PER ALTRI APPUNTI CONSULTARE IL SITO:

https://luigi-v.github.io/Appunti_Universita/

1. LOGICA PROPOSIZIONALE

Nel linguaggio comune si utilizzano spesso frasi imprecise o ambigue.

Esempio:

"Un americano muore di melanoma ogni ora"

Assurdo: significa che c'è un americano (sfortunato) che ogni ora muore di melanoma.

Corretta: Ogni ora, un americano muore di melanoma.

Il linguaggio matematico richiede ***certezze nelle affermazioni***, ossia determinare che sia ***vera*** o ***falsa***.

1.1. 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

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

Le seguenti frasi **NON** sono proposizioni:

- Il tuo cinismo mi addolora. → esprime un sentimento
- Toccare ferro porta fortuna → è una credenza
- Hai superato l'esame per la patente guida? → è una domanda
- Correre in bicicletta mi diverte molto. → esprime una sensazione
- Smettila d'essere maleducato! → è un ordine
- Come fa freddo oggi! → è un'esclamazione

1.2. PROPOSIZIONI COMPOSTE:

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

Esempio:

Proposizione A: Fuori piove

Proposizione B : Vedremo un film

Una nuova *proposizione composta*:

Se fuori piove allora vedremo un film.

2. CONNETTIVI LOGICI

2.1. 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*.

p	¬p
T	F
F	T

Il valore della negazione di p , cioè di ¬p , è l'opposto del valore di p.

Esempio1:

Se abbiamo una proposizione "*Salerno è una città della Campania*" allora due possibili negazioni sono:

- **Non è vero** che Salerno è una città della Campania
- Salerno **non è** una città della Campania

Se abbiamo la proposizione "*L'auto di Giovanni ha almeno tre anni di vita*" allora tre possibili negazioni sono:

- **Non è vero** che l'auto di Giovanni ha almeno tre anni di vita
- L'auto di Giovanni **non** ha almeno tre anni di vita
- L'auto di Giovanni ha **meno** di tre anni di vita

Esempio2:

- $2+5 \neq 3$
- 10 **non è** un numero primo
- **Non è vero** che l'autobus 31 passa ogni 10 minuti

2.2. 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 $p \wedge q$.
$p \wedge q$ è vera se entrambe p e q sono vere, altrimenti è falsa.

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Il valore della congiunzione $p \wedge q$ è vero se entrambe p e q sono vere, altrimenti è falso.

Esempi:

- Salerno è una città della Campania **e** 5+2=8.
- Oggi piove **e** 2+5 ≠ 3.
- 10 è un numero primo **e** 5+2=7.
- Oggi piove **e** l'autobus 31 passa ogni 10 minuti.

2.3. 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 $p \vee q$.
$p \vee q$ è falsa se entrambe p e q sono false, altrimenti è vera.

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Il valore della disgiunzione $p \vee q$ è vero se o p o q o entrambe sono vere.

Esempi:

- Salerno è una città della Campania **o** 5+2=8.
- Oggi piove **o** 2+5 ≠ 3.
- 10 è un numero primo **o** 5+2=7.
- Oggi piove **o** l'autobus 31 passa ogni 10 minuti.

2.4. DISGIUNZIONE ESCLUSIVA:

Siano p e q proposizioni. L'*or esclusivo di p e q* è denotato con $p \oplus q$.
$p \oplus q$ è vero quando esattamente uno tra p e q sono veri, altrimenti è falso.

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

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

Esempio:

Nel menù a prezzo fisso di un ristorante: Frutta o formaggio

2.5. IMPLICAZIONE:

Siano p e q proposizioni. La proposizione " p implica q " è chiamata *implicazione*.
Essa è denotata con $p \rightarrow q$ (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*.

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Il valore dell'implicazione **$p \rightarrow q$** è falsa solamente se la verità di p implica la falsità di q.

condizione sufficiente → condizione necessaria

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**

Esempio:

Consideriamo la proposizione "*Se ho la febbre allora sono ammalato*", tutte le situazioni che si possono presentare sono:

- Se ho la febbre allora sono ammalato → si può verificare
- Se ho la febbre allora non sono ammalato → non si può verificare
- Se non ho la febbre allora sono ammalato → si può verificare
- Se non ho la febbre allora non sono ammalato → si può verificare

Consideriamo la proposizione "*Se è una carta di cuori allora è una regina*", consideriamo i seguenti casi:

- Se è una carta di cuori ed è una regina
- Se è una carta di cuori ed è un re → solo qui abbiamo mentito
- Se è una carta di picche ed è una regina
- Se è una carta di picche ed è un re

NOTA: L'implicazione $p \rightarrow q$ non presuppone vi sia una qualche relazione tra p e q.

Esempio1:

Se Giulio Cesare è morto allora 2 * 3 = 6

- Giulio Cesare è morto → T
- 2 * 3 = 6 → T

Se T allora T → T

Esempio2:

Se la Salernitana vince lo scudetto nel 2013 allora 2 è un numero primo

- p = la Salernitana vince lo scudetto nel 2013
- q = 2 è un numero primo

Se F allora T → T

2.5.1. PROPOSIZIONI CONDIZIONALI DERIVANTI DALL'IMPLICAZIONE

L'INVERSO di $p \rightarrow q$ è $q \rightarrow p$

p	q	$p \rightarrow q$	$q \rightarrow p$
T	T	T	T
T	F	F	T
F	T	T	F
F	F	T	T

Esempio:

Se nevica allora le auto procedono lentamente

- p = nevica
- q = le auto procedono lentamente
- $p \rightarrow q$

L'inverso : Se le auto procedono lentamente allora nevica

- $q \rightarrow p$

L'OPPOSTO di $p \rightarrow q$ è $\neg p \rightarrow \neg q$

p	q	$p \rightarrow q$	$\neg p$	$\neg q$	$\neg p \rightarrow \neg q$
T	T	T	F	F	T
T	F	F	F	T	T
F	T	T	T	F	F
F	F	T	T	T	T

Esempio:

Se nevica allora le auto procedono lentamente

- p = nevica
- q = le auto procedono lentamente
- $p \rightarrow q$

L'opposto : Se non nevica allora le auto procedono velocemente

- $\neg p \rightarrow \neg q$

Il CONTRONOMINALE di $p \rightarrow q$ è $\neg q \rightarrow \neg p$

p	q	$p \rightarrow q$	$\neg q$	$\neg p$	$\neg q \rightarrow \neg p$
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

$\neg q \rightarrow \neg p$ ha gli stessi valori di verità di $p \rightarrow q$

Esempio:

Se nevica allora le auto procedono lentamente

- p = nevica
- q = le auto procedono lentamente
- $p \rightarrow q$

Il ***contronominale***: Se le auto procedono velocemente allora non nevica

- $\neg q \rightarrow \neg p$

2.6. BICONDIZIONE (O EQUIVALENZA):

Siano p e q proposizioni.
La proposizione " *p se e solo se q* " è chiamata bicondizione (o equivalenza).
Essa è denotata con $p \leftrightarrow q$ (talvolta anche con $p <=> q$).
$p \leftrightarrow q$ è vera quando p e q hanno lo stesso valore di verità, altrimenti è falsa.

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

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

- 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

$p \leftrightarrow q$ ha gli stessi valori di verità di $(p \rightarrow q) \wedge (q \rightarrow p)$

p	q	$p \rightarrow q$	$q \rightarrow p$	$p \leftrightarrow q$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

ESEMPIO RIEPILOGATIVO

p = 2 è un numero primo = T

q = 6 è un numero primo = F

- $\neg p$ = F
- $\neg q$ = T
- $p \wedge q$ = F
- $p \wedge \neg q$ = T
- $p \vee q$ = T
- $p \oplus q$ = T
- $p \to q$ = F
- $q \to p$ = T
- $p \leftrightarrow q$ = F

Costruire una tabella di verità per proposizioni composte per l'espressione **$(p \to q) \wedge (\neg p \leftrightarrow q)$**

p	q	$\neg p$	$p \to q$	$\neg p \leftrightarrow q$	$(p \to q) \wedge (\neg p \leftrightarrow q)$
T	T				
T	F				
F	T				
F	F				

proposizioni elementari

p	q	$\neg p$	$p \to q$	$\neg p \leftrightarrow q$	$(p \to q) \wedge (\neg p \leftrightarrow q)$
T	T				
T	F				
F	T				
F	F				

proposizioni composte ausiliarie

p	q	$\neg p$	$p \to q$	$\neg p \leftrightarrow q$	$(p \to q) \wedge (\neg p \leftrightarrow q)$
T	T	F	T	F	F
T	F	F	F	T	F
F	T	T	T	T	T
F	F	T	T	F	F

2. APPLICAZIONE DELLA LOGICA PROPOSIZIONALE

Traduzione di frasi di un linguaggio comune in proposizioni logiche

Supponiamo di avere la frase seguente: "*Se hai più di 12 anni o sei accompagnato dai tuoi genitori allora puoi salire su quella giostra*."

Analisi:

Se (hai più di 12 anni o sei accompagnato dai tuoi genitori) allora (puoi salire su quella giostra)

Proposizioni elementari:

a = hai più di 12 anni

b = sei accompagnato dai tuoi genitori

c = puoi salire su quella giostra

Traduzione:

$(a \lor b) \rightarrow c$

REGOLA GENERALE:

Individua nella frase le parole chiave che corrispondono ai connettivi logici ed usa essi per identificare le proposizioni elementari.

Esempio:

$\underbrace{\text{Puoi avere caffè gratis}}_{a}$ se $\underbrace{\text{sei maggiorenne}}_{b}$ ed $\underbrace{\text{è martedì}}_{c}$

- Passo 1: individua i connettivi logici
- Passo 2: identifica le proposizioni elementari
- Passo 3: riscrivi la frase come una proposizione logica

$(b \land c) \rightarrow a$

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

Traduci ciascuna delle seguenti frasi:

- Tu *non* guidi a più di 130 km/h → $(\neg p)$
- Tu guidi a più di 130 km/h, *ma non* prendi la multa → $(p \land \neg q)$
- *Se non* guidi a più di 130 km/h *allora non* prendi la multa → $(\neg p \rightarrow \neg q)$
- Guidare a più di 130 km/h *è sufficiente per* prendere una multa → $(p \rightarrow q)$
- Prendi la multa, *ma non* guidi a più di 130 km/h → $(q \land \neg p)$

3. 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.

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

3.1. TAUTOLOGIA:

Una tautologia è una proposizione composta che è sempre vera per tutti i possibili valori delle proposizioni elementari che la compongono.

p	¬p	p ∨ ¬p
T	F	T
F	T	T

Esempio:

$p \lor \neg p$ è una tautologia

3.2. CONTRADDIZIONE:

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

p	¬p	p ∧ ¬p
T	F	F
F	T	F

Esempio:

$p \land \neg p$ è una contraddizione

3.3. CONTINGENZA:

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

3.4. EQUIVALENZA LOGICA:

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.

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

Esempio:

$p \rightarrow q$ è equivalente a $\neg q \rightarrow \neg p$ (contronominale)

Le equivalenze logiche sono proposizioni composte logicamente equivalenti ed 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.

3.5. IMPORTANTI EQUIVALENZE LOGICHE

LEGGI DI DE MORGAN:

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

Esempio:
La negazione della frase "*L'estate in Messico è calda ed assolata*", usando le leggi di De Morgan "*L'estate in Messico non è calda o non è assolata*".

p	q	¬q	¬p	¬(p ∨ q)	¬p ∧¬q
T	T	F	F	F	F
T	F	T	F	F	F
F	T	F	T	F	F
F	F	T	T	T	T

IDENTITÀ:

- $p \wedge T \equiv p$
- $p \vee F \equiv p$

DOMINAZIONE:

- $p \vee T \equiv T$
- $p \wedge F \equiv F$

IDEMPOTENZA:

- $p \vee p \equiv p$
- $p \wedge p \equiv p$

DOPPIA NEGAZIONE:

- $\neg(\neg p) \equiv p$

COMMUTATIVA:

- $p \wedge q \equiv q \wedge p$
- $p \vee q \equiv q \vee p$

ASSOCIATIVA:

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

DISTRIBUTIVA:

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

ALTRE UTILI EQUIVALENZA:

- $p \vee \neg p \equiv T$
- $p \wedge \neg p \equiv F$
- $p \oplus q \equiv (p \wedge \neg q) \vee (\neg p \wedge q)$
- $p \rightarrow q \equiv (\neg p \vee q)$
- $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$

Le equivalenze possono essere usate per trasformare proposizioni o parti di esse per poter ottenere un qualche risultato.

