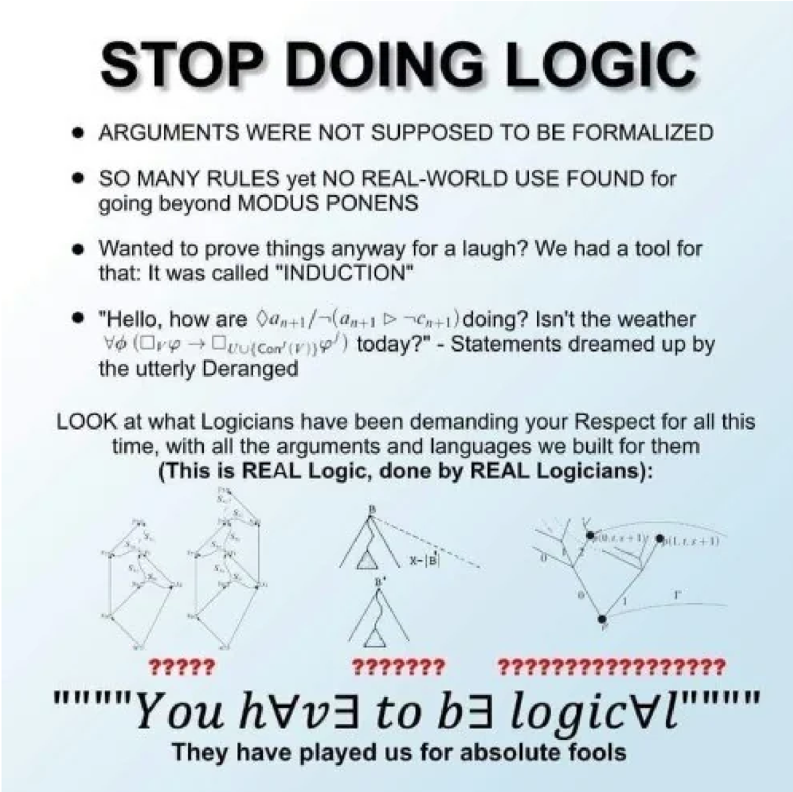
Logica



La logica è la disciplina che studia le condizioni di correttezza del ragionamento

- Sillogismo, dal greco συλλογισμός (σύν - λογισμός, unione di ragionamenti, concatenazione), Questo tipo di ragionamento fu formulato da Aristotele, che a partire da un predicato, se ne formulano altri veri sulla base del primo

Esempio di Sillogismo valido

- Tutti gli uomini sono mortali
- Socrate è un uomo
- Socrate è mortale

Socrate è un uomo e per conseguenza del primo predicato egli è anche mortale

Esempio di Sillogismo non valido

- Tutti gli dei sono immortali
- Gli uomini non sono dei
- Gli uomini sono mortali

Gli uomini non sono dei ma per nessuna conseguenza del primo predicato possiamo dire anche che sono mortali di sicuro

Usi della Logica Matematica

- Formalizzazione di requisiti
- Dimostrazione di proprietà di programmi
- Programmazione dichiarativa
- Programmazione funzionale e teoria dei tipi
- Rappresentazione della conoscenza

- Strumenti di analisi e verifica dei sistemi

Verso il calcolo proposizionale

- I valori di verità o booleani: $vero,\ falso\ -\ true,\ false$
  Anche
  $T, F \quad t, f \quad 1, 0$
- Le proposizioni sono frasi in linguaggio naturale che soddisfano:
  1. Principio del terzo escluso: vera o falsa
  2. Principio di non contradditorietà: non entrambi
- Le formule proposizionali
  - P, Q, R
  - $\neg P \quad P \wedge Q \quad P \vee Q \quad P \Rightarrow Q \quad P \Leftarrow Q \quad P \Leftrightarrow Q$

Riconoscere le proposizioni

Queste sono proporizioni?

- Firenze è la capitale d'Italia. E' una proposizione, falsa
- Forse Firenze è la capitale d'Italia. Non è una proposizione
- Firenze è la capitale d'Italia? Non è una proposizione
- Firenze è stata la capitale d'Italia. E' una proposizione, vera

La sintassi delle formule proposizionali

$X = \{A, B, C, \dots\}$ insieme di SIMBOLI PROPOSIZIONALI

$$\text{Linguaggio Proposizionale}$$

$$\begin{array}{l}
\langle Prop \rangle \rightsquigarrow \langle Atom \rangle \mid \neg \langle Atom \rangle \mid \langle Prop \rangle \langle OpB \rangle \langle Prop \rangle \\
\langle Angle \rangle \rightsquigarrow T \mid F \mid \langle X \rangle \mid (\langle Prop \rangle) \\
\langle OpB \rangle \rightsquigarrow \wedge \mid \vee \mid \Rightarrow \mid \Leftarrow \mid \Leftrightarrow \\
\langle X \rangle \rightsquigarrow A \mid B \mid C \mid \dots
\end{array}$$

- Esempi di formule proposizionali

$$A \wedge (B \vee \neg C) \quad ((A \wedge B \vee F) \Rightarrow \neg A \vee (C \wedge T))$$
$$(A \Rightarrow B) \wedge \neg (B \wedge \neg C) \Rightarrow (A \Rightarrow C)$$

- Esempi di stringhe che non sono formule proposizionali

$$A \wedge \vee B \quad (A \neg C) \quad A \neg$$

Connettivo	Forma simbolica	Operazione corrispondente
not	$\neg P$	$negazione$
$and,\ e$	$P \wedge Q$	$congiunzione$
$or,\ o$	$P \vee Q$	$disgiunzione$
$se\ P\ allora\ Q$	$P \Rightarrow Q$	$implicazione$
$P\ se\ Q$	$P \Leftarrow Q$	$conseguenza$
$P\ se\ e\ solo\ se\ Q$	$P \Leftrightarrow Q$	$doppia\ implicazione$

