LOGICA

Lezione 1: Introduzione

Laura Nenzi

DIA – Università degli Studi di Trieste

Informazioni sul corso

- Le registrazioni del corso saranno disponibili online dopo ogni lezione
- Le slide e il materiale del corso saranno anche loro disponibili online su moodle
- Libri:
  - "Logica a Informatica" A. Asperti & A. Ciabattoni
  - The Open Logic Text
  - Indicazioni di capitoli di libri liberamente disponibili

Modalità d’esame

- L’esame consiste di due parti:
  - Una prova scritta
  - Un esame orale
- È necessario il superamento della prova scritta per accedere all’orale

Obiettivi del corso

Capire il **linguaggio** e le **tecniche** della logica matematica per utilizzarli nella risoluzione dei problemi informatici.

Obiettivi del corso

- Tradurre in un linguaggio -> Formalizzazione

- Goethe: *“I matematici sono come i francesi: ogni volta che gli si dice qualcosa, la traducono nel loro linguaggio e subito appare diversa.”*

- Studiare sistemi di calcolo per di sviluppare dimostrazioni automatiche

Contenuti del Corso

- Logica Proposizionale
- Sistemi deduttivi per la La logica Proposizionale
- Logica dei Predicati
- Calcolo del primo ordine
- Metodo di risoluzione
- Forse altro se ci rimane tempo ☺

Contenuti della lezione

- Introduzione
- Richiamo di nozioni di base
- Denotazione e Senso

Le vie della logica

- La logica è tradizionalmente studiata in:
  - Linguistica
  - Filosofia
  - Matematica

La via dell’argomentazione

- La via dell’argomentazione
  - logos: parlare da solo, ragionare
  - dialogos: parlare in due, conversare

- Alcune strategie:
  - Riduzione all’assurdo delle posizioni avversarie (Zenone)
  - Argomentazione a favore e contro qualunque posizione (Socrate)

- Ogni parte della struttura del discorso si presta ad abusi retorici.

Esempi di abusi retorici

- Per esempio l'uso improprio di connettivi può portare a conclusioni sbagliate:

- **Disgiunzione:**
  - Può portare a falsi dilemmi
  - Ovvero un insieme di alternative non esaustive
  - Es: "siamo uomini o caporali?" dove l'eliminazione di una possibilità sembra implicare necessariamente l'accettazione dell'altra

Esempi di abusi retorici

- **Negazione:**
  - Ciò che non si sa essere vero viene asserito come falso e viceversa.
  - Es: Il massimalismo che considera permesso tutto ciò che non è espressamente proibito.

- **Quantificatori:**
  - Un errore tipico è quello di confondere uno o alcuni esempi con una proposizione universale
  - Es: “Se qualcuno è diventato ricco, tutti possono diventarlo”

Esempi di abusi retorici

- **Implicazione:**
  - Un errore tipico è quello di collegare due eventi solo perché si presentano in successione temporale.
  - Oppure quando si dimostrano conclusioni più forti o non implicate dalle premesse.
  - Es: “Se piove allora esco con l’ombrello” non implica che se esco con l’ombrello allora sta piovendo!