Esempio:

Mostrare che **$(p \wedge q) \rightarrow p$ è una tautologia**

Dim.1: dobbiamo mostrare che $((p \wedge q) \rightarrow p) \equiv T$

$$
\begin{aligned}
(p \wedge q) \rightarrow p &\equiv \neg(p \wedge q) \vee p \\
&\equiv (\neg p \vee \neg q) \vee p && \text{DeMorgan} \\
&\equiv (\neg q \vee \neg p) \vee p && \text{commutativa} \\
&\equiv \neg q \vee (\neg p \vee p) && \text{associativa} \\
&\equiv \neg q \vee T \\
&\equiv T && \text{dominazione}
\end{aligned}
$$

Dim.2: usiamo la tavola di verità

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

3.6. REGOLE DI PRECEDENZA DEGLI OPERATORI

L'uso di parentesi specifica l'ordine in cui gli operatori logici vanno applicati.

Per ridurre il numero di parentesi si stabilisce una convenzione sulla ***precedenza degli operatori***.

Esempio:

$(p \lor q) \land (\neg r)$ può essere scritta anche $(p \lor q) \land \neg r$

$(p \land q) \lor (\neg r)$ può essere scritta senza ambiguità $p \land q \lor \neg r$

operatore	precedenza
$\neg$	1
$\land$	2
$\lor$	3
$\rightarrow$	4
$\leftrightarrow$	5

4. PREDICATI E QUANTIFICATORI

4.1. LIMITAZIONI DELLA LOGICA PROPOSIZIONALE

Abbiamo visto nella ***logica proposizionale*** che il mondo è descritto attraverso proposizioni elementari e le 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.

Giovanni è uno studente dell'Università di Salerno

oggetto proprietà

Le asserzioni devono essere ripetute per oggetti diversi

Nella logica proposizionale ciascuna delle proposizioni deve essere ripetuta esaustivamente.

Esempio:

"Se Giovanni è laureato in Informatica allora ha sostenuto l'esame di MMI"

Traduzione: Giovanni è laureato in Informatica → ha sostenuto l'esame di MMI

Assumendo di avere altri laureati:

Anna è laureata in Informatica → ha sostenuto l'esame di MMI

Nicola è laureato in Informatica → ha sostenuto l'esame di MMI

Da questo esempio ricaviamo che il ***problema*** è quello di ***snellire la ripetizione esaustiva***.

La ***soluzione*** a questo problema è di ***costruite le proposizioni con le variabili***.

x è laureato in Informatica → ***x*** ha sostenuto l'esame di MMI

Esempio:

"Tutte le auto nuove devono essere immatricolate"

"Qualche laureato in Informatica si laurea con lode"

Qui il ***problema*** è *esprimere le proprietà di gruppo*.

La soluzione è *utilizzare i* ***quantificatori*****.** Ne esistono di due tipi:

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

4.2. LOGICA PREDICATIVA

Rimedia alle limitazioni della logica proposizionale:

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

Gli elementi fondamentali della logica predicativa:

- **costante**: modella uno specifico oggetto.
  Esempi:
  Giovanni, Salerno, 7.
- **variabile**: rappresenta un oggetto di un tipo specificato (il tipo è definito stabilendo un universo del discorso).
  Esempi:
  x, y (universo del discorso può essere persone, studenti, numeri).
- **predicato**: rappresenta la proprietà o le relazioni tra gli oggetti.
  Esempio:
  x è più grande di 3
  P = è più grande di 3 → predicato
  x è più grande di 3 → è denotata con ***P(x)***
  Può essere relativo ad uno, due o più oggetti (studente(x), sposati(Giovanni, Maria)).

4.3. PREDICATI

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 oggetto preso dall'***universo del discorso***.

Esempio1:

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

Esempio2:

Sia ***P(x)*** un predicato che rappresenta l'asserzione: ***x è un numero primo***

Quali sono i valori di verità di:

- P(2) T
- P(3) T
- P(4) F
- P(5) T
- P(6) F
- P(7) T

Tutte le asserzioni P(2), P(3), P(4), P(5), P(6), P(7) sono ***proposizioni***.

È P(x) una proposizione? No, perché P(x) può essere applicata a più oggetti ed assumere valori diversi

I predicati possono avere **più argomenti**. Il predicato rappresenta la **relazione tra gli argomenti (oggetti).**

Esempio1:

Piu_vecchio(Giovanni, Pietro), denota l'asserzione ***Giovanni è più vecchio di Pietro*** (È una proposizione perché è vera o falsa).

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).

Esempio2:

Q(x, y), denota x+5 > y

- Q(x,y) è una proposizione? ***NO***
- Q(3,7) è una proposizione? ***SI***

  Quali sono i valori di verità di:

  - Q(3,7) → ***T***
  - Q(1,6) → ***F***
- Q(3,y) è una proposizione? ***NO***. Non possiamo dire se è vera o falsa

4.4. ASSERZIONI COMPOSTE NELLA LOGICA PREDICATIVA

Le asserzioni composte sono ottenute attraverso connettivi logici.

Esempi:

Studente(Giovanni) ∧ 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) → Matricola(x)

- ***Traduzione***: Se x segue il corso di MMI allora x è una matricola
- ***Proposizione***: NO

LOGICA PROPOSIZIONALE	**LOGICA PREDICATIVA**
▪ Utilizza asserzioni che descrivono proprietà di **oggetti ben definiti** (proposizioni)	▪ Consente di utilizzare asserzioni valide per più oggetti (predicati) ▪ Permette di quantificare le asserzioni, consente di fare asserzioni riguardanti gruppi di oggetti (quantificatori)

4.5. ASSERZIONI QUANTIFICATE

La logica predicativa consente di fare asserzioni riguardanti gruppi di oggetti. Vengono utilizzate asserzioni quantificate:

- **Universale:**

<u>Esempio</u>:

Tutti gli studenti di MMI sono iscritti ad Informatica → L'asserzione è vera per ***tutti*** gli studenti di MMI

- **Esistenziale:**

<u>Esempio</u>:

Alcuni studenti di Informatica si laureano con lode → L'asserzione è vera per ***alcuni*** studenti di Informatica

4.5.1. 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 ∀x P(x) denota la quantificazione universale di P(x), ed è espressa dicendo per ogni x P(x) è vera

<u>Esempio1</u>:

Supponiamo che P(x) denoti x > x – 1. Quale è il valore di verità di ∀x P(x)?

Assumiamo che il dominio sia l'insieme di tutti i *numeri reali R*.

Risposta: poiché il numero reale x è più grande di sé stesso diminuito di 1, abbiamo ∀x P(x) è vera.

<u>Esempio2</u>:

MMI(x) → Matricola(x)

- ***Traduzione***: Se x segue il corso di MMI allora x è una matricola
- ***Proposizione***: NO

∀x (MMI(x) → Matricola(x))

- ***Dominio***: 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.

<u>Esempio</u>:

Supponiamo che P(x) denoti x ≥ 0:

- P(x) è una proposizione? ***NO***. Può assumere molti valori diversi
- ∀x P(x) è una proposizione? ***SI***. Il valore di x P(x) è ben definito: è ***vero*** se P(x) è vero per ogni x nel dominio, ed è ***falso*** se esiste un valore di x per cui P(x) risulta falso.

Nell'utilizzo del quantificatore è ***importante definire esattamente il dominio*** (l'universo del discorso).

<u>Esempio</u>:

Supponiamo che P(x) denoti x ≥ 0. Quale è il valore di ∀x P(x)?

Assumiamo che il dominio sia l'insieme dei numeri interi (ricordate Z = { ..., −1, 0, 1, 2, ... }):

∀x∈Z P(x) → ***Falso***. Poiché per x=−1 abbiamo x<0

Assumiamo che il dominio sia l'insieme dei numeri naturali (ricordate N = { 0, 1, 2, ... }):

∀x∈N P(x) → ***Vero***.

Un elemento x del dominio per il quale P(x) è falsa è detto ***controesempio*** di ∀x P(x). Per provare che una asserzione che utilizza un quantificatore universale è falsa basta individuare un ***controesempio***.

<u>Esempio</u>:

Con P(x) che denota x ≥ 0 e con dominio l'insieme dei numeri interi Z, si ha che ∀x P(x) è Falso. La prova è data dall'esistenza di un intero come x=−1 per il quale P(x) è falso. Cioè x=−1 è un ***controesempio*** per ∀x P(x).

4.5.2. 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 ∃x P(x) denota la quantificazione esistenziale di P(x), ed è espressa dicendo esiste un x tale che P(x) è vera.

<u>Esempio1</u>:

Supponiamo che P(x) denoti x > 5. ***Dominio***: insieme dei numeri reali R.

Quale è il valore di verità di ∃x P(x) ?

Risposta: poiché è possibile trovare un numero reale maggiore di 5, per esempio 10 > 5, abbiamo ∃x P(x) è ***vera***.

Esempio2:

Supponiamo che Q(x) denoti x = x+2. ***Dominio***: insieme dei numeri reali R.

Quale è il valore di verità di ∃x Q(x) ?

Risposta: poiché nessun numero reale è uguale a sé stesso aumentato di 2, abbiamo ∃x P(x) è ***falsa***.

Esempio3:

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

Asserzione	Quando è vera?	Quando è falsa?
∀x P(x)	P(x) è vera per tutti gli x	C'è un x per il quale P(x) è falsa
∃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

- ∀x P(x) è vera se $P(x_1) \wedge P(x_2) \wedge \ldots \wedge P(x_N)$ è vera
- ∃x P(x) è vera se $P(x_1) \vee P(x_2) \vee \ldots \vee P(x_N)$ è vera

Esempio1:

Supponiamo che P(x) denoti $x^2 > 10$. ***Dominio***: {1,2,3,4}.

Quale è il valore di verità di ∃x P(x) ?

Risposta: il valore di ∃x P(x) è lo stesso della disgiunzione P(1) ∨ P(2) ∨ P(3) ∨ P(4), poiché, P(4)= 16 > 10, abbiamo ∃x P(x) è T.

Esempio2:

Supponiamo che P(x) denoti x2 > 10. ***Dominio***: {1,2,3,4}.

Quale è il valore di verità di ∀x P(x) ?

Risposta: il valore di ∀x P(x) è lo stesso della disgiunzione P(1) ∧ P(2) ∧ P(3) ∧ P(4), poiché , P(1)= 1 < 10, abbiamo ∀x P(x) è F.

4.6. TRADUZIONI DI FRASI UTILIZZANDO I QUANTIFICATORI

La formulazione di un asserzione nella logica predicativa dipende dal dominio.

Esempio1:

"Tutti gli studenti di Informatica sono simpatici."

- ***Dominio***: studenti di Informatica — ***Traduzione***: ∀x Simpatici(x)
- ***Dominio***: studenti — ***Traduzione***: ∀x (Inf(x) → Simpatici(x))
- ***Dominio***: persone — ***Traduzione***: ∀x ((Stud(x) ∧ Inf(x)) → Simpatici(x))

Esempio2:

"Qualche studente di Ingegneria è simpatico."

- ***Dominio***: studenti di Ingegneria — ***Traduzione***: ∃x Simpatico(x)
- ***Dominio***: studenti — ***Traduzione***: ∃x (Ing(x) ∧ Simpatico(x))

Tipicamente, date due qualunque predicati S(x) e P(x): ***Le "asserzioni universali" sono legate alle "implicazioni"***

Tutti S(x) sono P(x): ∀x (S(x) → P(x))

Nessun S(x) è P(x): ∀x (S(x) → ¬P(x))

Esempio:

"Tutti gli italiani mangiano la pasta"

- ***Dominio***: italiani — ***Traduzione***: ∀x Mangia_pasta(x)
- ***Dominio***: persone — ***Traduzione***: ∀x (Italiano(x) → Mangia_pasta(x))

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

Qualche S(x) è P(x): $\exists x\, (S(x) \wedge P(x))$

Qualche S(x) non è P(x): $\exists x\, (S(x) \wedge \neg P(x))$

<u>*Esempio*</u>:

"Qualche italiano è vegano"

Dominio: italiani — ***Traduzione***: $\exists x$ Vegano(x)

Dominio: persone — ***Traduzione***: $\exists x$ (Italiano(x) $\wedge$ Vegano(x))

4.7. ASSERZIONI MATEMATICHE 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.

<u>*Esempio1*</u>:

"$x^2+2x+1=0$ 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: $\exists x\, (x^2+2x+1=0)$.

<u>*Esempio2*</u>:

"$\sqrt{2}$ è un numero irrazionale"

La natura esistenziale di questa asserzione è più esplicita se si esprime come: ***Non esistono due interi p e q tale che $\sqrt{2}$ = p/q***.

Simbolicamente può essere espressa come: $\neg(\exists p\in Z\ \ \exists q\in Z\ (\sqrt{2}= p/q))$.