Formalizziamo proposizioni strutturate

$$\neg P \quad P \wedge Q \quad P \vee Q \quad P \Rightarrow Q \quad P \Leftarrow Q \quad P \Leftrightarrow Q$$

- Piove e fa freddo

  $P \equiv piove \quad R \equiv fa\ freddo \rightarrow P \wedge R$

- Fa freddo, ma non piove

  $R \wedge \neg P$

- Se ci sono nuvole e non c'è vento, allora piove

  $N \equiv \text{"ci sono nuvole"}, V \equiv \text{"c'è vento"} \quad (N \wedge \neg V) \Rightarrow P$

- Nevica, ma non fa freddo se ci si copre

  $Ne \equiv \text{"nevica"}, C \equiv \text{"ci si copre"} \quad Ne \wedge (\neg R \Leftarrow C)$

- Se ci si copre, allora fa freddo o nevica

  $C \Rightarrow (R \vee Ne)$

- Piove solo se ci sono nuvole e non c'è vento

  $\neg(N \wedge \neg V) \Rightarrow \neg P$

Connettivi logici come funzioni su booleani

$\neg : Bool \rightarrow Bool$

$\wedge, \vee, \Rightarrow, \Leftarrow, \Leftrightarrow: Bool \times Bool \rightarrow Bool$

x	$\neg x$
f	*t*
t	*f*

x	y	$x \wedge y$	$x \vee y$	$x \Rightarrow y$	$x \Leftarrow y$	$x \Leftrightarrow y$
f	*f*	*f*	*f*	*t*	*t*	*t*
f	*t*	*f*	*t*	*t*	*f*	*f*
t	*f*	*f*	*t*	*f*	*t*	*f*
t	*t*	*t*	*t*	*t*	*t*	*t*

Semantica del Calcolo Proposizionale

Data una interpetazione $\mathcal{I} : X \to \{f, t\}$, definiamo indutivamente la semantica

$$[\![\_]\!]_{\mathcal{I}} : Prop \to \{f, t\}$$

1. $[\![T]\!]_{\mathcal{I}} = t$ e $[\![F]\!]_{\mathcal{I}} = f$
2. $[\![A]\!]_{\mathcal{I}} = \mathcal{I}(A),\ \forall A \in X$
3. $[\![P]\!]_{\mathcal{I}} = ([\![P]\!]_{\mathcal{I}}),\ \forall P \in Prop$
4. $[\![\neg Q]\!]_{\mathcal{I}} = \neg [\![Q]\!]_{\mathcal{I}},\ \forall$ formula atomica Q
5. $[\![P\ op\ Q]\!]_{\mathcal{I}} = [\![P]\!]_{\mathcal{I}}\ op\ [\![Q]\!]_{\mathcal{I}}\ \forall$ connettivo $op \in \{\wedge, \vee, \Rightarrow, \Leftarrow, \Leftrightarrow\} \wedge \forall P, Q \in Prop$

Esempio di valutazione

$\mathcal{I} = \{A \mapsto t, B \mapsto f, C \mapsto f, \ldots\}$

$$[\![(A \wedge B) \vee \neg C]\!]_{\mathcal{I}} \begin{array}{l} = [\![(A \wedge B)]\!]_{\mathcal{I}} \vee [\![\neg C]\!]_{\mathcal{I}} \\ = ([\![A]\!]_{\mathcal{I}} \wedge [\![B]\!]_{\mathcal{I}}) \vee \neg [\![\neg C]\!]_{\mathcal{I}} \\ = (t \wedge f) \vee \neg f \\ = f \vee t \\ = t \end{array}$$

Modelli, equivalenza e conseguenza logica

Una interpretazione $\mathcal{I}$ è un modelli di P se $[\![P]\!]_{\mathcal{I}} = t$

$$\mathcal{I} \vDash P \qquad (\mathcal{I} \text{ è modello di } P)$$

Due formule proposizionali P e Q sono logicamente equivalenti se hanno gli stessi modelli

$$P \equiv Q \qquad (P \text{ e } Q \text{ sono logicamente equivalenti})$$

P è Conseguenza Logica di un insieme di formule Γ se ogni modello di Γ è anche modello di P

$$\Gamma \vDash P \qquad (P \text{ è conseguenza logica di } Q)$$

Tavole della verità

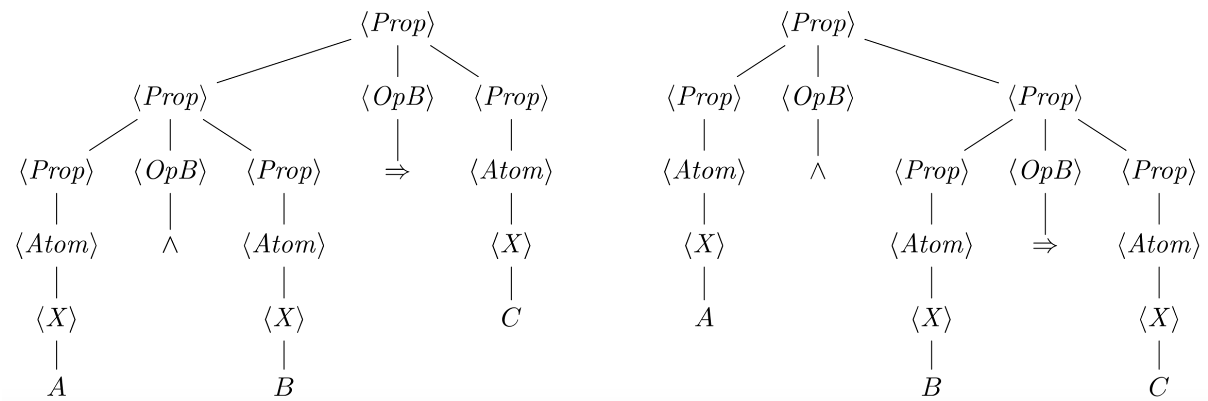
Valutiamo di nuovo la formula $(A \wedge B) \vee \neg C$

nell'interpretazione $\mathcal{I} = \{A \mapsto t, B \mapsto f, C \mapsto f, \ldots\}$