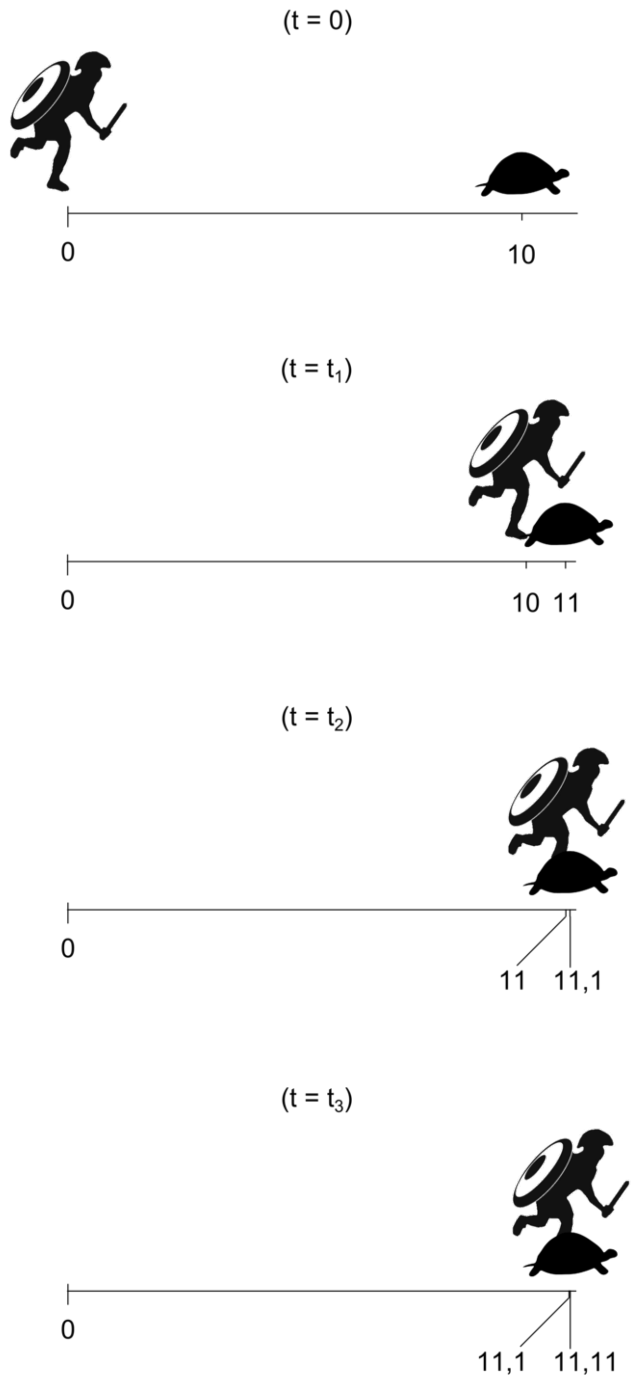
La via del paradosso

- **Paradosso:** dal greco *παρά* (*contro*) e *δόξα* (*opinione*)
- Fra i più famosi ci sono:
  - il paradosso di **Achille e la tartaruga**
  - il paradosso del mentitore: **Il cretese Epimenide**

Achille e la tartaruga

- Paradosso di Zenone
- Achille (A) simbolo di rapidità
- Tartaruga (T) simbolo di lentezza
- A corre 10 volte più veloce di T
- **A concede a T 10m di vantaggio**

- Quando A corre 10m, T corre 1
- Quando A corre 1m, T corre 1dm
- A non raggiunge mai T.



Achille e la tartaruga

- Caratteristiche di questo paradosso:
  - Infinita divisibilità dello spazio
  - Infinito regresso del ragionamento logico
  - Dicotomia = suddivisione infinitesimale

Ragionamento corretto

- Sia t è il tempo necessario ad Achille per raggiungere la tartaruga;
- Velocità di A 10m/s e di T 1m/s.
- Nell’istante in cui A raggiunge T
- abbiamo che:
  - In metri: $10t = 10 + 1t$ (10m di vantaggio)
  - $t=10/9$ (tempo finito!!!)

Cosa genera il paradosso?

- Il paradosso è generato dal fatto che anche la **somma di infiniti numeri** può dare per risultato un **numero finito**!!!

- $t = \frac{10}{9} = 1 + 0{,}1 + 0{,}01 + 0{,}001 + \cdots$

- Si osserva che tale somma infinita è riconducibile a una serie geometrica di ragione strettamente compresa tra -1 e 1, e dunque convergente.

Il cretese Epimenide

- Epimenide è un **cretese** del VI sec. a.C.
- Disse:
  - *“**tutti** i cretesi dicono **sempre** il falso”*
- Ci chiediamo:
  - *Questa frase può essere vera?*
  - *Questa frase può essere falsa?*
- Se la frase non può essere né vera né falsa è un **paradosso**.

La frase è vera?

- **Tutti** i cretesi dicono **sempre** il falso.
- *Supponiamo che sia vera:*
- Epimenide ha detto il vero almeno una volta (ha detto una frase vera).
- La frase “tutti i cretesi dicono sempre il falso” è vera.
- Assurdo: la frase *non può essere vera.*

La frase è falsa?

- **Tutti** i cretesi dicono **sempre** il falso.
- *Supponiamo che sia falsa:*
  - Epimenide sta dicendo il falso.
  - La frase “**tutti** i cretesi dicono **sempre** il falso” è falsa. Ovvero la frase “**qualche** cretese (non necessariamente Epimenide) **qualche** volta **non** dice il falso” è vera.
- La frase è quindi falsa!
- **Non** è un paradosso.