<u>*Esempio3*</u>:

"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: $\forall x\, (x^2 \geq 0)$.

4.8. QUANTIFICATORI INNESTATI

Più di un quantificatore può essere necessario per rappresentare una qualche asserzione.

<u>*Esempio1*</u>:

"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: $\forall x\, \exists y\, P(x,y)$.

<u>*Esempio2*</u>:

"C'è una persona che ama tutti gli altri"

Assumiamo che:

- il dominio sia l'insieme delle persone
- A(x,y) sia "x ama y"

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

Invertendo i quantificatori le asserzioni potrebbero avere un significato completamente differente. ***L'ordine dei quantificatori innestati è importante.***

<u>*Esempio1*</u>:

"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).***

<u>*Esempio2*</u>:

"$\forall x\, \exists y$ Ama(x,y) è diverso da $\exists y\, \forall x$ Ama(x,y)"

Infatti, se come prima A(x,y) è "x ama y", allora:

$\forall x\, \exists y$ Ama(x,y) significa: Ognuno ama qualcun altro

$\exists y\, \forall x$ Ama(x,y) significa: C'è una persona che è amato da tutti gli altri

Esempio3:

"Per tutte le x e le y, se x è un genitore di y allora y è figlio di x"

Consideriamo: Genitore(x,y) è "x è genitore di y" e Figlio(y,x) è "y è figlio di x"

L'asserzione può essere rappresentata in due modi equivalenti:

- $\forall x\ \forall y$ Genitore(x,y) $\rightarrow$ Figlio(y,x)
- $\forall y\ \forall x$ Genitore(x,y) $\rightarrow$ Figlio(y,x)

4.9. NEGAZIONE DI QUANTIFICATORI

Esempio1:

"Niente è perfetto"

Traduzione: $\neg$ ($\exists x$ Perfect(x))

Un altro modo per esprimere l'asserzione precedente è: "*Ogni cosa è imperfetta*"

Traduzione: $\forall x\ \neg$Perfect(x)

Un altro modo per esprimere l'asserzione precedente è: "*Ogni cosa è imperfetta*"

Conclusione: $\neg$ ($\exists x$ Perfect(x)) è equivalente a $\forall x\ \neg$Perfect(x)

Esempio2:

"Non è vero che tutti gli italiani mangiano la pasta"

Traduzione: $\neg\ \forall x$ (Italiano(x) $\rightarrow$ Mangia_pasta(x))

Un altro modo per esprimere l'asserzione precedente è: "*C'è qualche italiano che non mangia la pasta*"

Traduzione: $\exists x$ (Italiano(x) $\land\ \neg$Mangia_pasta(x))

Logicamente equivalente a: $\exists x\ \neg$(Italiano(x) $\rightarrow$ Mangia_pasta(x))

Conclusione: $\neg$ ($\forall x$ P(x)) è *equivalente* a $\exists x\ \neg$P (x)

4.10. 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)

Cominciamo col provare che $\neg\ \forall x$ P(x) $\rightarrow\ \exists x\ \neg$P (x)

Se $\neg$ ($\forall x$ P(x)) è vera => ($\forall x$ P(x)) è falsa

=> $\exists x$ per il quale P(x) è falsa, cioè

$\exists x$ per il quale $\neg$P (x) è vera, cioè $\exists x\ \neg$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) $\leftarrow\ \exists x\ \neg$P (x)

Ci rimane da provare che $\exists x\ \neg$P (x) $\rightarrow\ \neg\ \forall x$ P(x)

Se $\exists x\ \neg$P (x) è vera => $\exists x$ per cui P(x) è falsa

=> non è vero che $\forall x$ P(x) è vera, cioè

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

4.11. RAPPORTI TRA QUANTIFICATORI E CONNETTIVI LOGICI

Può accadere che: $\exists x$ [P(x) $\land$ D(x)] NON è lo stesso di $\exists x$ P(x) $\land$ $\exists x$ D(x).

Esempio:

Consideriamo come dominio N   P(x) = x è pari   D(x) = x è dispari

$\exists x$ [P(x) $\land$ D(x)] è Falsa

$\exists x$ P(x) $\land$ $\exists x$ D(x) è Vera

Portare il quantificatore esistenziale davanti a ciascun predicato può portare ad asserzioni completamente diverse
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

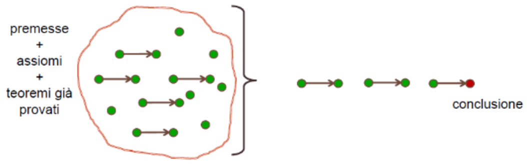
$\forall x$[(F(x) $\lor$ P(x)) $\rightarrow\ \exists y$ E(x,y)]   è equivalente a $\forall x\ \exists y$ [(F(x) $\lor$ P(x)) $\rightarrow$ E(x,y)]

2. DIMOSTRAZIONI

Una ***dimostrazione*** è un ragionamento corretto 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.*



Un problema importante di una dimostrazione si ha quando comprendere se un ragionamento è corretto, e quale metodo usare.

Consideriamo il caso p → q = T, quindi:

- Se p è F allora indipendentemente dal valore di q abbiamo p → q è T;
- Se p è T allora dobbiamo provare anche q è T per avere p → q è T.

2.1 TEOREMI

Un ***teorema*** è una asserzione che si può dimostrare essere vera.

Tipicamente un teorema lo si può vedere in questo modo:

$$\underbrace{(p_1 \land p_2 \land p_3 \land \ldots \land p_n)}_{\text{Premesse (ipotesi)}} \to \underbrace{q}_{\text{conclusione}}$$

<u>Esempio</u>: Teorema di Fermat

Premesse (ipotesi)

Se p è un primo ed a è un numero non divisivile per p

allora $a^{p-1} \equiv 1 \bmod p$ conclusione

Ci sono diversi *<u>metodi di base</u>* per provare teoremi.

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. Inoltre, alcune dimostrazioni possono richiedere l'utilizzo di più di un tipo di dimostrazione.

2.2 DIMOSTRAZIONE DIRETTA

p → 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***.

<u>Esempio1</u>:

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 qualunque intero;
- $n^2 = (2k + 1)^2$
  $= 4k^2 + 4k + 1$
  $= 2(2k^2 + 2k) + 1$
- Perciò, n^2 è dispari.

<u>Esempio2</u>:

Siano n ed m interi. Provare che "*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 m = 2h + 1 dove k ed h sono due qualunque interi;
- n+m = (2k + 1) + (2h + 1)
  = 2k + 2h + 2
- Perciò, n+m è pari.

2.3 DIMOSTRAZIONE PER CONTRAPPOSIZIONE

p → q viene dimostrata mostrando che "*se (¬q è T) allora (p è F)*" / "*se (¬q è T) allora (¬p è T)*".
NOTA: Ciò che si dimostra è che " se ¬q è T allora ¬p è T ". **Si ricordi che: ¬q → ¬p ≡ p → q *contronominale***

<u>Esempio</u>:

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
- 3n + 2 = 3(2k) + 2
  = 6k + 2
  = 2(3k + 1)
- Così *3n +2 è pari* . Quindi *3n +2 è dispari ≡ F*

2.4 DIMOSTRAZIONE PER CONTRADDIZIONE (ASSURDO)

$p \rightarrow q$ viene dimostrata mostrando che "*se [(p è T) e ($\neg q$ è T)] allora F*"

cioè: si parte dal fatto che

- $\neg q$ è T
- p è T

Si fanno una serie di deduzioni, usando assiomi, definizioni e teoremi precedentemente provati per arrivare ad una asserzione ***F***.

L'approccio è corretto perché: $(p \land \neg q) \rightarrow \mathbf{F} \equiv \neg (p \land \neg q) \lor \mathbf{F}$

$$\equiv \neg (p \land \neg q)$$
$$\equiv \neg p \lor q$$
$$\equiv p \rightarrow q$$

Esempio1:

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

Esempio2:

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 sono interi
- $5x + 25y = 1723$
  $5(x + 5y) = 1723$
  $x + 5y = 1723/5$
  ma 1723 non è divisibile per 5 => $x + 5y$ non è un intero
- Ma questo è F (è assurdo) poiché sappiamo che x e y sono interi

2.5 DIMOSTRAZIONE DI EQUIVALENZA

$p \leftrightarrow q$ è dimostrata con $(p \rightarrow q) \land (q \rightarrow p)$

Esempio1:

"*n è dispari se e solo se n^2 è dispari*"

Dim. di ***p → 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
- $n^2 = (2k + 1)^2$
  $= 4k^2 + 4k + 1$
  $= 2(2k^2 + 2k) + 1$
- Perciò, n^2 è dispari.

Dim. di ***q → 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
- $n^2 = (2k)^2 = 4k^2$
- 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 $(p_1 \rightarrow p2)$ $(p_2 \rightarrow p_3)$ …… $(p_n \rightarrow p_1)$

Esempio2:

Mostrare 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 $p_1 \rightarrow p_2$, $p_2 \rightarrow p_3$, $p_3 \rightarrow p_1$,

$p_1 \rightarrow p_2$

- Se n è pari, allora $n = 2k$, dove k è un intero
- $n - 1 = 2k - 1 = 2(k - 1) + 1$ che è un intero dispari

$p_2 \rightarrow p_3$

- Se n−1 è dispari, allora $n - 1 = 2k + 1$, dove k è un intero
- $n^2 = (2k +2)^2 =4k^2 + 8k + 4 = 2(2k^2 + 4k +2)$ che è un intero pari

$p_3 \rightarrow p_1$

- Per contrapposizione supponiamo che n sia dispari, cioè $n = 2k + 1$, dove k è un intero
- $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ che è un intero dispari

2.6 DIMOSTRAZIONE BANALE

Vogliamo provare che p → q. Se la conclusione *q è sempre vera*, allora *p → q* è banalmente *vera*.

Esempio1:

Sia P(n): "se a ≥ b allora $a^n \geq b^n$". Mostrare che P(n) → P(0).

Dim:

- $a^0 >= b^0$ è 1=1 che è banalmente vera indipendentemente da n.

Esempio2:

Proviamo che *'Se x>0 allora $(x+1)^2 - 2x \geq x^2$'*

Dim:

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

Siamo giunti alla conclusione senza usare l'ipotesi

2.7 DIMOSTRAZIONE VUOTA

Vogliamo provare che p → q. Se l'ipotesi p è *sempre falsa* allora p → q è banalmente *vera*.
F → q è sempre T, sia che q sia True o False.

Esempio:

Sia P(n): "*se n ≥ 1 allora $n^2 \geq 1$*". Mostrare che (se n=0) → P(0)

Dim:

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

2.8 DIMOSTRAZIONE PER ANALISI DEI CASI

Vogliamo provare che $(p_1 \lor p_2 \lor \ldots \lor p_n) \rightarrow q$
È equivalente a $(p_1 \rightarrow q) \land (p_2 \rightarrow q) \land \ldots \land (p_n \rightarrow q)$

Questo perché:

$(p_1 \lor p_2 \lor \ldots \lor p_n) \rightarrow q \equiv$

$\neg(p_1 \lor p_2 \lor \ldots \lor p_n) \lor q \equiv$ (applichiamo De Morgan)

$(\neg p_1 \land \neg p_2 \land \ldots \land \neg p_n) \lor q \equiv$ (applichiamo distributiva)

$(\neg p_1 \lor q) \land (\neg p_2 \lor q) \land \ldots \land (\neg p_n \lor q) \equiv$

$(p_1 \rightarrow q) \land (p_2 \rightarrow q) \land \ldots \land (p_n \rightarrow q)$

Quindi si prova la verità di tutti i casi, uno per uno…

Esempio1:

Mostrare che $|x||y|=|xy|$ per x ed y reali

Dim:

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

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

Tutti i casi sono provati…

Esempio2:

Sia n ∈ Z. Provare che 9n2+3n−2 è pari.

Dim:

Per prima cosa consideriamo che $9n^2+3n-2=(3n+2)(3n-1)$

Poiché n è un intero, allora (3n+2)(3n-1) è il prodotto di due interi. Consideriamo 2 casi:

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

Tutti i casi sono provati…

2.8.1 DIMOSTRAZINE ESAUSTIVA

Alcuni teoremi possono essere provati esaminando un numero relativamente piccolo di esempi.

