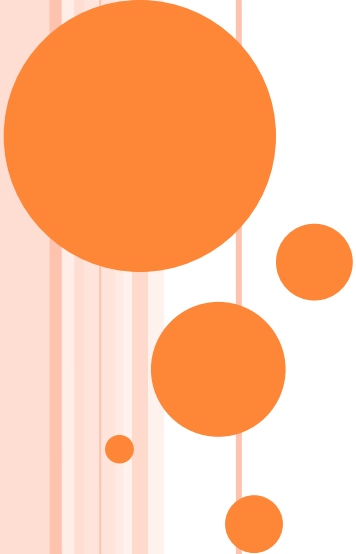




CALCOLO DEL PRIMO ORDINE

ANCORA SUL CONCETTO DI CALCOLO (PROOF SYSTEM)

- Un sistema di dimostrazione è un insieme di *regole di inferenza*
- Ciascuna regola di inferenza consente di derivare una formula φ (conseguenza) da un insieme di formule Γ (premesse)
- Una dimostrazione di una formula φ a partire da un insieme di premesse Γ è una sequenza di formule $\varphi_1, \dots, \varphi_n$ tale che
 - Ogni formula φ_i è un elemento di Γ oppure è ottenuta applicando una regola di inferenza a partire dalle premesse Γ e $\varphi_1, \dots, \varphi_{i-1}$
 - φ_n coincide con φ



OSSERVAZIONI

- Il calcolo proposizionale è un caso particolare di proof system
- Nel caso di dimostrazioni di equivalenza, il proof system è dato dalle leggi di equivalenza
- Nel caso di dimostrazioni di implicazione, il proof system è arricchito, essenzialmente, con
 - Modus ponens
 - Risoluzione
- Anche per il primo ordine ci limitiamo alle regole di inferenza che consentono di dimostrare teoremi del tipo:
 - $\varphi \equiv \psi$
 - $\varphi \Rightarrow \psi$



LEGGI GENERALI E IPOTESI (1)

- Anche nei calcoli del primo ordine useremo formule valide (tautologie nel calcolo proposizionale) come leggi generali
- L'uso di formule valide garantisce la *validità* del risultato:
 - Sia Γ un insieme di formule valide e φ una formula dimostrabile a partire da Γ ($\Gamma \vdash \varphi$)
 - se $\Gamma \vdash \varphi$ allora per la correttezza di $\vdash$, $\Gamma \models \varphi$ ovvero φ è vera in ogni modello di Γ
 - poiché ogni interpretazione è modello di Γ , φ è vera in ogni interpretazione
 - quindi è *valida*, ovvero $\models \varphi$



LEGGI GENERALI E IPOTESI (2)

- Se in Γ , oltre alle formule valide abbiamo anche altre formule (ipotesi) allora la dimostrazione

$$\Gamma \vdash \varphi$$

non garantisce la validità di φ , ma il fatto che φ sia una conseguenza logica delle ipotesi,

ovvero se $\Gamma = \Gamma_1 \cup \Gamma_2$, dove Γ_1 sono formule valide e Γ_2 ipotesi, allora

$$\Gamma_2 \models \varphi$$



GENERALIZZAZIONE DEL PRINCIPIO DI SOSTITUZIONE PER $\equiv$

$$(Q \equiv R) \in \Gamma$$

$$\Gamma \vdash P \equiv P[Q/R]$$

- N.B. La generalizzazione consiste nel far riferimento all'intero insieme delle premesse Γ



LEGGI GENERALI PER L'EQUIVALENZA (1)

Per le dimostrazioni di $\equiv$ continuano a valere
le leggi viste

$$p \equiv p$$

(Riflessività)

$$(p \equiv q) \equiv (q \equiv p)$$

(Simmetria)

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

(Associatività)

$$(p \equiv \mathbf{T}) \equiv p$$

(Unità)

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

(Transitività)



LEGGI GENERALI PER L'EQUIVALENZA (2)

$p \vee q \equiv q \vee p$ (Commutatività)

$p \wedge q \equiv q \wedge p$

$p \vee (q \vee r) \equiv (p \vee q) \vee r$ (Associatività)

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

$p \vee p \equiv p$ (Idempotenza)

$p \wedge p \equiv p$

$p \wedge \mathbf{T} \equiv p$ (Unità)

$p \vee \mathbf{F} \equiv p$

$p \wedge \mathbf{F} \equiv \mathbf{F}$ (Zero)

$p \vee \mathbf{T} \equiv \mathbf{T}$

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

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



LEGGI GENERALI PER L'EQUIVALENZA (3)

$\sim(\sim p) \equiv p$ (Doppia negazione)

$p \vee \sim p \equiv \mathbf{T}$ (Terzo escluso)

$p \wedge \sim p \equiv \mathbf{F}$ (Contraddizione)

$\sim p \vee \sim q \equiv \sim(p \wedge q)$ (De Morgan)