Paradosso di Eubulide

- Eubulide di Mileto (IV sec. a.C.) modifica la frase e arriva ad un vero paradosso.
- Disse: “Io sto mentendo”
- *Supponiamo che sia vera:*
  - Eubulide non sta mentendo.
  - La frase “io sto mentendo” è vera, quindi Eubulide sta mentendo.
- Assurdo: *non è vera.*

Paradosso di Eubulide

- “Io sto mentendo”
- *Supponiamo che sia falsa:*
  - Eubulide sta mentendo.
  - La frase “io sto mentendo” è falsa, quindi Eubulide non sta mentendo.
- Assurdo: *non è falsa.*
- Questo è un **paradosso** perché la frase non è né vera né falsa**!**

Paradosso di Eubulide

- Caratteristica di questo paradosso:
  - Autoriferimento (o riferimento incrociato)
- Come evitare questo tipo di paradosso:
  - Le frasi contraddittorie non hanno senso.
  - Diversi livelli di linguaggio. Le frasi che parlano di verità e falsità non possono riferirsi a se stesse (sono di un livello superiore).
  - Terzo valore di verità: indefinito.

La via della dimostrazione

- Antichi Greci già distinguevano tra
  - enunciati: affermazioni pure e semplici
  - teoremi: affermazioni dotate di una dimostrazione

- La necessità pratica di distinguere tra enunciati corretti ed errati ha portato alla formalizzazione delle dimostrazioni.

Indipendenza dal senso

- determinati schemi di ragionamento sono in una certa misura indipendenti dal senso (contenuto informative)che si attribuisce alle singole parti del discorso:
  - Ogni uomo è mortale, Socrate è un uomo, dunque Socrate è mortale”.

- Se proprietà P è soddisfatta da tutti gli elementi di un determinato insieme A, allora, per ogni $a \in A$, P è necessariamente soddisfatta da a.

Astrazione dal contenuto

- Astrazione dal contenuto, considerando solo la loro forma o struttura
- utilizzare un linguaggio di natura algebrica e formale per descrivere:
  - le sentenze che sono oggetto della logica
  - le sue regole di inferenza
- Interpretazione senza ambiguità dalle persone con cui si vuole comunicare

Esistono tante logiche

- Non esiste un linguaggio logico universal!!!
- E.g. logica classica, intuizionista, affine, lineare, modale, temporale, multi-valore, fuzzy, non-monotona, ecc.,
- Noi vedremo logica classica: proposizionale e dei predicati

Applicazioni

- modellizzazione algebrica di macchine astratte
- verifica della correttezza dei programmi
- progettazione (synthesis) e verifica di circuiti digitali
- implementazione di protocolli di comunicazione
- dimostrazioni automatiche

LEAN theorem prover

https://leanprover.github.io/

Scholze posted on Buzzard's blog that the main part of the experiment had succeeded. "I find it absolutely insane that interactive proof assistants are now at the level that, within a very reasonable time span, they can formally verify difficult original research," Scholze wrote.

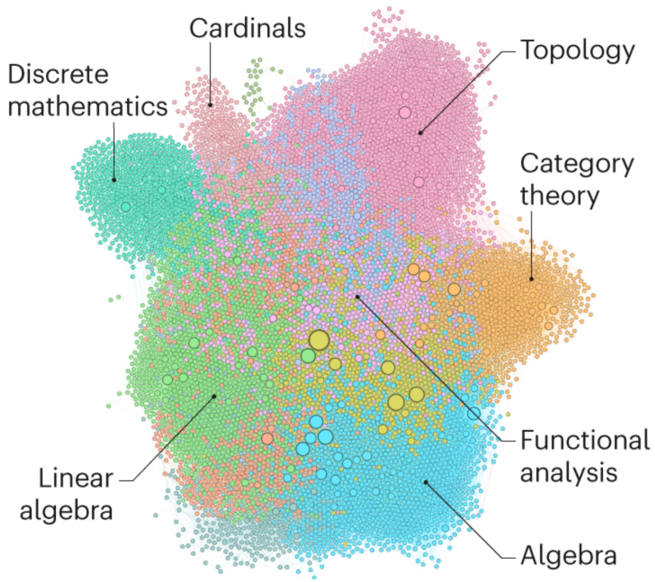
NEWS | 18 June 2021

Mathematicians welcome computer-assisted proof in 'grand unification' theory

Proof-assistant software handles an abstract concept at the cutting edge of research, revealing a bigger role for software in mathematics.