- 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 ≤ 4

Dim:

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

- n=1 $(n+1)^3 = (1+1)^3 = 8$ $3^n = 3^1 = 3$
- n=2 $(n+1)^3 = (2+1)^3 = 27$ $3^n = 3^2 = 9$
- n=3 ………
- n=4 ………

2.9 DIMOSTRAZIONE CON QUANTIFICATORI

Asserzioni espresse con un quantificatore esistenziale – dimostrazioni di esistenza
- Vogliamo provare che ∃x P(x)

Costruttiva:

- 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 ∃x P(x) ≡ ∀x ¬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 $B_1, B_2, \ldots, B_n$
- 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
  $k_i \leq 1$
  Allora $k_1 + k_2 + \ldots\ldots + k_n \leq 1+1+\ldots\ldots+1 = n$
- Ma questo contraddice l'ipotesi $k_1 + k_2 + \ldots\ldots + k_n = n + 1$.

Asserzioni espresse con una *negazione* di un quantificatore *esistenziale*.
- Vogliamo provare che ¬∃x P(x) ≡ ∀x ¬ 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 √2 è un irrazionale

- Si ricordi che l'asserzione: Il numero √2 è un irrazionale
  è equivalente a: Non esistono due interi p e q tale che √2 = p/q
  simbolicamente può essere espressa come: $\neg(\exists p \in Z \ \exists q \in Z \ (\sqrt{2} = p/q))$
- In questo caso l'ipotesi non è specificata, abbiamo solo la tesi.

Dim:

- Assumiamo ***per contraddizione*** che √2 è un razionale, cioè √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^2 è pari
  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 √2 è un irrazionale

Asserzioni espresse con un quantificatore *universale*: Vogliamo provare che ∀x P(x)

Provare che la proprietà vale per tutti i valori nel dominio (può essere complicato), si può utilizzare la dimostrazione per analisi dei casi (con suddivisione della dimostrazione per sottogruppi).

Esempio:

Siano n ed m interi. Provare che "*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 m = 2h + 1 dove k ed h sono due qualunque interi;
- 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 dim precedente prova anche ***∀n∈Z ∀m∈Z*** (Se ***n ed m sono dispari***, allora ***n+m è pari***).

Asserzioni espresse con una *negazione* di un quantificatore *universale*: Vogliamo provare che ¬∀x P(x) ≡ ∃x ¬ P(x)

Controesempi: Simile alla dimostrazione costruttiva di esistenzialità.

3. INSIEMI

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*** è una collezione non ordinata di oggetti, chiamati ***elementi*** dell'insieme.

Esempio:

- 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: $E= \{ x \mid x \text{ è un intero pari e } 50 \leq x \leq 63 \}$

Se gli elementi dell'insieme sono molti si utilizza l'ellissi (…) nella rappresentazione dell'insieme attraverso l'enumerazione.

Esempio:

"insieme degli interi compresi tra 1 e 100" → $A= \{1, 2, \dots, 100\}$ ***("…" sono chiamati ellissi)***

INSIEMI IMPORTANTI

Numeri naturali:	→	$N = \{0,1,2,3, \dots\}$
Interi:	→	$Z = \{\dots, -2,-1,0,1,2, \dots\}$
Interi positivi:	→	$Z^+ = \{1,2, 3, \dots\}$
Numeri razionali:	→	$Q = \{p/q \mid p\in Z, q\in Z, q\neq 0\}$
Numeri reali:	→	R

Esempio:

L' insieme dei numeri *pari* è $\{ 0, 2, 4, 6, 8, 10, \dots \}= \{ 2n \mid n\in N \}$

L' insieme dei numeri *dispari* è $\{ 1, 3, 5, 7, 9, 11, \dots \}= \{ 2n+1 \mid n\in N \}$

Es: Se $P = \{ 2n \mid n\in N \}$ allora $4\in P$, ma $5\notin P$.

3.1 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.

Un ***modo alternativo*** per dire che $A = B$ è $\forall x\ (x\in A) \leftrightarrow (x\in B)$

Esempio:

- $\{1, 2, 3\} = \{1, 2, 2, 3\} = \{3, 1, 2\}$
- 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
- Sono $\{1, 2, 3, 4\}$ e $\{1, 2, 2, 3\}$ insiemi uguali? ***NO***

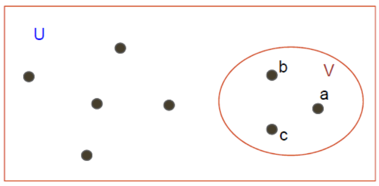
3.2 INSIEMI SPECIALI

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.

Un insieme può essere rappresentato visivamente usando i ***diagrammi di Venn***.

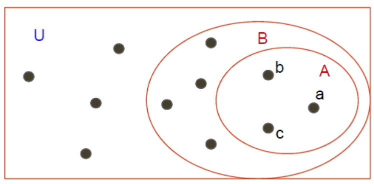
$V = \{a, b, c\}$



3.3 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 $\forall x\ (x\in A) \rightarrow (x\in B)$



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***

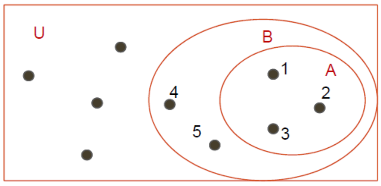
Ma una implicazione → è sempre ***vera*** se l'ipotesi è ***falsa***, quindi $\forall x\ (x\in\emptyset) \rightarrow (x\in S)$ è ***vera***

3.3.1 SOTTOINSIEMI PROPRI

Un insieme A è detto un ***sottoinsieme proprio*** di un insieme B se e solo se ***A⊆B* e *A ≠B***.
Usiamo ***A⊂B*** per indicare che A è un sottoinsieme proprio di B.

<u>*Esempio*</u>:

A={1,2,3} B ={1,2,3,4,5}
A⊂B? SI



3.4 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|***.

<u>*Esempio*</u>:

- A={1,2,3} → |A| = 3
- B ={1,2,3,….., 20} → |B| = 20
- |∅| = 0

Un insieme ***infinito*** è un insieme non finito.

<u>*Esempio*</u>:

- L'insieme dei numeri naturali è infinito: N={0, 1, 2, …} (***N è numerabile***)
- L'insieme dei numeri reali R è infinito (***R non è numerabile***)

3.5 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)***.

Osservazione: Se S è un insieme con |S|=n allora |P(S)| = 2^n.

<u>*Esempi*</u>:

- Consideriamo l'insieme vuoto, ∅
- Quale è l'insieme potenza di ∅? P(∅) = {∅}
- Quale è la cardinalità di P(∅)? |P(∅)| = 1

- Consideriamo l'insieme **{1}**
- Quale è l'insieme potenza di {1} ? P({1}) = {∅, {1}}
- Quale è la cardinalità di P({1}) ? |P({1})| = 2

- Consideriamo l'insieme **{1,2}**
- Quale è l'insieme potenza di {1,2} ? P({1,2}) = { ∅, {1}, {2}, {1,2}}
- Quale è la cardinalità di P({1,2}) ? |P({1,2})| = 4

- Consideriamo l'insieme **{1,2,3}**
- Quale è l'insieme potenza di {1,2,3}? P({1,2,3}) = { , {1}, {2}, {3}, {1,2}, {1,3}, {2,3}, {1,2,3}}
- Quale è la cardinalità di P({1,2,3})? |P({1,2,3})| = 8

3.6 N-PLE (ENNUPLE)

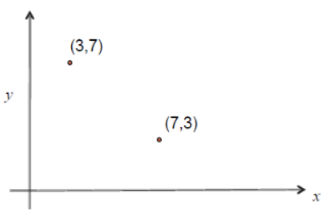
Un insieme è usato per rappresentare una collezione non ordinata di oggetti.
Una ***n-pla*** è usata per rappresentare una ***collezione ordinata*** di oggetti.

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 ≥ 2***.

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

<u>*Esempio*</u>:

Coordinate di un punto nel piano:



3.7 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∈S e t∈T.
Quindi, S x T = { (s,t) | s∈S e t∈T}.

<u>*Esempio*</u>:

S = {1,2} and T = {a,b,c}
S x T = { (1,a), (1,b), (1,c), (2,a), (2,b), (2,c) }
T x S = { (a,1), (a, 2), (b,1), (b,2), (c,1), (c,2) }

Nota: S x T ≠ T x S

Nota: La cardinalità di S x T è |S x T| = |S| * |T|

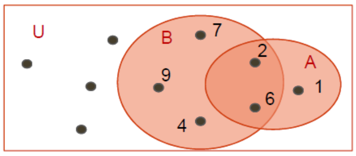
3.8 OPERAZIONI SUGLI INSIEMI

3.8.1 UNIONE

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

<u>*Esempio*</u>:

A = {1,2,6}   B = { 2,4,6,7,9}
A ∪ B = { 1,2,4,6,7,9 }

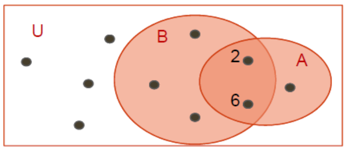


3.8.2 INTERSEZIONE

Siano A e B due insiemi. L'***intersezione*** di A e B, denotata con ***A* ∩ *B***, è l'insieme che contiene gli elementi in A e quelli in B.
Quindi ***A* ∩ *B = { x | x∈A* ∧ *x∈B }***.

<u>*Esempio*</u>:

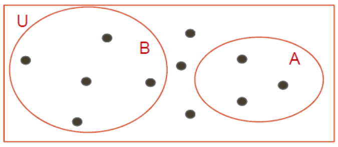
A = {1,2,6}   B = { 2,4,6,7,9}
A ∩ B = {2,6}



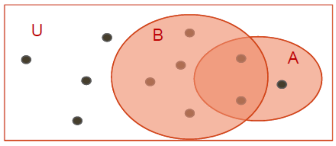
Due insiemi, si dicono ***disgiunti*** se la loro intersezione è vuota, cioè ***A* ∩ *B = ∅***.

<u>*Esempio*</u>:

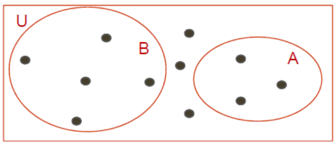
A = {1,2,6}   B = { 0,5,3,8}
A ∩ B = ∅



Cardinalità dell'insieme unione:
La cardinalità dell'insieme unione è ***|A* ∪ *B| = |A| + |B| − |A* ∩ *B|***.
Se si considera |A| + |B| allora si conta |A ∩ B| due volte.
Vale il ***Principio di inclusione ed esclusione.***



Se A e B sono disgiunti allora la cardinalità dell'insieme unione è ***|A* ∪ *B| = |A| + |B|***.

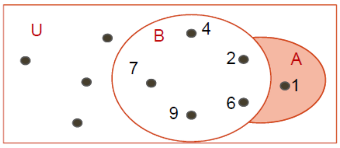


3.8.3 DIFFERENZA

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 ***A − B = { x | x∈A* ∧ *x∉B }***.

<u>*Esempio*</u>:

A = {1,2,6}   B = { 2,4,6,7,9}
A − B = { 1 }



3.8.4 COMPLEMENTO

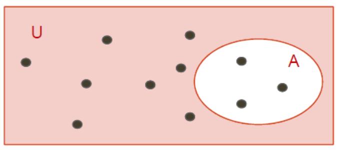
Sia U insieme universale ed A un insieme. Il ***complemento di A***, denotato con $\overline{A}$, è l'insieme di tutti gli elementi di U che non appartengono ad A.
Quindi $\overline{A}$ ***= { x | x∈U* ∧ *x∉A }***.

<u>*Esempio*</u>:

U={1,2,3,4,5,6,7,8} A ={1,3,5,7}
$\overline{A}$ = {2,4,6,8}

<u>*Esempio*</u>:

A = { 2n | n N }
$\overline{A}$ = { 2n+1 | n N } = insieme dei numeri dispari



3.8.5 OPERAZIONI ED IDENTITÀ

A = B   ∀𝑥 (𝑥 ∈ A) ↔ (𝑥 ∈ B)
A ⊆ B   ∀𝑥 (𝑥 ∈ A) → (𝑥 ∈ B)
A ∪ B = { x | x ∈ A ∨ x ∈ B }
A ∩ B = { x | x ∈ A ∧ x ∈ B }
A − B = { 𝑥 | 𝑥 ∈ A ∧ 𝑥 ∉ B }
$\overline{A}$ = { 𝑥 | 𝑥 ∈ U ∧ 𝑥 ∉ A }

Identità
- A ∪ ∅ = A
- A ∩ U = A

Dominazione
- A ∪ U = U
- A ∩ ∅ = ∅

Idempotenza
- A ∪ A = A
- A ∩ A = A

Doppio complemento
- $\overline{\overline{A}}$ = A

Commutativa
- A ∪ B = B ∪ A
- A ∩ B = B ∩ A

Associativa
- (A ∪ B) ∪ C = A ∪ (B ∪ C)
- (A ∩ B) ∩ C = A ∩ (B ∩ C)

Distributiva
- A ∪ (B ∩ C) = (A ∪ B) ∩ (A ∪ C)
- A ∩ (B ∪ C) = (A ∩ B) ∪ (A ∩ 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 ∪ (A ∩ B) = A
- A ∩ (A ∪ B) = A

Leggi del complemento
- A ∪ $\overline{A}$ = U
- A ∩ $\overline{A}$ = ∅

Le identità tra insiemi possono essere provate utilizzando le ***tavole di appartenenza***.