A	B	C	$((A$	$\wedge$	$B)$	$\vee$	$\neg$	$C)$
f	f	f	f	f	f	**t**	t	f
f	f	t	f	f	f	**f**	f	t
f	t	f	f	f	t	**t**	t	f
f	t	t	f	f	t	**f**	f	t
t	f	f	t	f	f	**t**	t	f
t	f	t	t	f	f	**f**	f	t
t	t	f	t	t	t	**t**	t	f
t	t	t	t	t	t	**t**	f	t

Ambiguità

Esistono due alberi di derivazione distinti per $A \wedge B \Rightarrow C$



I due alberi danno risultati diversi

- $(A \wedge B) \Rightarrow C$
- $A \wedge (B \Rightarrow C)$

Gestione delle ambiguità

Per la gestione delle ambiguità in primis si stabiliscono delle regole di precedenza tra i connettivi

connettivo	*livello di precedenza*
$\Leftrightarrow$	*0*
$\Rightarrow, \Leftarrow$	*1*
$\wedge, \vee$	*2*
$\neg$	*3*

$A \wedge B \Rightarrow C$ si legge $[A \wedge B] \Rightarrow C$

$A \wedge B \Rightarrow \neg C \vee D \Leftrightarrow C \wedge \neg A \Leftarrow B \vee C$
si legge

$$[[A \wedge B] \Rightarrow [\neg C \vee D]] \Leftrightarrow [[C \wedge \neg A] \Leftarrow [B \vee C]]$$

Questo non basta però, possono esserci due connettivi con stessa precedenza adiacenti

- $A \wedge B \wedge C \quad A \vee B \vee C$, è Ok, solo ambiguità sintattica, il risultato è lo stesso
- $A \wedge B \vee C$, No, con $\{A = f, C = t\} \rightarrow [A \wedge B] \vee C = t \mid A \wedge [B \vee C] = f$
- $A \Rightarrow B \Rightarrow C$, No, con $\{A = f, B = f, C = f\}$

$\to (A \Rightarrow B) \Rightarrow C = f \mid A \Rightarrow (B \Rightarrow C) = t$

Tautologie, contraddizioni e formule soddisfacibili

Una tautologia (dal greco ταυτολογια, ripetizione) è una formula proposizionale che è vera in ogni interpretazione

- Ogni interpretazione è un modello di una tautologia
- Una tautologia è una formula proposizionale che è sempre vera

$$\models P \qquad (P \text{ è una tautologia})$$

Una contraddizione è una formula proposizionale che è falsa in ogni interpretazione ($Q \text{ è una contraddizione} \Rightarrow \neg Q \text{ è una tautologia})$

Una formula proposizionale è soddisfacibile se esiste almeno una interpretazione in cui è vera

	in tutte le interpretazioni	*in almeno una interpretazione*
Vera	TAUTOLOGIA	SODDISFACIBILE
Falsa	CONTRADDIZIONE	NON TAUTOLOGICA

Come si vede se una formula è o non è soddisfacibile, una contraddizione o una tautologia

Si possono usare tavole della verità, possibile, ma molto costoso

- Tautologia o contraddizione: tutte le righe vere o false
- Soddisfacibile o non tautologica: almeno una riga vera o falsa

Vediamo un modo più diretto per mostrare che questa non è una tautologia

$$\not\models (((A \Rightarrow B) \land \neg A) \Rightarrow B)$$
$$\mathcal{I} = \{a \mapsto f, b \mapsto f\}$$

- B deve essere f
- $\neg A$ deve essere t
- $A \Rightarrow \neg B$ deve essere t
- Controlliamo $f \Rightarrow \neg f = t$

Dimostrazione per sostituzione di tautologie

Molti problemi del calcolo proposizionale si riducono a dimostrare che una formula è tautologica

Consideriamo formule del tipo $P \Leftrightarrow Q$ e le dimostriamo per sostituzione

Introduciamo delle leggi $\rightarrow$ $\text{commutatività}: P \vee Q \Leftrightarrow Q \vee P$

- Dimostriamo $P \Leftrightarrow Q$ con una sequenza di doppie implicazioni come

$$P = R_1 \Leftrightarrow R_2 \Leftrightarrow \cdots \Leftrightarrow R_n = Q$$

Ogni passo è giustificato da una legge

$$((A \wedge B) \vee C \Rightarrow D) \quad \Leftrightarrow \quad (C \vee (A \wedge B) \Rightarrow D) \qquad\qquad (\text{commutatività})$$

Anatomia di un passo di dimostrazione: Rimpiazzamento

P, Q, R formule proposizionali

$P[^Q/_R]$ è la formula ottenuta da P rimpiazzando una specifica occorrenza di R con Q

$$(A \wedge B \Rightarrow (C \Rightarrow D))[^{\neg C \vee D}/_{C \Rightarrow D}] := (A \wedge B \Rightarrow (\neg C \vee D))$$

Principio di Sostituzione

$$\text{Principio di Sostituzione}$$

$$\frac{Q \Leftrightarrow R}{P \Leftrightarrow P[^R/_Q]}[\mathbf{PDS}]$$

- E' una regola di inferenza
- Si può leggere: "se $Q \Leftrightarrow R$ è una tautologia allora anche $P \Leftrightarrow P[^R/_Q]$ è una tautologia"

Leggi

Ogni legge deve essere una tautologia

In realtà rappresenta una infinità di tautologie ottenute sostituendo i simboli proposizionali con arbitrarie formule, ex. $(A \wedge B) \vee C \Leftrightarrow C \vee (A \wedge B)$