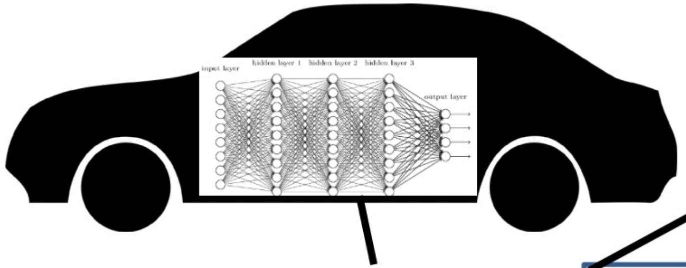
Davide Castelvecchi

https://www.nature.com/articles/d41586-021-01627-2



L'output è un complex network

Verified AI



System **S**

Environment **E**

Specification **φ**

Does S || E satisfy φ?

YES [+ proof]

NO [+ counterexample]

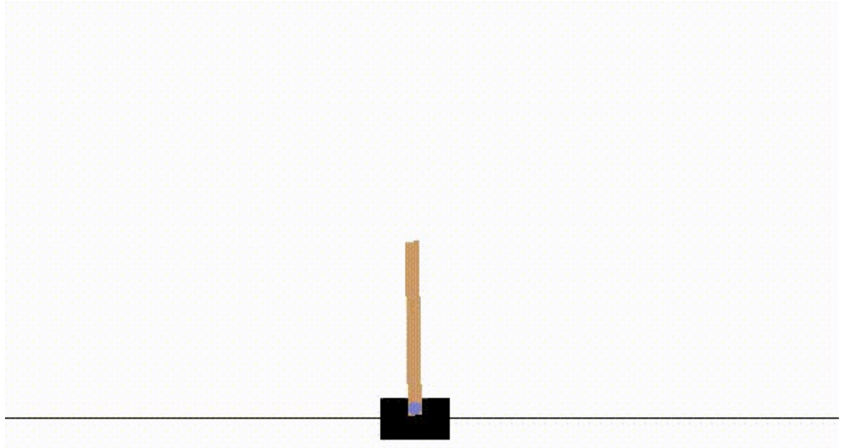
Need to Search Very High-Dimensional Input and State Spaces

Design Correct-by-Construction?

S. A. Seshia, D. Sadigh, S. S. Sastry. Towards Verified Artificial Intelligence. July 2016, here

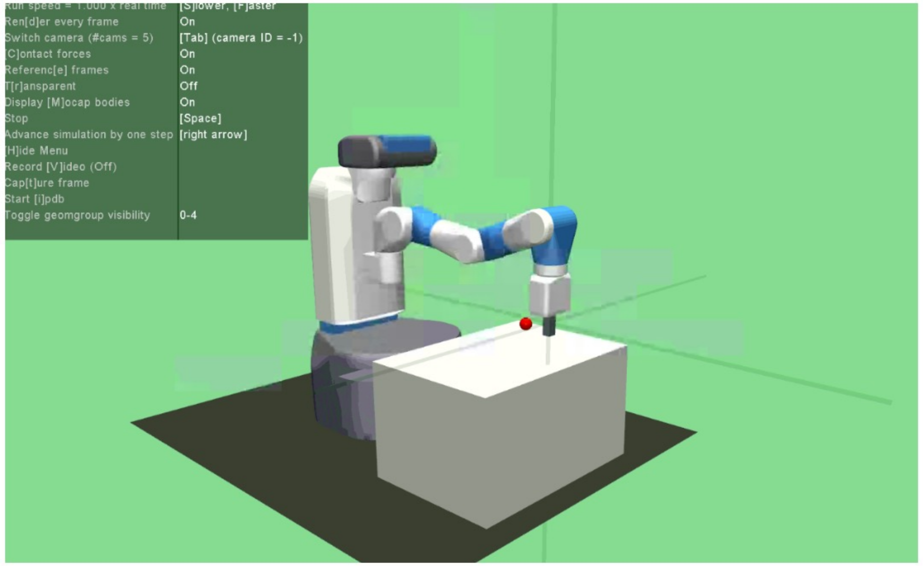
Reinforcement Learning e Logiche Temporali

Cartpole



$$\varphi := G(|x| < 0.1 \wedge |\theta| < 12^{\circ})$$

Bracci Robotici



$$\varphi := F(|x_g - x| < 0.1 \wedge |y_g - y| < 0.1 \wedge |z_g - z| < 0.1)$$

P. Kapoor, A. Balakrishnan, J. V. Deshmukh, Model-based Reinforcement Learning from Signal Temporal Logic Specifications, here

“La Logica potrebbe e dovrebbe assumere, nei confronti dell’Informatica, lo stesso ruolo svolto dalla Matematica, e in particolare dall’Analisi, nei confronti della Fisica ”

Logiche e Informatica

Eentrambe si occupano di problemi di *formalizzazione*, *elaborazione* e *comunicazione* della conoscenza.