- 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.

Altrimenti possono essere utilizzate le ***equivalenze logiche***.

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

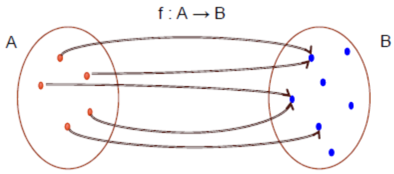
A	B	$\overline{A}$	$\overline{B}$	$\overline{A \cap B}$	$\overline{A} \cup \overline{B}$
1	0	0	1	1	1
1	1	0	0	0	0
0	0	1	1	1	1
0	1	1	0	1	1

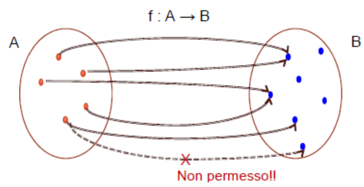
$\overline{A \cap B} = \{ x \mid x \notin A \cap B \}$	def di complemento
$= \{ x \mid \neg(x \in A \cap B) \}$	def di non appartenenza
$= \{ x \mid \neg(x \in A \wedge x \in B) \}$	def di intersezione
$= \{ x \mid \neg(x \in A) \vee \neg(x \in B) \}$	da Legge di DeMorgan
$= \{ x \mid x \notin A \vee x \notin B \}$	def di non appartenenza
$= \{ x \mid x \in \overline{A} \vee x \in \overline{B} \}$	def di complemento
$= \{ x \mid x \in \overline{A} \cup \overline{B} \}$	def di unione
$= \overline{A} \cup \overline{B}$	

3.9 FUNZIONI

Una ***funzione*** mette in relazione oggetti appartenenti ad un insieme con oggetti appartenenti ad un altro insieme (non necessariamente diverso dal primo).

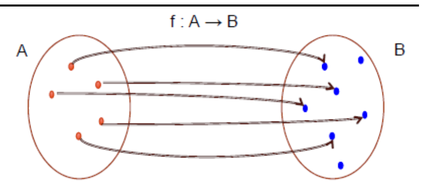
Siano A e B due insiemi. Una ***funzione*** da A in B, denotata f : A → B , associa ciascun elemento di A ad esattamente un elemento di B.





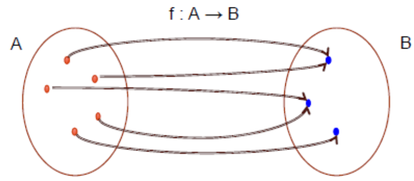
3.9.1 FUNZIONE INIETTIVA

Una funzione è detta ***iniettiva*** se e solo se ***f(x) = f(y) => x =y*** per ogni x ed y nel dominio di f.
Alternativamente, ***x ≠ y => f(x) ≠ f(y).***



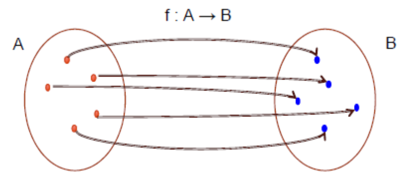
3.9.2 FUNZIONE SURIETTIVA

Una funzione da A a B è detta ***suriettiva*** se e solo se ∀*b*∈B ∃*a*∈A tale che ***f(a) = b.***
Alternativamente, ***f(A)=B***.



3.9.3 FUNZIONE BIETTIVA

Una funzione è detta ***biettiva*** se è sia ***iniettiva*** che ***suriettiva***.



3.9.4 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|.***

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:

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.

3.10 INSIEMI NUMERABILI

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

Dimostrazione:

A={0,2,4,6, ...} cioè A è l'insieme dei numeri pari. Dimostriamo che *A è numerabile*:

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

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

- 1 → 2*1−2 = 0
- 2 → 2*2−2 = 2
- 3 → 2*3−2 = 4 ...

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

Dimostrazione:

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:

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

f è ***iniettiva*** perché:

$f(x) = f(y) \Rightarrow x/2 = y/2 \Rightarrow x=y$ (se x e y sono ***pari***)

$f(x) = f(y) \Rightarrow -(x-1)/2 = -(y-1)/2 \Rightarrow x=y$ (se x e y sono ***dispari***)

f è ***suriettiva*** perché:

$\forall z \in Z$ 2z è un intero pari positivo se z=***positivo***

−2z+1 è un intero dispari positivo se z=***negativo***

Perciò $|Z| = |Z^+|$

Teorema: I numeri razionali positivi sono numerabili

Dimostrazione:

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 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 1/2 e 2/1)
- etc.

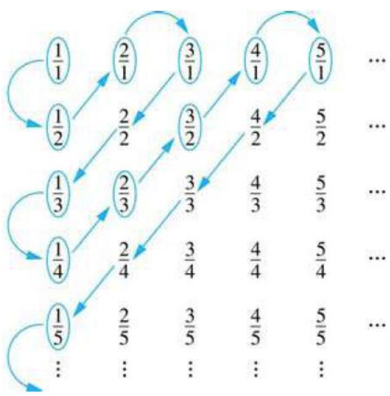
Ogni volta che si incontra un p/q già incontrato non lo si inserisce

- (per esempio 2/2=1/1, 2/4=1/2, ...)

Siccome

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

=> I numeri razionali positivi sono numerabili



Teorema: L'insieme dei numeri reali R non è numerabile

4. INDUZIONE

È una tecnica che può essere applicata per provare asserzioni generali per insiemi di interi positivi, per sequenze associate ad interi.

Usata per provare asserzioni con ***dominio*** $\mathbb{Z}^+$ della forma: $\forall n\ P(n)$

Consiste di due passi:

1. ***Base***: La proposizione P(1) è vera;
2. ***Passo di induzione***: fissato un intero positivo n, l'implicazione P(n) → P(n+1) è vera. (L'assunzione P(n) è chiamata ***ipotesi induttiva***)

Si conclude perciò che ∀n P(n).

Nota:

- Dalla Base so che P(1) è vera;
- Dal Passo di induzione so che P(1) → P(2) è vera (perché P(1) è vera)
- Dal Passo di induzione so che P(2) → P(3) è vera (perché P(2) è vera)
- …

Quindi P(n) è vera $\forall n \in \mathbb{Z}^+$

Esempio:

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

In questo caso P(n): $1+3+5+7+\ldots+(2n-1) = n^2$

Base:

Mostrare che P(1) è vera: Banale: $1=1^2$

Passo Induttivo:

Mostrare che ***se*** P(n) è vera ***allora*** P(n+1) è vera, per un qualunque fissato n

Supponiamo che P(n) è vera: $1+3+5+7+\ldots+(2n-1) = n^2$

Mostriamo che P(n+1) è vera: $\underbrace{1+3+5+7+\ldots+(2n-1)}_{n^2}+(2n+1) = (n+1)^2$

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

4.1 CORRETTEZZA DELL'INDUZIONE MATEMATICA

Supponiamo che P(1) è vera, allora P(n) → P(n+1) è vera per tutti gli interi positivi, quindi vogliamo provare che ∀n P(n) è vera.

Per ***contraddizione***, assumiamo che c'è almeno un intero positivo ***m*** tale che ***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 che $k \neq 1$ poichè P(1) è vera)

Sia k il più piccolo intero in S tale che P(k) è falsa

Questo implica che k − 1 > 0 e P(k − 1) è vera

Ma P(k − 1) → P(k) è vera, per ipotesi

Siamo arrivati ad una contraddizione → ∀n P(n) è vera

Esempio1:

Proviamo che $n < 2^n$ 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)
- 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
  - $n + 1 < 2^n + 1$ (per ipotesi induttiva)

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

Esempio2:

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: Mostrare che

  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
  - $(n+1)^3 - (n+1) = n^3 + 3n^2 + 3n + 1 - n - 1 =$
  - $(n^3 - n) + 3n^2 + 3n = \underbrace{(n^3 - n)}_{\text{divisibile per 3 (ipotesi induttiva)}} + \underbrace{3(n^2 + n)}_{\text{divisibile per 3}}$ □

4.2 INDUZIONE MATEMATICA (GENERALIZZAZIONE)

Si può usare l'induzione matematica anche quando si vuole provare che ***P(n)*** è vera 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) → P(n+1) è vera.

Nota che ***b*** può essere negativo, zero o positivo.

Esempio1:

Proviamo che $n^2 < 2^n$ per tutti gli interi $n \geq 5$

Dim. P(n): $n^2 < 2^n$ per ogni intero $n \geq 5$

- Base: P(5) è vera , infatti $25 = 5^2 < 2^5 = 32$ (ovvio)
- Passo di induzione: Mostrare che

  se P(n) è vera allora P(n+1) è vera per $n \geq 5$

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

    $= n^2 + 3n < n^2 + n\,n = n^2 + n^2$ (perché $n \geq 5 > 3$)

    $= 2\,n^2 < 2\;2^n = 2^{n+1}$ (per ipotesi induttiva)

Esempio2:

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) è vera:

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

  $= (1 + 2 + 2^2 + \ldots + 2^n) + 2^{n+1}$

  $= 2^{n+1} - 1 + 2^{n+1}$ (per ipotesi induttiva)

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

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

Esempio3:

Provare per induzione che un insieme con n elementi ha 2^n sottoinsiemi

Dim. P(n): "un insieme con n elementi ha 2^n sottinsiemi"

- Base: Proviamo P(0)
  - Se un insieme ha 0 elementi allora esso è l'insieme vuoto
  - L'insieme vuoto ha $1 = 2^0$ sottinsiemi (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 => $T = S \cup \{a\}$ dove $|S|=n$
  - I sottinsiemi di T possono essere ottenuti in questo modo:
    * Per ogni sottinsieme X di S, ci sono 2 sottinsiemi di T, cioè X e $X \cup \{a\}$
    * Tali insiemi sono tutti distinti
    * Quindi ci sono 2 sottinsiemi di T per ogni sottinsieme di S
    * Il numero di sottinsiemi di T = 2 (il numero di sottinsiemi di S)

      $= 2\;2^n$

      $= 2^{n+1}$

INDUZIONE FORTE		INDUZIONE REGOLARE	
1. Passo base:	P(1)	1. Passo base:	P(1)
2. Passo di induzione:	$[P(1) \wedge P(2) \wedge \ldots \wedge P(n)] \rightarrow P(n+1)$	2. Passo di induzione:	$P(n) \rightarrow P(n+1)$

Esempio1:

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) (ipotesi induttiva)

  Dimostriamo che P(n+1) è anch'essa vera

  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 essere scritto come il prodotto di primi

Esempio2:

P(n): con n cerini per ciascuna delle due scatole, il giocatore che gioca per secondo può vincere.

Dim.

- Base: n=1

  - il primo giocatore ha una sola scelta: togliere l'unico cerino da una delle due scatole
  - il secondo giocatore vince togliendo l'unico ed ultimo cerino dalla 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 x il numero di cerini che il primo giocatore elimina da una delle due scatole => 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

  ➔ 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) è vera

4.4 SCHEMA PER LE DIMOSTRAZIONI PER INDUZIONE

Formula un predicato che descrive il problema in funzione di un intero ***n***: individua ***P(n)***

Esprimi ciò che deve essere provato come $\forall n \geq b$, P(n): individuare sempre il ***b*** più adatto al problema

Suddividi la dimostrazione in:

BASE	IPOTESI	PASSO DI INDUZIONE
Mostrare che P(b) è vera	Esprimi in modo chiaro: "Assumiamo che P(n) è vera per un arbitrario $n \geq b$".	Affermare ciò che si deve provare, scrivendo in maniera esplicita che cosa dice P(n+1). Provare P(n+1) facendo uso dell'ipotesi induttiva P(n).

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

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

5. RICORSIONE

Dato un oggetto, come funzioni, insiemi, algoritmi, … in alcuni casi esso può essere ***definito in termini di sé stesso, ma di più piccole dimensioni***.