Ogni passo è una istanza del Principio di Sostituzione

$$\begin{aligned} P &\mapsto ((A \wedge B) \vee C \Rightarrow D) \\ Q &\mapsto (A \wedge B) \vee C \\ R &\mapsto C \vee (A \wedge B) \end{aligned}$$

$$\frac{(A \wedge B) \vee C \Leftrightarrow C \vee (A \wedge B)}{((A \wedge B) \vee C \Rightarrow D) \Leftrightarrow (C \vee (A \wedge B) \Rightarrow D)[^{C \vee (A \wedge B)}/_{(A \wedge B) \vee C}]}$$

$$((A \wedge B) \vee C \Rightarrow D) \Leftrightarrow (C \vee (A \wedge B) \Rightarrow D) \qquad\qquad (\text{commutatività})$$

unità	$P \vee \mathsf{F} \Leftrightarrow P$	$P \wedge \mathsf{T} \Leftrightarrow P$
assorbimento	$P \vee \mathsf{T} \Leftrightarrow \mathsf{T}$	$P \wedge \mathsf{F} \Leftrightarrow \mathsf{F}$
idempotenza	$P \vee P \Leftrightarrow P$	$P \wedge P \Leftrightarrow P$
commutatività	$P \vee Q \Leftrightarrow Q \vee P$	$P \wedge Q \Leftrightarrow Q \wedge P$
associatività	$P \vee (Q \vee R) \Leftrightarrow (P \vee Q) \vee R$	$P \wedge (Q \wedge R) \Leftrightarrow (P \wedge Q) \wedge R$
distributività	$P \vee (Q \wedge R) \Leftrightarrow (P \vee Q) \wedge (P \vee R)$	$P \wedge (Q \vee R) \Leftrightarrow (P \wedge Q) \vee (P \wedge R)$

Tabella 9.1: Leggi per disgiunzione e congiunzione

T : F	$\neg \mathsf{T} \Leftrightarrow \mathsf{F}$	
doppia negazione	$\neg (\neg P) \Leftrightarrow P$	
terzo escluso	$P \vee \neg P \Leftrightarrow \mathsf{T}$	
contraddizione	$P \wedge \neg P \Leftrightarrow \mathsf{F}$	
De Morgan	$\neg(P \vee Q) \Leftrightarrow \neg P \wedge \neg Q$	$\neg(P \wedge Q) \Leftrightarrow \neg P \vee \neg Q$

Tabella 9.2: Leggi per negazione

riflessività	$P \Leftrightarrow P$
simmetria	$(P \Leftrightarrow Q) \Leftrightarrow (Q \Leftrightarrow P)$
eliminazione dell'implicazione	$P \Rightarrow Q \Leftrightarrow \neg P \vee Q$
eliminazione dell'implicazione negata	$\neg(P \Rightarrow Q) \Leftrightarrow P \wedge \neg Q$
eliminazione della doppia implicazione (1)	$(P \Leftrightarrow Q) \Leftrightarrow (P \Rightarrow Q) \wedge (Q \Rightarrow P)$
eliminazione della doppia implicazione (2)	$(P \Leftrightarrow Q) \Leftrightarrow (P \wedge Q) \vee (\neg P \wedge \neg Q)$

Tabella 9.3: Leggi di altri connettivi e di eliminazione

Come si può dimostrare una conseguenza logica

- Dalla definizione?
  - Costoso per il calcolo proposizionale
  - Impossibile per altre logiche
- Con dimostrazioni basate su manipolazioni simboliche di formule
  - Necessità di definire con precisione concetto di dimostrazione
  - Identificare assunzioni legittime
  - Discutere correttezza o anche completezza

Sistemi di dimostrazione

Fissato Δ insieme di formule (esempio: formule proposizionali, formule predicative, equazioni, ...)

Sistema di dimostrazioni su Δ insieme di regole di inferenza e assiomi

$$\frac{P_1 \dots P_n}{P}[r] \qquad \frac{\text{premesse}}{\text{conseguenza}}[\text{regola}]$$

- Esempio: $[PDS]$
- Premesse e conseguenza

Dimostrazione di una formula Q in Δ da un insieme di premesse Γ

Una dimostrazione in un proof system $\mathcal{R}$ di una formula $Q \in \Delta$ a partire da un insieme di premesse $\Gamma \subseteq \Delta$ è una

- Sequenza di formule

  $Q_1, Q_2, \dots, Q_n$ dove

1. ogni formula Q_i è un elemento di Γ oppure è ottenuta applicando una regola di inferenza di $\mathcal{R}$ a partire dalle formule in Γ o in $Q_1, \dots, Q_{i-1}$
2. Q_n è proprio Q

Se esiste una dimostrazione di Q a partire da Γ in $\mathcal{R}$ scriveremo

$$\Gamma \vdash_{\mathcal{R}} Q \qquad (Q \text{ è dimostrabile da } \Gamma \text{ (in } \mathcal{R}))$$

Correttezza e completezza di un proof system

P è una conseguenza logica di un insieme di formule Γ se ogni modello di Γ è anche un modello di P

$$\Gamma \vdash_{\mathcal{R}} P \text{ implica } \Gamma \models P \quad \text{(correttezza)}$$
$$\Gamma \models P \text{ implica } \Gamma \vdash_{\mathcal{R}} P \quad \text{(completezza)}$$

Espressività del Calcolo Proposizionale: possiamo “internalizzare” concetti semantici con tautologie

1. $P \equiv Q \;\Leftrightarrow\; P \Leftrightarrow Q$ è una tautologia
2. $\Gamma \models Q \;\Leftrightarrow\; P_1 \wedge \dots \wedge P_n \Rightarrow Q$ è una tautologia, dove $\Gamma = \{P_1, \dots, P_n\}$

Quindi per dimostrare equivalenza o conseguenza logica ci basta poter dimostrare certe tautologie

Vediamo un esempio: come verificare che semplici inferenze logiche siano corrette dimostrando tautologie

Poi vediamo che le dimostrazioni per sostituzione sono dimostrazioni di un opportuno Proof System corretto

> *“Se studio oggi oppure domani, ma domani non studio, allora studio oggi”*

- E’ una inferenza corretta? Come lo si può dimostrare?