- L'enfasi sulla natura umana o meccanica dell'agente di calcolo è in realtà del tutto marginale

- Punto di incontro: la necessità di utilizzare un linguaggio formale.

Logiche e Informatica

- Tutti sappiamo cosa sia un programma, visto come mera composizione sintattica delle sue istruzioni elementari.

- Tuttavia, la logica del processo complessivo, il suo significato, e dunque il suo comportamento ci è ancora largamente sconosciuto.

Richiamo di nozioni di base

- Insiemi
- Operazioni tra insiemi
- Funzioni

Gli Insiemi

- Un **insieme** è una collezione di oggetti detti elementi dell'insieme.

- Principio di estensionalità:
  Gli insiemi sono completamente caratterizzati dai loro elementi:
  due insiemi sono uguali se contengono gli stessi elementi

L'universo

- Gli insiemi che consideriamo conterranno solo elementi di tale universo U.
- Esempi di universo:
  - Naturali $\{0, 1, 2, \ldots.\}$
  - Interi $\{\ldots -2, -1, 0,1,2, \ldots.\}$
  - Reali Booleani $B = \{0, 1\}$
  - $B^n = \{0, 1\}^n =$ {numeri di n cifre booleane}.
    Es. $n = 2, \{0, 1\}^2 = \{00, 01, 10, 11\}$

Rappresentazione di insiemi

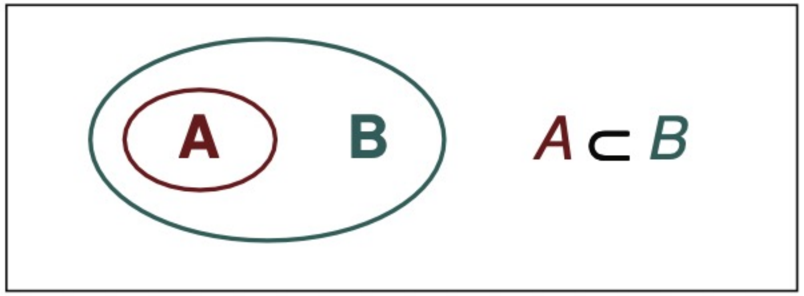
- Consideriamol’universodeinaturali. L'insieme che contiene gli elementi $1, 7,$ e 4 può essere denotato con $\{1, 7, 4\}$.
- L'ordine non conta.
- Non contano le ripetizioni.
- Es: $\{1,7,4\} = \{1,4,7\} = \{1,7,4,7\}$.

Appartenenza

- l simbolo di appartenenza: ∈
- Sia a è un elemento e A un insieme, allora $a \ \in \ A$ significa che a **appartiene** ad A.
- Scriveremo $a \notin A$ per dire che a non appartiene ad A.
- **L'insieme vuoto** $\emptyset = \{\}$ è un insieme che non contiene alcun elemento.

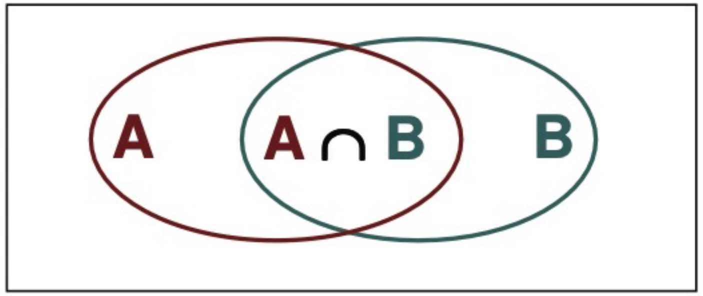
Inclusione

- Un insieme A è un **sottoinsieme** di B $(A \subseteq B)$ se ogni elemento di A appartiene anche a B.
- Un insieme A è un **sottoinsieme proprio** di B $(A \subset B)$ se $A \subseteq B$ ma A è diverso da B $(A =/ B)$.
- Se $A \subseteq B$ e $B \subseteq A$ allora $A = B$