Esempi:

Consideriamo la sequenza di interi 1, 3, 9, 27, 81, …

È evidente che è la sequenza di potenze di 3, cioè

- 1, 3, 9, 27, 81, …, 3^n, …
- $3^0, 3^1, 3^2, 3^3, 3^4, \ldots, 3^n, \ldots$
- $b_n = 3^n$ (n--simo termine della sequenza), $n \in \mathbf{N}$

Definizione ricorsiva della sequenza

- $b_n = 3\ 3^{n-1}$
- $b_n = 3\ b_{n-1}$ per $n \geq 1$

  $b_0 = 1$

Consideriamo la sequenza aritmetica (progressione aritmetica)

- a, a+d, a+2d, a+3d, …, a+nd, …
  - a= −1 e d= 4 => −1, 3, 7, 11, …, −1+n4, …
- b_n = a+nd (n--simo termine della sequenza), $n \in \mathbf{N}$

Definizione ricorsiva della sequenza

- b_n = a+nd = a+ (n−1)d +d
- $b_n = b_{n-1} + d$ per $n \geq 1$

  $b_0 = a$

Consideriamo la sequenza geometrica (progressione geometrica)

- a, ar, ar^2, ar^3, …, ar^n, …
  - a= 6 e r= 1/3 => 6, 2, 2/3, 2/9, …, $6\ (1/3)^n$, …
- $b_n = a\ r^n$ (n--simo termine della sequenza), $n \in \mathbf{N}$

Definizione ricorsiva della sequenza

- $b_n = a\ r^n = a\ r^{n-1}\ r$
- $b_n = b_{n-1}\ r$ per $n \geq 1$

  $b_0 = a$

5.1 DEFINIRE FUNZINI RICORSIVE

In alcuni casi la definizione ricorsiva di un oggetto può essere molto facile da scrivere.

Esempio: Funzione fattoriale

- n! = n (n − 1)! per $n \geq 1$

  0!=1

In altri casi la definizione ricorsiva di un oggetto è l'unico modo per descriverlo.

Esempio: Numeri di Fibonacci

- $F_n = F_{n-1} + F_{n-2}$ per $n \geq 2$

  $F_0=0$ $F_1=1$

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

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

Esempio: 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) = 2 n +1= 2 (n −1+1) + 1 = 2 (n −1) +1 + 2 = f(n−1) + 2

Quindi

1. f(0)=1 e 2. f(n)= f(n−1) +2 per $n \geq 1$

Esempio: definire ricorsivamente la funzione che somma i primi n interi positivi f(n) = 1+2+3+…. +n per $n \geq 1$

- f(1)=1

So che f(n) = 1+2+3+…. +n−1 + n

- f(n) = (1+2+3+…. +n−1) + n

  = f(n−1) +n

Quindi

1. f(1)=1
2. f(n)= f(n−1) +n per $n \geq 2$

Esempio: definire ricorsivamente la funzione $f(n) = n^2$ per $n \geq 1$

- f(1) = 1

So che $f(n-1) = (n-1)^2$ Devo arrivare a $f(n) = n^2$

Come posso "manipolare" $f(n-1) = (n-1)^2$ per arrivare a $f(n) = n^2$?

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

Quindi

1. f(1)=1 e 2. f(n)= f(n-1) +2n-1 per $n \geq 2$

5.2 CALCOLO DI FUNZIONI RICORSIVE

Esempio: sia f una funzione ricorsiva definita come

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

Quale 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: Funzione fattoriale

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

Calcoliamo 4!

- 4! = 4 • 3! Passo ricorsivo

  = 4 • 6 =24
- 3! = 3 • 2! Passo ricorsivo

  = 3 • 2 =6
- 2! = 2 • 1! Passo ricorsivo

  = 2 • 1 =2
- 1! = 1 • 0! Passo ricorsivo

  = 1 • 1 =1
- 0! = 1 Passo base

Esempio: 1. f(1)=1 e 2. f(n)= f(n-1) +2n-1 per $n \geq 2$

- f(4) = f(3) + 2 • 4 - 1
- f(3) = f(2) + 2 • 3 - 1
- f(2) = f(1) + 2 • 2 - 1
- f(1) = 1

  f(2) = f(1) + 2 • 2 - 1 = 1 + 2 • 2 - 1 = 4

  f(3) = f(2) + 2 • 3 - 1 = 4 + 2 • 3 - 1 = 9

  f(4) = f(3) + 2 • 4 - 1 = 9 + 2 • 4 - 1 = 16

5.3 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.

Esempio 1: 1. f(0)=3 e 2. f(n)=2 f(n−1) +3 per $n \geq 1$

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

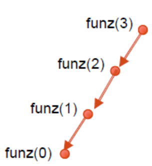
Tale procedura realizza quanto abbiamo fatto precedentemente nella slide 16

f(3) = 2 f(2) + 3

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

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

f(0) = 3



f(3) = 2 f(2) + 3

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

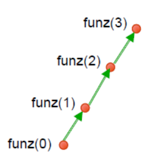
f(1) = 2 f(0) + 3

f(0) = 3

f(1) = 2 • 3 + 3 = 9

f(2) = 2• 9 + 3 = 21

f(3) = 2• 21 + 3 = 45



Correttezza degli Algoritmi Ricorsivi: (correttezza = produce output corretto per ogni possibile input)

Proviamo la correttezza dell'algoritmo descritto dalla procedura ***funz(n)***

Dimostriamo, cioè che il valore restituito dalla procedura ***funz(n)*** coincide con ***f(n)***

Dimostrazione:

Usiamo l'induzione matematica su n.

Base: Se n=0, il primo passo dell'algoritmo ci 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 2 funz(n) + 3 coincide con 2 f(n) +3 = ***f(n+1)***

Esempio 2: funzione fattoriale

1. 0!=1 e 2. n!=n (n−1)! per n≥1

```
procedure fattoriale(n)
if n=0 then return 1
      else return n• fattoriale(n−1)
```

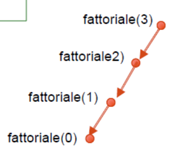
Dovendo calcolare fattoriale(3)

fattoriale(3) = 3 • fattoriale(2) =

fattoriale(2) = 2 • fattoriale(1) =

fattoriale(1) = 1 •fattoriale(0)

fattoriale(0) = 1



fattoriale(3) = 3 • fattoriale(2) =

fattoriale(2) = 2 • fattoriale(1) =

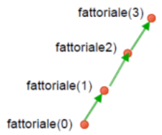
fattoriale(1) = 1 •fattoriale(0)

fattoriale(0) = 1

fattoriale(1) = 1 • 1 = 1

fattoriale(2) = 2 • 1 = 2

fattoriale(3) = 3 • 2 = 6



Proviamo la correttezza dell'algoritmo descritto dalla procedura ***fattoriale(n)***

Dimostriamo, cioè che il valore restituito dalla procedura ***fattoriale(n)*** coincide con ***n!***

Dimostrazione:

Usiamo l'induzione matematica su n.

Base: Se n=0, il primo passo dell'algoritmo ci 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)*n!= ***(n+1)!***

Esempio 3: Numeri di Fibonacci

1. F(0)=0, F(1)=1 e 2. F(n) = F(n−1) + F(n−2) per n≥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)
```

Dovendo calcolare Fibonacci(4)

Fibonacci(4) = Fibonacci(3) + Fibonacci(2)

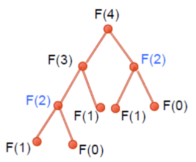
Fibonacci(3) = Fibonacci(2) + Fibonacci(1)

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

Fibonacci(1) = 1 Fibonacci(0) = 0

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

Fibonacci(1) = 1 Fibonacci(0) = 0

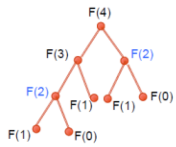


NOTA Non sempre gli algoritmi ricorsivi sono efficienti, essi però sono semplici da progettare

Nel calcolo di Fibonacci(4) con l'algoritmo ricorsivo valutiamo due volte Fibonacci(2)

Fibonacci(4)= Fibonacci(3) + Fibonacci(2) =

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



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

1. F(0)=0, F(1)=1

2. F(n) = F(n-1) + F(n-2) per n≥3

```
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***.

5.4 USO DI DEFINIZIONI RICORSIVE

Le definizioni ricorsive possono essere usate nelle ***dimostrazioni***:

Esempio:

Sia F(n) n-simo termine della sequenza dei numeri di Fibonacci.

Provare che per $n \geq 3$, $F(n) > \alpha^{n-2}$ dove $\alpha = (1+\sqrt{5})/2$

Dimostrazione:

Usiamo l'induzione forte:

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 $F(j) > \alpha^{j-2}$

Passo di induzione: Consideriamo ora F(n+1) e la sua definizione, poi applichiamo l'ipotesi induttiva

$F(n+1) = F(n-1)+F(n) > \alpha^{n-3} + \alpha^{n-2} = \alpha^{n-3}(1+\alpha) = \alpha^{n-3}\alpha^2 = \alpha^{n-1}$

Ricordate: 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 proprieta P}***

Un altro modo per descrivere ***insiemi*** è attraverso una definizione 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 $x + 2 = 3 + 2 = 5 \in A$

$1, 3, 5, 7, 9 \dots \in A$

Proveremo utilizzando l'induzione strutturale che A è l'insieme degli interi dispari positivi

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

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

L'insieme di stringhe Σ^* sull'alfabeto Σ è definito ricorsivamente nel modo seguente:

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.
$\Sigma = \{a,b,\dots,z\}$, zaino $\in \Sigma^*$ l(zaino) = 5

La ***lunghezza di una parola*** in Σ^* sull'alfabeto Σ è definito ricorsivamente nel modo seguente

Passo base: $l(\lambda) = 0$

Passo ricorsivo: Se ***w*** $\in \Sigma^*$ e $x \in \Sigma$ allora l(***w***x) = l(***w***) + 1

Le definizioni ricorsive possono essere usate per descrivere ***parole palindrome:***

Una stringa è ***palindroma*** se letta da sinistra a destra o viceversa, è la stessa.
alla, otto, ingegni, Anna, ottetto.

L'insieme delle parole palindrome sull'alfabeto $\Sigma = \{a, b\}$ è definito ricorsivamente nel modo seguente:

Passo base: a, b, λ sono parole palindrome

Passo ricorsivo: Se w è una parola palindroma allora anche awa e bwb sono parole palindrome

Esempio:

abba è una parola palindroma:

- λ è una parola palindroma ***Passo base***
- $b\lambda b$ =bb è una parola palindroma ***Passo ricorsivo***
- a bb a è una parola palindroma ***Passo ricorsivo***

Le definizioni ricorsive possono essere usate per descrivere ***espressioni aritmetiche***.

Una ***espressione aritmetica*** è definita ricorsivamente nel modo seguente

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 $(E_1 + E_2)$, $(E_1 - E_2)$, $(E_1 \times E_2)$, $(E_1 \backslash E_2)$ sono espressioni aritmetiche.

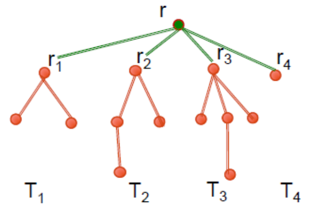
Se E è un'espressione aritmetica allora $(-E)$ è un'espressione aritmetica.

Le definizioni ricorsive possono essere usate per descrivere ***strutture dati***.

Un ***albero radicato*** può essere descritto ricorsivamente nel modo seguente:

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 <u>radici</u> $r_1, r_2, \ldots, r_n$.
Allora, il grafo formato dalla <u>radice</u> 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:

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

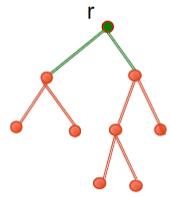
Passo Ricorsivo: Supponiamo che $T_1= (V_1,E_1)$, $T_2= (V_2,E_2)$, …, $T_n= (V_n,E_n)$ sono alberi radicati disgiunti, cioè $V_i \cap V_j =$ per $1 \leq i \neq j \leq n$ con <u>radici</u> $r_1, r_2, \ldots, r_n$, dove $r_1 \in V_1$, $r_2 \in V_2$, …, $r_n \in V_n$.
Allora, il grafo T=(V,E) con $V=\{r\}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

Un ***albero binario pieno*** è un albero radicato dove ciascun vertice ha 0 o 2 figli; se tali figli esistono, essi sono chiamati figlio destro e figlio sinistro.

Un **albero binario pieno** è descritto ricorsivamente nel modo seguente:

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 la radice del sottoalbero destro T_2 è un albero binario pieno.

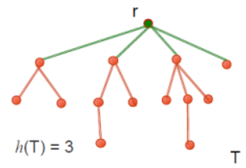


Le definizioni ricorsive possono essere usate per ***ottenere nuove definizioni ricorsive***.