  ”studio oggi” deve essere conseguenza logica di *“studio oggi oppure domani, ma domani non studio”*

- Formalizziamola e controlliamo se è una tautologia

  $(O \vee D) \wedge \neg D \Rightarrow O$ è una tautologia?

$$(O \lor D) \land \neg D \Rightarrow O \;\Leftrightarrow\; (O \land \neg D) \lor (D \land \neg D) \Rightarrow O \;\Leftrightarrow\; (O \land \neg D) \Rightarrow O$$
$$\neg(O \land \neg D) \Rightarrow O \;\Leftrightarrow\; \neg O \lor \neg(\neg D) \Rightarrow O \;\Leftrightarrow\; D \lor O \lor \neg O \;\Leftrightarrow\; D \;\Leftrightarrow\; t$$

Un proof system per il calcolo proposizionale

Proof System $\mathcal{S}_{\Leftrightarrow}$ per il Calcolo Proposizionale

Il sistema di dimostrazioni $\mathcal{S}_{\Leftrightarrow}$ sull'insieme di formule $Prop$ è costituito dalle regole di inferenza proprie *Transitività* $[TR]$ e *Principio di Sostituzione* $[PDS]$ e, come assiomi, dall'insieme di tautologie viste.

$$\textbf{Transitività}$$

$$\frac{P \Leftrightarrow Q \quad Q \Leftrightarrow R}{P \Leftrightarrow R}[\mathbf{TR}]$$

Correttezza del proof system per il calcolo proposizionale

Il sistema di dimostrazioni $\mathcal{S}_{\Leftrightarrow}$ è corretto, cioè per ogni insieme $\Gamma \subseteq Prop$ e per ogni formula $P \Leftrightarrow Q \in Prop$, se $\Gamma \vdash_{\mathcal{S}_{\Leftrightarrow}} P \Leftrightarrow Q$ allora $\Gamma \vDash P \Leftrightarrow Q$.

Dimostrazione per induzione sulla lunghezza della dimostrazione

[Caso Base] assiomi "se $R_i \in \Gamma \Rightarrow R_i$ è una tautologia"

[Passo Induttivo] applicazione delle regole di inferenza

quando considero $R_i \quad R_1, \ldots, R_{i-1}$ so già che valgono
dalla definizione so che

$$\sigma = \begin{cases} R_i \in \Gamma \cup \{R_1, \ldots, R_i\} \\ \exists \text{ regola } \gamma \text{ con } \frac{P_1, \ldots, P_x}{R_i}[\gamma] \,.\, P_1, \ldots, P_x \in \Gamma \cup \{R_1, \ldots, R_{i-1}\} \end{cases}$$

dato che $[\gamma]$ è corretta concludiamo che $\Gamma \cup \{R_1, \ldots, R_{i-1}\} = R_i$

Dimostrazione per sostituzione e dimostrazione completa del complemento

$$\begin{aligned}
P \lor (\neg P \land Q) \quad & \Leftrightarrow \quad \underline{(P \lor \neg P)} \land (P \lor Q) && \text{(distributività)} \\
& \Leftrightarrow \quad \mathsf{T} \land (P \lor Q) && \text{(terzo escluso)} \\
& \Leftrightarrow \quad (P \lor Q) \land \mathsf{T} && \text{(commutatività)} \\
& \Leftrightarrow \quad (P \lor Q) && \text{(unità)}
\end{aligned}$$

$$
\begin{align}
\underline{P \lor (\neg P \land Q)} \Leftrightarrow \underline{(P \lor \neg P) \land (P \lor Q)} && (\text{[}\mathbf{PDS}\text{], distributività}) \tag{9.1}\\
\underline{(P \lor \neg P)} \land (P \lor Q) \Leftrightarrow \underline{\mathsf{T}} \land (P \lor Q) && (\text{[}\mathbf{PDS}\text{], terzo escluso}) \tag{9.2}\\
P \lor (\neg P \land Q) \Leftrightarrow \mathsf{T} \land (P \lor Q) && (\text{[}\mathbf{TR}\text{], (9.1) e (9.2)}) \tag{9.3}\\
\underline{\mathsf{T} \land (P \lor Q)} \Leftrightarrow \underline{(P \lor Q) \land \mathsf{T}} && (\text{[}\mathbf{PDS}\text{], commutatività}) \tag{9.4}\\
P \lor (\neg P \land Q) \Leftrightarrow (P \lor Q) \land \mathsf{T} && (\text{[}\mathbf{TR}\text{], (9.3) e (9.4)}) \tag{9.5}\\
\underline{(P \lor Q) \land \mathsf{T}} \Leftrightarrow \underline{(P \lor Q)} && (\text{[}\mathbf{PDS}\text{], unità}) \tag{9.6}\\
P \lor (\neg P \land Q) \Leftrightarrow (P \lor Q) && (\text{[}\mathbf{TR}\text{], (9.5) e (9.6)}) \tag{9.7}
\end{align}
$$

Tecniche di dimostrazione, diretta e con ipotesi non tautologiche

Dimostare un teorema consiste nel dimostrare

$$Ipotesi \models Tesi$$

- Dimostrazione Diretta: Si dimostra che $Ipotesi \Rightarrow Tesi$ è una tautologia
- Dimostrazione con ipotesi non tautologiche: Si dimostra Tesi usando quando serve una $Ipotesi$ per giustificare un passaggio
- Completata la dimostrazione abbiamo $Ipotesi \vdash Tesi$

Dimostrazione per assurdo

Per dimostrare $Ipotesi \models Tesi$ faccio vedere che se le $Ipotesi$ sono vere e la $Tesi$ è falsa, ho una contraddizioni, formalmente $(Ipotesi \land \neg Tesi \Leftrightarrow f)$

Per dimostrare che è corretta, mostriamo che questa è una tautologia

$$
\begin{aligned}
(Ipotesi \Rightarrow Tesi) \quad &\Leftrightarrow \quad (Ipotesi \land \neg Tesi \Rightarrow f)\\
(Ipotesi \Rightarrow Tesi) \quad &\Leftrightarrow \quad (\neg Ipotesi \lor Tesi)
\end{aligned}
$$