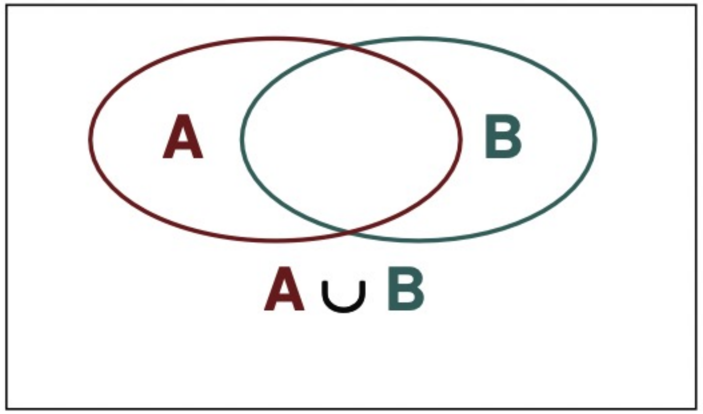
Intersezione

- L'insieme degli elementi che appartengono sia a A che a B si chiama **intersezione** di A e B $(A \cap B)$.
- Due insiemi tali che $A \cap B = \emptyset$ si dicono **disgiunti**.



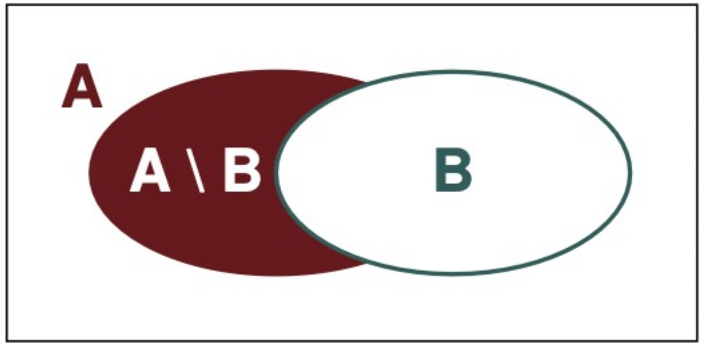
Unione

- L'**unione** di A e B $(A \cup B)$ è l'insieme degli elementi che appartengono ad almeno uno dei due insiemi A e B



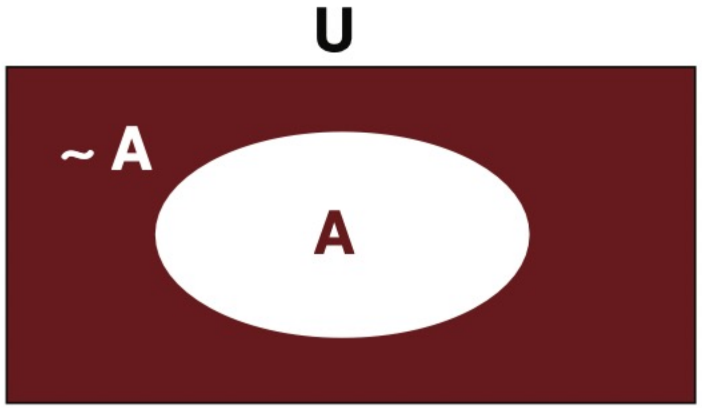
Differenza

- la **differenza** tra A e B $(A \setminus B)$ è l'insieme degli elementi che appartengono ad A ma non a B.



Il complemento

- Il **complemento** di un insieme A $(\neg A)$ è la differenza tra l'universo e l'insieme A
- Non esiste una notazione standard per il complemento di un insieme. Le notazioni più usate sono $\sim A, \neg A, A', Ac$.



Leggi di associatività

- Leggi di associatività:
  - $(A \cup B) \cup C = A \cup (B \cup C)$
  - $(A \cap B) \cap C = A \cap (B \cap C)$
- Grazie a queste identità possiamo omettere alcune parentesi.
- Ad esempio possiamo scrivere:
  - $A \cup B \cup C$

Altre proprietà

- Idempotenza
  - $(A \cup A) = A$
  - $(A \cap A) = A$
- Commutatività
  - $(A \cup B) = (B \cup A)$
  - $(A \cap B) = (B \cap A)$
- Distributività
  - $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
  - $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Le coppie

- $< a, b >$ è una **coppia ordinata** il cui primo elemento è a e il cui secondo elemento è b.
- Osservazioni:
  - $< a, b > = < c, d >$ solo se $a = c$ e $b = d$.
  - Se $a \neq b$ allora $< a, b > \neq < b, a >$
- Un insieme di due elementi $\{a, b\}$ è anche chiamato **coppia non ordinata**.