L'altezza h(T) di un albero radicato T è definita ricorsivamente come:

Passo base: h(T) = 0 se T consiste della sola radice r

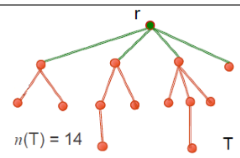
Passo ricorsivo: $h(T) = 1 + \max \{h(T_1), \ldots, h(T_n)\}$ se $T_1, \ldots, T_n$ sono i sottoalberi di T



Il **numero di vertici n(T)** di un albero radicato T è definita ricorsivamente come:

Passo base: n(T) = 1 se T consiste della sola radice r

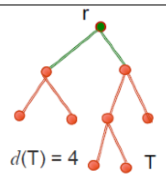
Passo ricorsivo: $n(T) = 1 + n(T_1) + \ldots + n(T_n)$ se $T_1, \ldots, T_n$ sono i sottoalberi di T



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

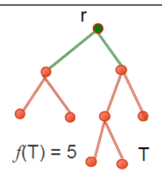
Passo ricorsivo: $d(T) = 1 + d(T_1) + d(T_2)$ se T_1 e T_2 sono i sottoalberi di T



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

Passo ricorsivo: f(T) = f(T1) + f(T2) se T1 e T2 sono i sottoalberi di T

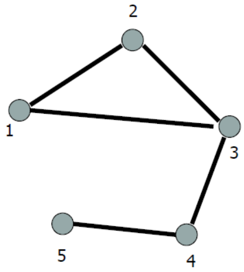
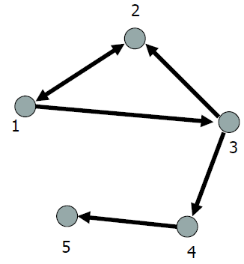
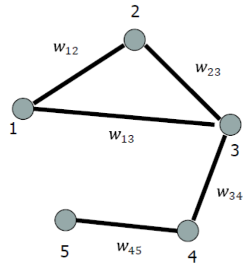


6. GRAFI

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 ***nodi*** (***vertici***), e i link sono ***archi***.

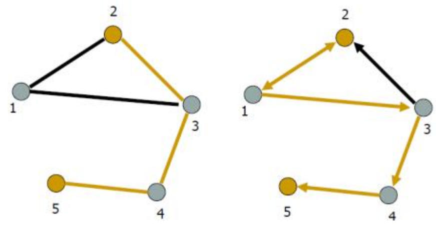
Un ***grafo*** è definito come **G= (V, E)**, dove **V= insieme dei vertici** (**nodi**) e **E= insieme degli archi**.

Esistono diversi tipi di grafi, tra cui:

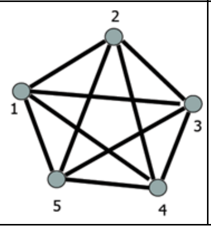
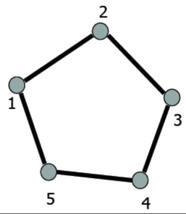
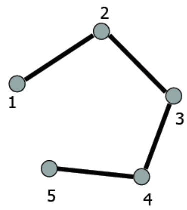
GRAFI NON DIREZIONATI	GRAFI DIREZIONATI	GRAFI PESATI
Grafo G= (V, E), dove V= {1, 2, 3, 4, 5} E= {(1,2),(1,3),(2,3),(3,4),(4,5)}  **Neighborhood N(i)** del nodo i è l'insieme dei nodi adiacenti ad i, nell'esempio precedente: N(1)={2,3}, N(2)={1,3}, N(3)={1,2,4}, N(4)={3,5}, N(5)={4}. **Degree** (**grado**) **d(i)** del nodo i è la Size di N(i), ovvero il numero di archi incidenti su i: d(1)=2,d(2)=2,d(3)=3,d(4)=2,d(5)=1.	Grafo G= (V, E), dove 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 è il numero di archi che entrano in i: $d_{in}(1)=1$, $d_{in}(2)=2$, $d_{in}(3)=1$, $d_{in}(4)=1$, $d_{in}(5)=1$. **out-degree d_{out}(i)** del nodo i è il numero di archi che escono da i: $d_{out}(1)=2$, $d_{out}(2)=1$, $d_{out}(3)=2$, $d_{out}(4)=1$, $d_{out}(5)=0$.	Grafo G= (V, E), dove 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})} 

6.1 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***.
La ***lunghezza di un cammino*** è il numero di archi del cammino.
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.
Lo ***Shortest Path*** dal nodo ***i*** al nodo ***j*** è il cammino più corto tra tutti i cammini che congiungono i e j.
Il ***diametro*** è il più lungo shortest path nel grafo.

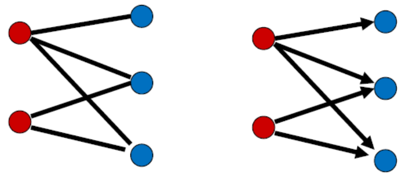


Esistono casi particolari di grafi, come:

GRAFO COMPLETO	GRAFO CICLO	GRAFO LINEA
È un grafo che ha ogni nodo connesso a tutti gli altri, denotato con **Clinque K_n.** K_n V = {v_1, v_2, …, v_n} E = {(v_i, v_j) | 1≤i,j ≤n e i≠j }	È un grafo che consiste di un unico ciclo o di un certo numero di vertici connessi in una catena chiusa, denotato con **Ciclo C_n**. C_n V = {v_1, v_2, …, v_n} E= {(v_1, v_2),(v_2, v_3),… , (v_{n-1}, v_n), (v_n, v_1)}	È un grafo che consiste in un unico path, denotato con **Linea L_n**. L_n V = {v_1, v_2, …, v_n} E= {(v_1, v_2),(v_2, v_3),… , (v_{n-1}, v_n)}
K_5 con V={1,2,3,4,5} ed E={(1,2), (1,3), (1,4), (1,5), (2,3), (2,4), (2,5), (3,4), (3,5), (4,5)} 	C_5 con V={1,2,3,4,5} ed E={(1,2), (2,3), (3,4), (4,5), (5,1)} 	L_5 con V={1,2,3,4,5} ed E={(1,2), (2,3), (3,4), (4,5)} 

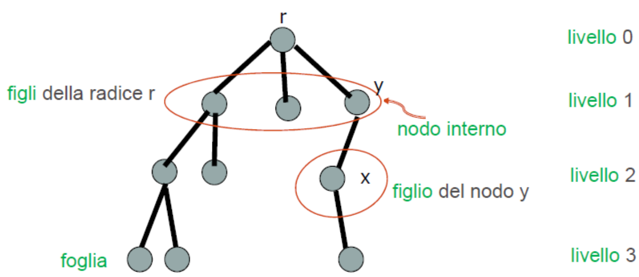
GRAFO BIPARTITO

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



6.2 ALBERO

Un **Albero** è un grafo connesso non direzionato ***senza cicli***.
Un **Albero radicato** è 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;
L'***altezza h(T)*** di T è definita la più grande profondità di un vertice in T, *h(T) = 3.*



7. INDUZIONE STRUTTURALE

Dovendo provare proprietà di oggetti ***definiti ricorsivamente*** può essere utile la ***induzione strutturale***.

Sia A = un insieme di ***elementi definiti ricorsivamente*** e P = ***proprietà*** avente come oggetto gli elementi di A, si vuole provare che ∀x∈A P(x), con l'***induzione strutturale*** basta provare che:

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 nel Passo Ricorsivo della definizione di A
- Allora l'enunciato P è vero per questi nuovi elementi.

Esempio 0: 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
$D=\{y \in Z^+ \mid \exists k \ (k \geq 0 \land y=2k+1)\}$

Dobbiamo provare che D = A

Proveremo quindi che $D \subseteq A$ e $A \subseteq D$

Dim. Proviamo prima che $D \subseteq A$

Procediamo usando l'induzione matematica
P(k): $2k+1 \in A \quad \forall k \geq 0$

Base: proviamo che P(0) è vera

$2 \bullet 0+1 = 1 \in A$

Ipotesi induttiva: assumiamo che P(k) è vera

Passo di induzione: proviamo che P(k+1) è vera
$2 \bullet (k+1) + 1 = (2 \bullet k+ 1) +2 \in A$

ipotesi induttiva — definizione ricorsiva

Dim. Ora proviamo che $A \subseteq D$

Procediamo usando l'induzione strutturale
P(x): $x = 2k+1$ per qualche intero $k \geq 0 \quad \forall x \in A$

Usiamo la definizione ricorsiva di A

Base: Da passo base della definizione ricorsiva sappiamo che 1∈A, poichè $1 = 2 \bullet 0 +1$ => P(1) è vera

Passo di ricorsione: usiamo la seconda parte della definizione ricorsiva di A, e consideriamo un $x+2 \in A$
- assumiamo che P(x) è vera
- proviamo che P(x+2) è vera

$x=2k+1$ per qualche intero $k \geq 0$

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

Esempio 1: 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
$M=\{y \in Z^+ \mid \exists k \ (k \in Z^+ \land y=3k)\}$

Dobbiamo provare che M = A

Proveremo quindi che $M \subseteq A$ e $A \subseteq M$

Dim. Proviamo prima che $M \subseteq A$

Procediamo usando l'induzione matematica
P(k): $3k \in A \quad \forall k \geq 1$

Base: proviamo che P(1) è vera

$3 \bullet 1 = 3 \in A$

Ipotesi induttiva: assumiamo che P(k) è vera

Passo di induzione: proviamo che P(k+1) è vera

$3 \bullet (k+1) = 3 \bullet k+ 3 \in A$

ipotesi induttiva — definizione ricorsiva

Dim. 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

Base: Dalla base della definizione ricorsiva sappiamo che 3∈A, poichè $3 = 3 \bullet 1$ => 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) e P(y) è vera
- proviamo che P(x+y) è vera

$x=3k$ e $y= 3h$ per qualche intero $k \geq 1$ e $h \geq 1$

$x+y = 3k + 3h = 3(h+k) \in M$

Esempio 2: 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 $w \in \Sigma^*$" (ricordiamola)

Passo base: $\lambda \in \Sigma^*$

Passo ricorsivo: Se $w \in \Sigma^*$ e $x \in \Sigma$ allora $wx \in \Sigma^*$

Ricordiamo la "definizione ricorsiva di lunghezza della stringa $w \in \Sigma^*$"

Passo base: $\lambda \in \Sigma^*$

Passo ricorsivo: Se $w \in \Sigma^*$ e $x \in \Sigma$ allora $wx \in \Sigma^*$

Dobbiamo provare che $\forall w \in \Sigma^*$ P(w)

dove P(w): $\ell(u\,w) = \ell(u) + \ell(w)$ per ogni $u \in \Sigma^*$

P(w): $\ell(u\,w) = \ell(u) + \ell(w)$ per ogni $u \in \Sigma^*$

Base: dobbiamo mostrare che P(λ) è vera

$\ell(u\,\lambda) = \ell(u) = \ell(u) + 0 = \ell(u) + \ell(\lambda)$

Passo di ricorsione: - assumiamo che P(w) sia vera

- proviamo che P(wx) è vera per ogni $x \in \Sigma$

$\ell(u\,wx) = \ell(u\,w) + 1 = \ell(u) + \ell(w) +1 = \ell(u) + \ell(wx)$

def. ricorsiva di ℓ — ipotesi induttiva — def. ricorsiva di ℓ

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

Il numero di nodi con due figli $d(\mathrm{T})$ di un albero binario pieno T è definita

Passo base $d(\mathrm{T}) = 0$ se T consiste della sola radice r

Passo ricorsivo $d(\mathrm{T}) = 1 + d(\mathrm{T}_1) + d(\mathrm{T}_2)$ se T_1 e T_2 sono i sottoalberi destro e sinistro di T

Il numero di foglie $f(\mathrm{T})$ di una albero binario pieno T è definito

Passo base $f(\mathrm{T}) = 1$ se T consiste della sola radice r

Passo ricorsivo $f(\mathrm{T}) = f(\mathrm{T}_1) + f(\mathrm{T}_2)$ se T_1 e T_2 sono i sottoalberi destro e sinistro di T

L'altezza $h(\mathrm{T})$ di una albero binario pieno T è definita

Passo base $h(\mathrm{T}) = 0$ se T consiste della sola radice r

Passo ricorsivo $h(\mathrm{T}) = 1 + \max\{h(\mathrm{T}_1), h(\mathrm{T}_2)\}$ se T_1 e T_2 sono i sottoalberi destro e sinistro di T

Il numero di vertici $n(\mathrm{T})$ di una albero binario pieno T è definito

Passo base $n(\mathrm{T}) = 1$ se T consiste della sola radice r

Passo ricorsivo $n(\mathrm{T}) = 1 + n(\mathrm{T}_1) + n(\mathrm{T}_2)$ se T_1 e T_2 sono i sottoalberi destro e sinistro di T

Esempio 3: Se T è un albero binario pieno, sia

$d(\mathrm{T})$ = il numero di vertici di T con due figli

$f(\mathrm{T})$ = il numero di foglie di T

allora $f(\mathrm{T}) \leq d(\mathrm{T}) + 1$

Dim. Usiamo l'induzione strutturale ("definizione ricorsiva di T").

