1)/3$
$= n^3 * 2 + n\ (n^2 - 1)/3$
$= (7\ n^3 + n)/3$ **Quindi $T(n) = (7\ n^3 + n)/3$**

Esempio 5: sequenza di Fibonacci: $T(n) = \begin{cases} T(1) = 1 & n = 1 \\ T(2) = 1 & n = 2 \\ T(n-1) + T(n-2) & altrimenti \end{cases}$

Risolvere questa relazione di ricorrenza con il metodo iterativo è molto complesso.
Proviamo però a limitarla:

1. $T(n) = T(n-1) + T(n-2) \leq 2\ T(n-1)$
2. $T(n) = T(n-1) + T(n-2) \geq 2\ T(n-2)$

- Applichiamo il metodo di iterazione alla 1, cioè risolviamo: $T(n) \leq 2\ T(n-1)$
$T(n) \leq 2\ T(n-1)$
$\leq 2 * 2T(n-2)$
$\leq 2 * 2 * 2T(n-3) = 2^3T(n-3)$
…
$\leq 2^k\ T(n-k)$ **ci fermeremo quando $n - k = 1 \rightarrow k = n - 1$**
…
$\leq 2^{n-1}\ T(1) = 2^{n-1}$ **quindi $T(n) \leq 2^{n-1}$**

- Applichiamo il metodo di iterazione alla 2, cioè risolviamo: $T(n) \geq 2\ T(n-2)$
$T(n) \geq 2\ T(n-2)$
$\geq 2 * 2T(n-2-2)$
$\geq 2 * 2 * 2T(n-2-2-2) = 2^3T(n-3 * 2)$ **proseguendo in questo modo do k iterazioni avremo**
…
$\geq 2^k\ T(n-k)$ **ci fermeremo quando $n - k * 2 = 2 \rightarrow k = (n - 2)/2$**
…
$\geq 2^{n-1}\ T(1) = 2^{n-1}$ **quindi $T(n) \geq 2^{(n-2)/2}$**

SOMME FINITE

Proprietà delle somme **Linearità:** **1)** $\sum_{k=1}^{n}(ca_k+b_k)=c\sum_{k=1}^{n}a_k+\sum_{k=1}^{n}b_k$ **Serie telescopiche:** **1)** $\sum_{k=1}^{n}(a_k-a_{k-1})=a_n-a_0$ **2)** $\sum_{k=0}^{n}(a_k-a_{k+1})=a_0-a_n$	**Somme notevoli** **Se r ≠ 1:** **1)** $\sum_{k=0}^{n}r^k=\frac{r^{n+1}-1}{r-1}$ **2)** $\sum_{k=1}^{n}kr^k=r\frac{1-r^n}{1-r^2}-\frac{nr^{n+1}}{1-r}$ **3)** $\sum_{k=1}^{n}k=\frac{n(n+1)}{2}$ **4)** $\sum_{k=1}^{n}k^2=\frac{n(n+1)(2n+1)}{6}$ **5)** $\sum_{k=1}^{n}k^3=\frac{n^2(n+1)^2}{4}$
ESKEREEEEEEEEE!!!!	**per n ≥ 2:** **1)** $\sum_{k=1}^{n-1}\frac{1}{k(k+1)}=1-\frac{1}{n}$ **2)** $\sum_{k=1}^{n}\frac{1}{k}\leq\log_n+1$ **3)** $\sum_{k=1}^{n}\binom{n}{k}a^{(n-k)}b^k=(a+b)^n$ **4)** $\sum_{k=0}^{n}\binom{n}{k}=2^k$ **5)** $\sum_{k=0}^{n}(-1)^k\binom{n}{k}=0$ **6)** $\sum_{k=0}^{n}\binom{n}{m}=\binom{n+1}{m+1}$