Dimostrazione per contrapposizione

Per dimostrare $Ipotesi \models Tesi$ faccio vedere che la $Tesi$ è falsa allora le $Ipotesi$ sono false

La tecnica è corretta perché abbiamo già dimostrato la contronominale:

$$(Ipotesi \Rightarrow Tesi) \quad \Leftrightarrow \quad (\neg Ipotesi \Rightarrow \neg Tesi)$$

Logica dei Predicati

$$\underbrace{\underline{Se\ Anna\ è\ la\ mamma\ di\ Bruno}}_{A}\ \underbrace{e}_{\land}\ \underbrace{Bruno\ ha\ figli}_{B},\ \underbrace{\underline{allora}}_{\Rightarrow}\ \underbrace{\underline{Anna\ è\ Nonna}}_{C}$$

Vorremmo poter parlare, per esempio, di:

- Persone (elementi del dominio): *Anna, Bruno,...*
- Proprietà delle persone: *ha figli, è nonna,...*
- Relazioni tra le persone: *è la mamma di,...*

$$((mamma(Anna, Bruno) \land haFigli(Bruno)) \Rightarrow èNonna(Anna))$$

Vorremmo poter parlare anche di insiemi infiniti, come i naturali

I quantificatori

Permettono di rappresentare pronomi o aggettivi indefiniti come *tutti, nessuno, alcuni,...,* facendo riferimento a elementi del dominio.

- Tutti gli uomini sono mortali $(\forall x \,.\, mortale(x))$
- Nessuno pesa più di 100kg $(\forall x \,.\, \neg(peso(x) > 100))$
- Qualcuno è più alto di suo padre $(\exists x \,.\, altezza(x) > altezza(padre(x)))$

Variabili e Quantificatori

- Quantificatore Universale $(\forall x \,.\, P)$
- Quantificatore Esistenziale $(\exists x \,.\, P)$

Alfabeti del primo ordine

Un Alfabeto del primo ordine $\mathcal{A}$ è una quadrupla $\mathcal{A} = (\mathcal{C}, \mathcal{F}, \mathcal{P}, \mathcal{V})$ dove:

- $\mathcal{C}$ è l'insieme dei simboli di costante
- $\mathcal{F} = \{\mathcal{F}_n\}_{n \in \mathbb{N}}$ è una famiglia di insiemi di simboli di funzione. Per ogni $n \in \mathbb{N}, \mathcal{F}_n$ è l'insieme dei simboli di funzione di arietà n (o con n argomenti)
- $\mathcal{P} = \{\mathcal{P}_n\}_{n \in \mathbb{N}}$ è una famiglia di insiemi di simboli di predicato. Per ogni $n \in \mathbb{N}, \mathcal{P}_n$ è l'insieme dei simboli di predicato di arietà n (o con n argomenti)
- $\mathcal{V}$ è l'insieme delle variabili

L'alfabeto dei naturali

Usiamo i simboli che ci suggeriscono il loro significato:

L'alfabeto dei naturali $\mathcal{A}_\mathbb{N} = (\mathcal{C}_\mathbb{N}, \mathcal{F}_\mathbb{N}, \mathcal{P}_\mathbb{N}, \mathcal{V}_\mathbb{N})$

- i simboli di costante $\mathcal{C}_\mathbb{N} = \mathbb{N}$
- i simboli di funzione $\mathcal{F}_\mathbb{N} = \{succ(\_), \_ + \_, \_ \times \_, \_/\_, \_\%\_, \dots\}$
- i simboli di predicato $\mathcal{P}_\mathbb{N} = \{\_ \leq \_, \_ \geq \_, \_ < \_, \_ > \_, \_ = \_, primo(\_), pari(\_), \dots\}$
- le variabili $\mathcal{V} = \{x, y, \dots, n, m, \dots\}$

$$\text{Logica dei Predicati}$$

$$\langle Pred \rangle \rightsquigarrow \langle Atom \rangle \mid \neg\langle Atom \rangle \mid \langle Pred \rangle\langle OpB \rangle\langle Pred \rangle \mid (\forall\langle Var \rangle \,.\, \langle Pred \rangle \mid (\exists\langle Var \rangle \,.\, \langle Pred \rangle)$$

$$\langle Atom \rangle \rightsquigarrow T \mid F \mid (\langle Pred \rangle) \mid \langle PIde_0 \rangle \mid \langle PIde_n \rangle\overbrace{(\langle Term \rangle, \dots, \langle Term \rangle)}^{n}, n \in \mathbb{N}^+$$

$$\langle Term \rangle \rightsquigarrow \langle Var \rangle \mid \langle Const \rangle \mid \langle FIde_n \rangle\overbrace{(\langle Term \rangle, \dots, \langle Term \rangle)}^{n}, n \in \mathbb{N}^+$$

$$\langle OpB \rangle \rightsquigarrow \wedge \mid \vee \mid \Rightarrow \mid \Leftarrow \mid \Leftrightarrow$$

$$(n \in \mathbb{N}) \quad \langle\langle\ \langle PIde_n \rangle\ \rangle\rangle = \mathcal{P}_n \quad \langle\langle\ \langle Const \rangle\ \rangle\rangle = \mathcal{C} \quad \langle\langle\ \langle Var \rangle\ \rangle\rangle = \mathcal{V}$$

Esempi di termini e formule sui naturali

- Termini: $5, x, x + 5, succ(succ(4 + 5)) \dots$

$$\langle Term\rangle \rightsquigarrow \langle Var\rangle \mid \langle Const\rangle \mid \langle FIde_n\rangle\overbrace{(\langle Term\rangle, \ldots, \langle Term\rangle)}^{n}, n \in \mathbb{N}^+$$