Tuple

- La nozione di tupla generalizza quella di coppia.
- Una **n-tupla** (ordinata) di un insieme A è una sequenza $< a_1, \ldots , a_n >$ di elementi di A.
- Es: una 4-tupla di numeri naturali: $< 10, 3, 10, 5 >$

Prodotti cartesiani

- Il **prodotto cartesiano** degli insiemi A e B è l'insieme di coppie il cui primo elemento appartiene ad A ed il secondo appartiene a B:
- $A{\times}B = \{< a, b > |a \in A\ e\ b \in B\}$
- Es {0,1} × {1,2} = {<0,1>,<0,2>,<1,1>,<1,2>}
- In generale, il prodotto cartesiano degli insiemi $A_1, \ldots\ , A_n$ è
- $A_1 \times\ \ldots \times A_n =\ \{< a_1, \ldots\ , a_n > |a_1\ \in\ A_1, \ldots, .\ a_n\ \in\ A_n\}$

Potenze cartesiane

- Il **quadrato cartesiano** dell'insieme A è:
  - $A^2 = A \times A = \{< a, b > | a \in A \; e \; b \in A\}$
- La **potenza cartesiana** n-esima dell'insieme A è l'insieme delle n-tuple di elementi di A :
  - $A^n = A \times \ldots \times A == \{< a_1, \ldots, a_n > | a_1 \in A, \ldots, a_n \in A\}$

Funzioni parziali

- Siano A e B due insiemi, una **funzione parziale** $F\colon A \to B$ è un insieme di coppie $< a, b >$ (con $a \in A$ e $b \in B$) in cui ogni elemento di A è in coppia con al più un elemento di B.
- Es. $A = \{0,1,2,4\}, B = \{0,3,6\}$
- F: $A \to B = \{< 0,0 >, < 1,0 >, < 4,6 >\}$
- ovvero $F(0) = 0, F(1) = 0, F(2) = ?, F(4) = 6$

Funzioni totali

- Siano A e B due insiemi, una **funzione totale** $F\colon A \rightarrow B$ è una funzione parziale che associa **ad ogni** elemento di A un elemento di B.
- Es. $A = \{a, b, c, d\}, B = \{0,3,6\}$
- $F = \{< a, 0 >, < b, 0 >, < c, 6 >, < d, 6 >\}$
- ovvero $F(a) = 0, F(b) = 0, F(c) = 6, F(d) = 6$

Dominio e immagine

- L'insieme degli x dove F è definita si chiama **dominio di definizione** di F $(Dom\ (F))$.
- L'insieme degli y tali che $< x, y > \in\ F$, per ogni $x\ \in\ Dom(F)$, si chiama **immagine** di F $(Im(F))$.
- Esempio $F\ :\ \{a, b, c, d\} \rightarrow\ \{0,2,6\}$

$$\begin{aligned} F\ &=\ \{< a, 0 >, < c, 6 >, < d, 6 >\} \\ Dom(F)\ &=\ \{a, c, d\} \\ Im(F)\ &=\ \{0,6\}. \end{aligned}$$

- Se il dominio di $F: A \rightarrow B$ è A allora la funzione è totale.

Funzioni suriettive

- Sia $F: A \to B$, se $Im(F) = B$ allora la funzione di dice **suriettiva**.
- Esempio $F : \{a, b, c, d\} \to \{0,2,6\}$
- $F = \{< a, 0 >, < c, 6 >, < d, 6 >\}$
$$Im(F) = \{0,6\} \neq \{0,2,6\}: \boldsymbol{non} \text{ è } suriettiva.$$
- $Esempio\ G : \{a, b, c, d\} \to \{0,2,6\}$
$$G = \{< a, 0 >, < c, 2 >, < d, 6 >\}$$
$$Im(G) = \{0,2,6\}, \text{è } suriettiva!$$

Funzioni iniettive

- Una funzione F si dice **iniettiva** se per ogni $y \in Im(F)$ esiste al più un x tale che $< x, y > \in F$.
- *Esempio* $F : \{a, b, c, d\} \rightarrow \{0,2,6\}$