P(T): $f(\mathrm{T}) \leq d(\mathrm{T}) + 1$ 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 è l'albero costituito dalla sola radice: dalla definizione di d e di di f si ha

$$d(\mathrm{T}) = 0 \quad \text{e} \quad f(\mathrm{T}) = 1$$

Quindi $f(\mathrm{T}) = 1 = 0+1 = d(\mathrm{T}) + 1$

Passo di ricorsione:

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

- assumiamo che P(T_1) e che P(T_2) siano vere:

$$f(\mathrm{T}_1) \leq d(\mathrm{T}_1) + 1$$

$$f(\mathrm{T}_2) \leq d(\mathrm{T}_2) + 1$$

- proviamo che P(T) è vera: $f(\mathrm{T}) \leq d(\mathrm{T}) + 1$

Ricordando che

$f(\mathrm{T}) = f(\mathrm{T}_1) + f(\mathrm{T}_2)$

$d(\mathrm{T}) = 1 + d(\mathrm{T}_1) + d(\mathrm{T}_2)$

Quindi $f(\mathrm{T}) = f(\mathrm{T}_1) + f(\mathrm{T}_2)$ def. ricorsiva di f

$\leq (d(\mathrm{T}_1) + 1) + (1 + d(\mathrm{T}_2))$ ipotesi induttiva su T_1 e T_2

$= (1 + d(\mathrm{T}_1) + d(\mathrm{T}_2)) + 1 = d(\mathrm{T}) + 1$ def. ricorsiva di d

Esempio 3: Se T è un albero binario pieno, allora

$$n(\mathrm{T}) \leq 2^{h(\mathrm{T})+1} - 1$$

Dim. Usiamo l'induzione strutturale (definizione ricorsiva di T).

P(T): $n(\mathrm{T}) \leq 2^{h(\mathrm{T})+1} - 1$ 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 è l'albero costituito dalla sola radice

Dalla definizione di h si ha $h(\mathrm{T}) = 0$

Dalla definizione di n si ha $n(\mathrm{T}) = 1$

Quindi $n(\mathrm{T}) = 1 = 2^{0+1} - 1 = 2^{h(\mathrm{T})+1} - 1$

Passo di ricorsione:

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

- assumiamo che P(T_1) e che P(T_2) siano vere:

$$n(\mathrm{T}_1) \leq 2^{h(\mathrm{T1})+1} - 1$$

$$n(\mathrm{T}_2) \leq 2^{h(\mathrm{T2})+1} - 1$$

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

$n(\mathrm{T}) = 1 + n(\mathrm{T}_1) + n(\mathrm{T}_2)$ def. ricorsiva di n

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

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

$\leq 2 \max\{2^{h(\mathrm{T1})+1}, 2^{h(\mathrm{T2})+1}\} - 1$

$\leq 2\, 2^{\max\{h(\mathrm{T1}),\, h(\mathrm{T2})\}+1} - 1$

$\leq 2\, 2^{h(\mathrm{T})} - 1 = 2^{h(\mathrm{T})+1} - 1$ def. ricorsiva di h

8. RELAZIONI DI RICORRENZA

Una ***definizione ricorsiva di una sequenza*** è uguale ad 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

$a_n = a_{n-1}\, r \qquad n \geq 1$ (relazione di ricorrenza)

$a_0 = b$ (condizione iniziale)

Nelle lezioni precedenti abbiamo visto come dare una definizione ricorsiva alle sequenze. Ora ci poniamo il problema inverso:
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.

Esempio: complessità asintotica della procedure fattoriale(n) può essere descritta dalla relazione di ricorrenza

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

$T(1) = a$

dove a = costo per effettuare *return* 1
b = costo per effettuare il prodotto n• fattoriale(n−1)

8.1 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*** o ***limiti inferiori*** alle relazioni di ricorrenza

METODO DELLA SOSTITUZIONE:

Idea: "*indovinare*" una soluzione, e verificare che essa "funziona", il metodo consiste nei passi seguenti:

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

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

$T(1) = b$

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

Base: $T(1) = b \leq c \cdot 1$ per ogni $c \geq b$

Ipotesi induttiva: supponiamo che $T(n-1) \leq c\,(n-1)$

Passo induttivo: $T(n) = T(n-1) + a \leq c\,(n-1) + a = c\,n + (a-c)$

ma $c\,n + (a-c) \leq c\,n$ per $a - c \leq 0$

quindi $T(n) \leq c\,n$ per $c \geq a$ e $c \geq b$

abbiamo determinato un limite superiore per T(n):
$T(n) \leq c\,n$ per $c \geq a$ e $c \geq b$

Possiamo però volere anche un limite inferiore per T(n).

- ipotizziamo che $T(n) \geq h\, n$ una costante h opportuna (che deve essere ancora determinata),
- verifichiamolo con l'induzione

Base: $T(1) = b \geq h \cdot 1$ per ogni $h \leq b$

Ipotesi induttiva: supponiamo che $T(n-1) \geq h\,(n-1)$

Passo induttivo: $T(n) = T(n-1) + a \geq h\,(n-1) + a = h\,n - h + a$

ma $h\,n + (a-h) \geq h\,n$ per $a - h \geq 0$

quindi $T(n) \geq h\,n$ per $h \leq a$ e $h \leq b$

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

Possiamo però essere più precisi.

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

Base: $T(1) = b = a \cdot 0 + b$

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

$T(1)=1$

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

Base: $T(1)=1 \le c \cdot 1$ 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 $(c/2+1)\, n \le c\, n$ per $c \ge 2$

quindi $T(n) \le c\, n$ per $c \ge 2$

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

$T(2)=1$

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

Base: $T(2)=1 \le c \cdot 1 = c \log_2 2$ per ogni $c \ge 1$

Ipotesi induttiva: supponiamo che $T(n/2) \le c \log_2(n/2)$

Passo induttivo: $T(n)= 1 + T(n/2) \le 1 + c \log_2(n/2)$

$= 1 + c\,(\log_2 n - 1)$

$= 1 - c + c \log_2 n$

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 $c \ge 1$

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

$T(1)=1$

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

Base: $T(1)=1 \le c \cdot 1 = c\,(\log_2 1+1)$ 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 $1+ c \log_2 n \le c\,(\log_2 n +1)$ per $c \ge 1$

quindi $T(n) \le c\,(\log_2 n +1)$ per $c \ge 1$

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

$T(1) = 1$

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

Base: $T(1)=1 \le c \cdot 1$ per ogni $c \ge 1$

Ipotesi induttiva: supponiamo che $T(n/2) \le c\,(n/2)^2$

$T(2n/3) \le c\,(2n/3)^2$

Passo induttivo: $T(n)= T(\lfloor n/2 \rfloor) + T(\lfloor 2n/3 \rfloor) + n^2$

$\le c\,(\lfloor n/2 \rfloor)^2 + c\,(\lfloor 2n/3 \rfloor)^2 + n^2$

$< c\,(n/2)^2 + c\,(2n/3)^2 + n^2$

$= n^2\,(c/4 + 4c/9+1)$

ma $n^2\,(c/4 + 4c/9+1) \le c\, n^2$ per $c \ge c/4 + 4c/9+1$

quindi $T(n) \le c\, n^2$ 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: $T(n) = T(n-1) + a$

$T(1) = b$

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

ma $T(n-1) = T(n-2) + a$

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

ma $T(n-2) = T(n-3) + a$

$= T(n-3) + a + a + a$

....

proseguendo in questo modo dopo k iterazioni avremo

$= T(n-k) + \underbrace{a + a + \dots + a}_{k}$

....

le iterazioni si fermano quando si arriva alla condizione iniziale $n-k=1$

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

$T(1) = b$

$= b + (n-1)a$

Esempio: Sia n pari $T(n) = 2\,T(n-2) + 3$

$T(0) = 1$

$T(n) = 2\,T(n-2) + 3$

ma $T(n-2) = 2T(n-4) + 3$

$= 2\,(2\,T(n-4) + 3) + 3$

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

ma $T(n-4) = 2T(n-6) + 3$

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

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

....

proseguendo in questo modo dopo k iterazioni avremo

$= 2^k\,T(n - 2 \cdot k) + 2^{k-1} \cdot 3 + 2^{k-2} \cdot 3 + \dots + 3$

....

le iterazioni si fermano quando si arriva alla condizione iniziale $n-2k=0 \Rightarrow k=n/2$

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

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

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

Quindi $T(n)= 4 \cdot 2^{n/2} - 3$

Esempio: 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: Sia $n=2^k$ $\quad T(n) = 8\,T(n/2) + n$

$T(1) = 2$

$T(n) = 8\,T(n/2) + n$ $\quad$ ma $T(n/2) = 8T(n/2^2) + n/2$

$= 8\,(8T(n/2^2) + n/2\,) + n$

$= 8^2\,T(n/2^2) + 8 \cdot n/2 + n$

$= 8^2\,T(n/2^2) + 4 \cdot n + n$ $\quad$ ma $T(n/2^2) = 8T(n/2^3) + n/2^2$

$= 8^2\,(8T(n/2^3) + n/2^2) + 4 \cdot n + n$

$= 8^3\,T(n/2^3) + 8^2 \cdot n/2^2 + 4 \cdot n + n$

$= 8^3\,T(n/2^3) + 4^2 \cdot n + 4 \cdot n + n$

....

$T(n) = 8^3\,T(n/2^3) + 4^2 \cdot n + 4 \cdot n + n$

....

proseguendo in questo modo dopo k iterazioni avremo

$= 8^k\,T(n/2^k) + 4^{k-1} \cdot n + 4^{k-2} \cdot n + \ldots + n$

$= 8^k\,T(n/2^k) + n\,\Sigma_{i=0,\ldots,k-1}\,4^i$

$= 8^k\,T(n/2^k) + n\,(4^{k-1+1} - 1)/3$

$= 8^k\,T(n/2^k) + n\,(4^k - 1)/3$

$= (2^k)^3\,T(n/2^k) + n\,((2^k)^2 - 1)/3$ $\quad$ ma $T(1)=2$ $\quad$ e $n = 2^k$

$= n^3 \cdot T(1) + n\,(n^2 - 1)/3$

$= n^3 \cdot 2 + n\,(n^2 - 1)/3$

$= (7\,n^3 + n)/3$ $\quad$ Quindi $T(n) = (7\,n^3 + n)/3$

Esempio: $T(n) = T(n-1) + T(n-2)$ $\quad$ (sequenza di Fibonacci)

$T(2) = 1$

$T(1) = 1$

Risolvere questa relazione di ricorrenza con il metodo iterativo è molto complesso.

Proviamo però a limitarla

1. $T(n) = T(n-1) + T(n-2) \le 2\,T(n-1)$

e

2. $T(n) = T(n-1) + T(n-2) \ge 2\,T(n-2)$

Applichiamo il metodo di iterazione alla 1.

cioè risolviamo

$T(n) \le 2\,T(n-1)$

$T(n) \le 2\,T(n-1)$

$\le 2 \cdot 2\,T(n-2)$

$\le 2 \cdot 2 \cdot 2T(n-3) = 2^3T(n-3)$

.....

$\le 2^kT(n-k)$ $\quad$ ci fermeremo quando $n-k=1 \Rightarrow k=n-1$

.....

$\le 2^{n-1}T(1) = 2^{n-1}$ $\quad$ Quindi $T(n) \le 2^{n-1}$

Applichiamo il metodo di iterazione alla 2.

cioè risolviamo

$T(n) \ge 2\,T(n-2)$

$T(n) \ge 2\,T(n-2)$

$\ge 2 \cdot 2\,T(n-2-2)$

$\ge 2 \cdot 2 \cdot 2\,T(n-2-2-2)$

$= 2^3\,T(n-3 \cdot 2)$ $\quad$ proseguendo in questo modo dopo k iterazioni avremo

.....

$\ge 2^k\,T(n-k \cdot 2)$ $\quad$ ci fermeremo quando $n-k \cdot 2=2 \Rightarrow k=(n-2)/2$

.....

$\ge 2^{(n-2)/2}\,T(2) = 2^{(n-2)/2}$ $\quad$ Quindi $T(n) \ge 2^{(n-2)/2}$

Esercizi Risolvere la seguente relazione di ricorrenza utilizzando il metodo iterativo

1. Sia n dispari,

   $T(n) = 2\,T(n-2) + 3$

   $T(1) = 1$

2. $T(n) = n + T(n-1)$

   $T(1) = 1$

3. Sia $n=3^k$

   $T(n) = 9\,T(n/3) + n$

   $T(1) = 1$