- Formule: $primo(x), pari(y+1), y\%2 = 0, \ldots$

$$\langle Atom\rangle \rightsquigarrow T \mid F \mid (\langle Pred\rangle) \mid \langle PIde_0\rangle \mid \langle PIde_n\rangle\overbrace{(\langle Term\rangle, \ldots, \langle Term\rangle)}^{n}, n \in \mathbb{N}^+$$

- $x \leq 6 \wedge pari(x), \neg(primo(x) \Rightarrow x > 0), \ldots$

$$(\exists y \,.\, y < 5), (\forall x \,.\, x \geq 0), \ldots$$

$$(\forall x \,.\, \neg primo(x) \Leftrightarrow (\exists y \,.\, \neg(y = 1 \vee y = x) \wedge (x\%y = 0))), \ldots$$

$$\langle Pred\rangle \rightsquigarrow \langle Atom\rangle \mid \neg\langle Atom\rangle \mid \langle Pred\rangle\langle OpB\rangle\langle Pred\rangle \mid \langle\forall\langle Var\rangle \,.\, \langle Pred\rangle \mid \langle\exists\langle Var\rangle \,.\, \langle Pred\rangle\rangle$$

Esempi di formalizzazione

- Quantificazione Ristretta

  "Esiste un numero che è sia pari che primo" $(\exists x \,.\, (pari(x) \wedge primo(x)))$
  "Tutti i numeri naturali dispari sono maggiori di zero"
  $(\forall x \,.\, (dispari(x) \Rightarrow (x > 0)))$

Formule quantificate

- Portata o Campo d'Azione di un quantificatore

$$(\forall x \,.\, \overbrace{x \leq 0 \Rightarrow (\forall y \,.\, \underbrace{y \geq x}_{\forall y})}^{\forall x})$$

- Variabile legata o chiusa

$$(\forall x \,.\, \underbrace{x > 0}_{\forall x}) \Rightarrow (\exists y \,.\, \underbrace{y < \overbrace{x}^{libera}}_{\exists y})$$

- Formula chiusa: ogni occorrenza di variabile è legata, altrimenti aperta

Interpretazioni

Interpretazione per alfabeto del primo ordine

Un interpretazione $\mathcal{I}$ per $\mathcal{A} = (\mathcal{C}, \mathcal{F}, \mathcal{P}, \mathcal{V})$ è una coppia $\mathcal{I} = (\mathcal{D}, \alpha)$ dove $\mathcal{D}$ è il dominio di interpretazione (un insieme di valori), mentre $\alpha = \langle \alpha_{\mathcal{C}}, \alpha_{\mathcal{F}}, \alpha_{\mathcal{P}} \rangle$ è una associazione dove:

- $\alpha_{\mathcal{C}} : \mathcal{C} \to \mathcal{D}$ costante viene interpretata con un valore del dominio
- $\alpha_{\mathcal{F}} = \{\alpha_{\mathcal{F}_n}\}_{n \in \mathbb{N}}$ è una famiglia di funzioni: $\forall f \in \mathcal{F}_n, \alpha_{\mathcal{F}_n}(f) : \mathcal{D}^n \to \mathcal{D}$
- $\alpha_{\mathcal{P}} = \{\alpha_{\mathcal{P}_n}\}_{n \in \mathbb{N}}$ è definito come
  - $\alpha_{\mathcal{P}_0} : \mathcal{P}_0 \to Bool$

- $\alpha_{\mathcal{P}_n} \subseteq \mathcal{D}, \forall n \in \mathbb{N}^+, \forall A \in \mathcal{P}_n$

Interpretazione standard dei naturali

L'interpretazione standard per l'alfabeto dei naturali $\mathcal{A}_{\mathbb{N}} = (\mathcal{C}_{\mathbb{N}}, \mathcal{F}_{\mathbb{N}}, \mathcal{P}_{\mathbb{N}}, \mathcal{V}_{\mathbb{N}})$ è la coppia $\mathcal{I}_{\mathbb{N}} = (\mathcal{D}_{\mathbb{N}}, \alpha^{\mathbb{N}})$, dove $\mathcal{D}_{\mathbb{N}} = \mathbb{N}$, mentre $\alpha^{\mathbb{N}} = \langle \alpha^{\mathbb{N}}_{\mathcal{C}}, \alpha^{\mathbb{N}}_{\mathcal{F}}, \alpha^{\mathbb{N}}_{\mathcal{P}} \rangle$ dove

- $\alpha^{\mathbb{N}}_{\mathcal{C}} : \mathcal{C}_{\mathbb{N}} \to \mathbb{N},\ \text{con } \alpha^{\mathbb{N}}_{\mathcal{C}}(n) = n$
- $\alpha^{\mathbb{N}}_{\mathcal{F}}$ associa ad ogni simbolo in $\mathcal{F}_{\mathbb{N}}$ la corrispondente funzione sui naturali. Per esempio

  $\alpha^{\mathbb{N}}_{\mathcal{F}}(succ)(n) = n + 1$

  $\alpha^{\mathbb{N}}_{\mathcal{F}}(+)(3, 5) = 8$
- $\alpha^{\mathbb{N}}_{\mathcal{P}}$ associa ogni simbolo predicato in $\mathcal{P}_{\mathbb{N}}$ di arietà n l'insieme di n-uple di naturali che la soddisfano. Per esempio

  $(n, m) \in \alpha^{\mathbb{N}}_{\mathcal{P}}(\leq)$ se e solo se n è minore o uguale di m

  $n \in \alpha^{\mathbb{N}}_{\mathcal{P}}(primo)$ se e solo se n è primo

Assegnamenti per dare un valore alle variabili

- Interpretazioni forniscono valore a simboli di costante, funzione e predicato
- Assegnamenti forniscono valore a variabili, elementi del dominio