  $F = \{< a, 0 >, < c, 6 >, < d, 6 >\}$

  $Im(F) = \{0,6\}, sia < c, 6 >$ che $< d, 6 >$ sono in F

  F **non** è iniettiva.
- *Esempio* $G : \{a, b, c, d\} \rightarrow \{0,2,6\}$

  $G = \{< a, 0 >, < d, 6 >\}$

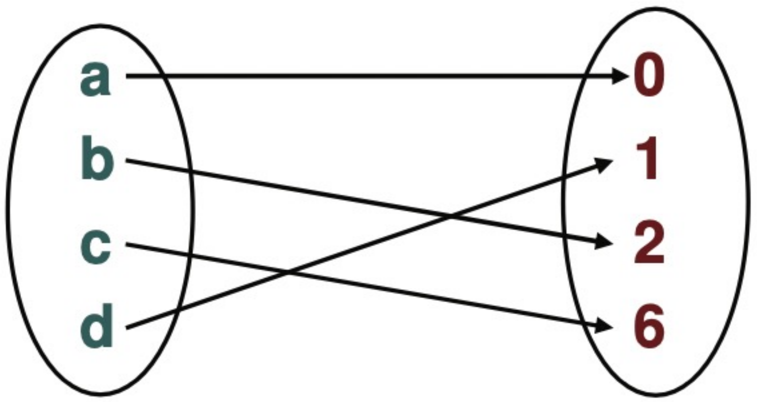
  $Im(G) = \{0,6\}$, è iniettiva!

Funzioni biiettive

- Una funzione totale, suriettiva ed iniettiva è detta **biiettiva**.
- *Esempio* $F : \{a, b, c, d\} \rightarrow \{0,1,2,6\}$

  $F = \{< a, 0 >, < b, 2 >, < c, 6 >, < d, 1 >\}$

  F è biiettiva.



Inversa

- Sia $F\!:\ A\ \rightarrow\ B$ una funzione biiettiva, la **funzione inversa** di F (F^{-1}) è la funzione F^(-1) : B → A tale che
$< a, b > \in\ F\ se\ solo\ se < b, a > \in\ F^{-1}$

- Esempio: F : $\{a, b, c, d\} \rightarrow\ \{0,1,2,6\}$
F = $\{< a, 0 >, < b, 2 >, < c, 6 >, < d, 1 >\}$
$\{< 0, a >, < 1, d >, < 2, b >, < 6, c >\}$

Denotazione e Senso

Denotazione

- Un nome è un’espressione linguistica che denota una qualche entità.
- Esempio:
  - Quattro
  - Il quadrato di due
  - Il predecessor di cinque
  - Tre più uno

Sono modi diversi per denotare lo stesso oggetto: il numero 4

Senso

- Il senso di un nome è quanto effettivamente esprime ovvero la sua connotazione.
- Esempio:
  - Quattro
  - Il quadrato di due
  - Il predecessor di cinque
  - Tre più uno
- Questi nomi hanno tutti un senso diverso anche se si riferiscono allo stesso oggetto
- Esempio: algoritmi di Ordinamento

Sostituzioni

- La denotazione è invariante per sostituzione
- Esempio:
  - Il quadrato di quattro
  - Il quadrato di (tre più uno)
- Denotano sempre lo stesso numero, ovvero sedici

Sostituzioni

- Il senso non è invariante per sostituzione
- Esempio:
  - Quattro è il quadrato di due
  - Quattro è quattro
- Le due frasi non hanno lo stesso senso.

Tipi di enunciati

- Tre tipi di enunciati (o sentenze):
  - **Interrogativi**: Piove? X=5?
  - **Imperativi**: Fate i compiti! X:=5
  - **Dichiarativi**: Oggi piove. X=5

- Gli enunciati dichiarativi sono detti anche **asserzioni**
- Noi parleremo solo di enunciati dichiarativi e li chiameremo semplicemente enunciati.

Principi

- **Principio di bivalenza**: Ogni enunciato è sempre vero o falso.

- **Principio di estensionalità**: Il valore di verità degli enunciati composti dipende solamente dal valore di verità degli enunciati che li compongono (*invarianza per sostituzione*)

Enunciati atomici

- Un enunciato è **semplice** (o **atomico**) se non contiene nessun altro enunciato.
- Esempi di enunciati atomici:
  - Paolo corre
  - Laura ha i capelli rossi
  - X = 3

Enunciati composti

- Un enunciato è **composto** se contiene altri enunciati (è possibile scomporlo in enunciati più semplici).
- Esempi di enunciati composti:
  - Piove e c'è vento
  - Se c'è il sole allora esco
  - Carla ha gli occhi neri o Carla ha i capelli neri
  - Non piove

Niels Bohr: "you are not thinking you are just being logical"