Dato un alfabeto $\mathcal{A}$ con un insieme di variabili $\mathcal{V}$ e un'interpretazione $\mathcal{I}$ con dominio $\mathcal{D}$, un assegnamento è una funzione parziale

$$r : \mathcal{V} \to \mathcal{D}$$

Dati $r : \mathcal{V} \to \mathcal{D}, v \in \mathcal{V} \wedge d \in \mathcal{D}$, definiamo

$$r[x \mapsto d](y) = \begin{cases} d & \text{se } y = x \\ r(y) & \text{altrimenti} \end{cases}$$

Semantica dei termini

Data $\mathcal{I} = \langle \mathcal{D}, \alpha \rangle$ e $r : \mathcal{V} \to \mathcal{D}$, il valore rispetto ad $\mathcal{I}$ ed r è la funzione parziale

$$[\![\_]\!]^r_{\mathcal{I}} : Term \to \mathcal{D}$$

definita per induzione strutturale

1. $[\![x]\!]^r_{\mathcal{I}} = r(x) \text{ per } x \in \mathcal{V}$
2. $[\![C]\!]^r_{\mathcal{I}} = \alpha_{\mathcal{C}}(c) \text{ per } c \in \mathcal{C}$
3. Se f è un simbolo di funzione di arietà n e $[\![t_1]\!]^r_{\mathcal{I}} = d_1, \dots, [\![t_n]\!]^r_{\mathcal{I}} = d_n$, allora

$$[\![f(t_1, \dots, t_n)]\!]^r_{\mathcal{I}} = \alpha_{\mathcal{F}}(f)(d_1, \dots, d_n)$$

Esempio di semantica dei termini

$r : \mathcal{V}_{\mathbb{N}} \to \mathbb{N}$ tale che $r(y) = 3$

$$
[\![succ((y \times 4)/5]\!]^r_{\mathcal{I}} \begin{aligned}[t] &= \alpha^{\mathbb{N}}_{\mathcal{F}}(succ)([\![(y \times 4)/5]\!]^r_{\mathcal{I}_{\mathbb{N}}}) \\ &= \alpha^{\mathbb{N}}_{\mathcal{F}}(succ)(([\![y]\!]^r_{\mathcal{I}_{\mathbb{N}}} \times [\![4]\!]^r_{\mathcal{I}_{\mathbb{N}}})/[\![5]\!]^r_{\mathcal{I}_{\mathbb{N}}}) \\ &= \alpha^{\mathbb{N}}_{\mathcal{F}}(succ)((r(y) \times 4))/5) \\ &= \alpha^{\mathbb{N}}_{\mathcal{F}}(succ)((3 \times 4))/5) \\ &= \alpha^{\mathbb{N}}_{\mathcal{F}}(succ)(2) \\ &= 2 + 1 \\ &= 3 \end{aligned}
$$

$$
\langle Atom \rangle \rightsquigarrow T \mid F \mid (\langle Pred \rangle) \mid \langle PIde_0 \rangle \mid \langle PIde_n \rangle \overbrace{(\langle Term \rangle, \dots, \langle Term \rangle)}^{n}, n \in \mathbb{N}^+
$$

Semantica di formule (atomiche)

Semantica delle formule predicative, dati $\mathcal{I} = \langle \mathcal{D}, \alpha \rangle$ e $r : \mathcal{V} \to \mathcal{D}$, il valore rispetto ad $\mathcal{I}$ ed r delle formule predicative è dato da

$$
[\![\_]\!]^r_{\mathcal{I}} : Pred \to \mathcal{D}
$$

definita per induzione strutturale

1. $[\![T]\!]^r_{\mathcal{I}} = t$ e $[\![F]\!]^r_{\mathcal{I}} = f$
2. $[\![A]\!]^r_{\mathcal{I}} = \alpha_{\mathcal{P}_0}(A) \text{ per } A \in \mathcal{P}_0$
3. Per ogni $A \in \mathcal{P}_n$ di arietà $n > 0$

$$
[\![A(t_1, \dots, t_n)]\!]^r_{\mathcal{I}} = \begin{cases} t & \text{se } ([\![t_1]\!]^r_{\mathcal{I}}, \dots, [\![t_n]\!]^r_{\mathcal{I}}) \in \alpha_{\mathcal{P}_n}(A) \\ f & \text{altrimenti} \end{cases}
$$

4. $[\![(P)]\!]^r_{\mathcal{I}} = ([\![P]\!]^r_{\mathcal{I}}),\ \forall P \in Pred$

$$
\langle Pred \rangle \rightsquigarrow \langle Atom \rangle \mid \neg \langle Atom \rangle \mid \langle Pred \rangle \langle OpB \rangle \langle Pred \rangle \mid \langle \forall \langle Var \rangle \ .\ \langle Pred \rangle \mid \langle \exists \langle Var \rangle \ .\ \langle Pred \rangle \rangle
$$

Semantica di formule

5. $[\![\neg P]\!]^r_{\mathcal{I}} = \neg [\![P]\!]^r_{\mathcal{I}}$ per ogni formula atomica P
6. $[\![P \ op \ Q]\!]^r_{\mathcal{I}} = [\![P]\!]^r_{\mathcal{I}} \ op \ [\![Q]\!]^r_{\mathcal{I}}$ per ogni connettivo $op \in \{\wedge, \vee, \Rightarrow, \Leftarrow, \Leftrightarrow\}$
7. $[\![\forall x \ .\ P]\!]^r_{\mathcal{I}} = t$ se e solo se $[\![P]\!]^{r[x \mapsto d]}_{\mathcal{I}} = t,\ \forall d \in \mathcal{D}$
8. $[\![\exists x \ .\ P]\!]^r_{\mathcal{I}} = t$ se e solo se $[\![P]\!]^{r[x \mapsto d]}_{\mathcal{I}} = t,\ \text{per almeno un } d \in \mathcal{D}$

Classificazione di formule della Logica dei Predicati

- Vera in tutte le interpretazioni: $\models P$
- Falsa in tutte le interpretazioni: $\models \neg P$
- Vera in almeno una interpretazione: $\not\models \neg P$
- Falsa in almeno una interpretazione: $\not\models P$