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

$\sim \mathbf{T} \equiv \mathbf{F}$ (**T:F**)

$\sim \mathbf{F} \equiv \mathbf{T}$ (**F:T**)



LEGGI GENERALI PER L'EQUIVALENZA (4)

- $(p \Rightarrow q) \equiv (\sim p \vee q)$ (elim- $\Rightarrow$)
- $(p \equiv q) \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$ (elim- $\equiv$)
- $(p \equiv q) \equiv (p \wedge q) \vee (\sim p \wedge \sim q)$
- $p \Rightarrow (q \Rightarrow r) \equiv (p \wedge q) \Rightarrow r$ (simpl- $\Rightarrow$)



PRINCIPIO DI SOSTITUZIONE PER $\Rightarrow$

$(Q \Rightarrow R) \in \Gamma$ Q occorre positivamente in P

$\Gamma \vdash P \Rightarrow P[R/Q]$

$(Q \Rightarrow R) \in \Gamma$ Q occorre negativamente in P

$\Gamma \vdash P[R/Q] \Rightarrow P$



ESEMPI

$$(P \vee R) \wedge \sim P$$

$$\Rightarrow \{Ip: P \Rightarrow Q\}$$

$$(Q \vee R) \wedge \sim P$$

corretto

$$(P \vee R) \wedge \sim P$$

$$\Rightarrow \{Ip: P \Rightarrow Q\}$$

$$(P \vee R) \wedge \sim Q$$

sbagliato!



TEOREMA DI DEDUZIONE

$$\Gamma \vdash P \Rightarrow Q$$

se e soltanto se

$$\Gamma, P \vdash Q$$

Ovvero per dimostrare una implicazione

$$P \Rightarrow Q$$

è possibile costruire una dimostrazione per Q
usando le leggi generali e P come ipotesi

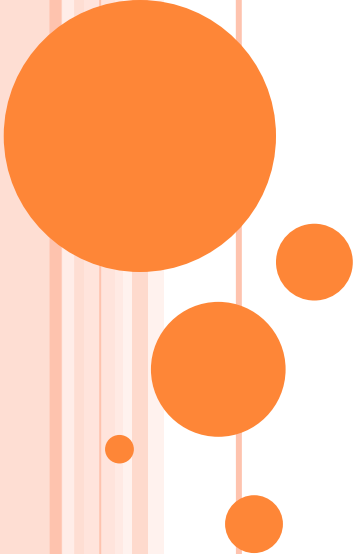


LEGGI GENERALI PER L'IMPLICAZIONE

- $((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$ (transitività)
- $(p \Rightarrow q) \equiv (\sim p \vee q)$ (elim- $\Rightarrow$)
- $(p \wedge (p \Rightarrow q)) \Rightarrow q$ (modus ponens)
- $p \wedge q \Rightarrow q$ (simpl- $\wedge$)
- $p \Rightarrow p \vee q$ (intr- $\vee$)
- $(p \vee q) \wedge (\sim p \vee r) \Rightarrow (q \vee r)$ (Risoluzione)

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





LEGGI PER I QUANTIFICATORI

LEGGI PER I QUANTIFICATORI

- Per il Calcolo Proposizionale, le **leggi** che abbiamo visto sono **tautologie**: lo abbiamo dimostrato usando tavole di verità o dimostrazioni di vario formato
- Per il Calcolo dei Predicati le **leggi** sono **formule valide**. Per convincerci della validità di una legge possiamo usare la definizione, oppure una dimostrazione che usi solo premesse valide
- In una formula con quantificatore come $(\forall x.P)$, la **portata** di $\forall x$ è la sottoformula P . Analogamente per $(\exists x.P)$.



LEGGI PER I QUANTIFICATORI (1)

- $(\forall x.P) \Rightarrow P[t/x]$ (elim- $\forall$)

dove t è un *termine chiuso* e $P[t/x]$ è ottenuto da P sostituendo tutte le occorrenze di x con t

- Esempi:

$$(\forall x.\text{pari}(x) \wedge x > 2 \Rightarrow \sim \text{primo}(x))$$

$$\Rightarrow \{ \text{elim-} \forall \}$$

$$\text{pari}(7) \wedge 7 > 2 \Rightarrow \sim \text{primo}(7)$$

$$(\forall x.\text{uomo}(x) \Rightarrow \text{mortale}(x))$$

$$\Rightarrow \{ \text{elim-} \forall \}$$

$$\text{uomo}(\text{Socrate}) \Rightarrow \text{mortale}(\text{Socrate})$$



VALIDITA' DELLA LEGGE ELIM- $\forall$

- $(\forall \mathbf{x}.P) \Rightarrow P[t/\mathbf{x}]$ **elim- $\forall$** [t chiuso]
- Poiché non abbiamo visto altre leggi, usiamo la definizione di validità: **elim- $\forall$** deve essere vera in qualunque interpretazione
- Sia $I = (D, \alpha)$ un'interpretazione e ρ un assegnamento:

(S6) $I_\rho(\text{elim-}\forall) = \mathbf{F}$ se $I_\rho((\forall \mathbf{x}.P)) = \mathbf{T}$ e $I_\rho(P[t/\mathbf{x}]) = \mathbf{F}$
 $= \mathbf{T}$ altrimenti **[OK]**
- Supponiamo allora che $I_\rho((\forall \mathbf{x}.P)) = \mathbf{T}$. Abbiamo

(S8) $I_\rho(\forall \mathbf{x}.P) =$
 $\mathbf{T}$ se $I_{\rho[d/\mathbf{x}]}(P) = \mathbf{T}$ per qualunque d in D , $\mathbf{F}$ altrimenti
- Sia $\underline{d} = I_\rho(t)$. Allora $I_{\rho[\underline{d}/\mathbf{x}]}(P) = \mathbf{T}$, quindi $I_\rho(P[t/\mathbf{x}]) = \mathbf{T}$
 [perché $I_\rho(P[t/\mathbf{x}]) = I_{\rho[\underline{d}/\mathbf{x}]}(P(\mathbf{x}))$, crediamoci...]

LEGGI PER I QUANTIFICATORI (2)

- $P[t/x] \Rightarrow (\exists x.P)$ (intro- $\exists$)

- Esempio

$\text{pari}(8) \wedge 8 > 2$

$\Rightarrow \{ \text{intro-}\exists \}$

$(\exists x.\text{pari}(x) \wedge x > 2)$



LEGGI PER I QUANTIFICATORI (3)

- $\sim(\exists x.P) \equiv (\forall x.\sim P)$ (De Morgan)
- $\sim(\forall x.P) \equiv (\exists x.\sim P)$
- $(\forall x. (\forall y.P)) \equiv (\forall y. (\forall x.P))$ (annidamento)
- $(\exists x. (\exists y.P)) \equiv (\exists y. (\exists x.P))$
- $(\forall x.P) \equiv P$ se x non occorre in P (costante)
- $(\exists x.P) \equiv P$ se x non occorre in P



LEGGI PER I QUANTIFICATORI (4)

- $(\forall x.P \wedge Q) \equiv (\forall x.P) \wedge (\forall x.Q)$ $(\forall: \wedge)$

- $(\exists x.P \vee Q) \equiv (\exists x.P) \vee (\exists x.Q)$ $(\exists: \vee)$

(Distrib.)

- $(\forall x.P \wedge Q) \equiv (\forall x.P) \wedge Q$

se x non compare in Q

- $(\forall x.P \vee Q) \equiv (\forall x.P) \vee Q$

se x non compare in Q

- $(\exists x.P \wedge Q) \equiv (\exists x.P) \wedge Q$

se x non compare in Q

- $(\exists x.P \vee Q) \equiv (\exists x.P) \vee Q$

se x non compare in Q

- $(\forall x.P) \Rightarrow (\forall x.P \vee Q)$

- $(\exists x.P) \Rightarrow (\exists x.P \vee Q)$

- $(\forall x.P \wedge Q) \Rightarrow (\forall x.P)$

- $(\exists x.P \wedge Q) \Rightarrow (\exists x.P)$



Esempi

- Dimostrare la validità delle seguenti formule mostrando come siano dimostrabili a partire dalle leggi viste precedentemente:

$$(\forall x. P \vee Q \Rightarrow R) \equiv (\forall x. P \Rightarrow R) \wedge (\forall x. Q \Rightarrow R) \quad \textbf{(Dominio)}$$

$$(\exists x. (P \vee Q) \wedge R) \equiv (\exists x. P \wedge R) \vee (\exists x. Q \wedge R) \quad \textbf{(Dominio)}$$

[suggerimento: sfruttare la legge precedente usando De Morgan]

$$(\forall x. P \wedge Q) \equiv (\forall x. P) \wedge Q \quad \text{se } x \text{ non compare in } Q \quad \textbf{(Distrib)}$$


LEGGI PER L'UGUAGLIANZA (=)

- Il termine $t = t'$ è vero in una data interpretazione se t e t' denotano lo stesso elemento del dominio di interesse
- $x = y \Rightarrow (P \equiv P[y/x])$ (Leibniz)
- $(x = y \wedge P) \equiv (x = y \wedge P[y/x])$
- $(x = y \wedge P) \Rightarrow P[y/x]$
- $(\forall x. x = y \Rightarrow P) \equiv P[y/x]$ (singoletto)
- $(\exists x. x = y \wedge P) \equiv P[y/x]$



REGOLA DI GENERALIZZAZIONE

Per dimostrare una formula del tipo $(\forall x.P)$ possiamo procedere sostituendo x con un nuovo ('fresco') simbolo di costante d e dimostrare $P[d/x]$

$$\Gamma \vdash P[d/x], \text{ con } d \text{ nuova costante}$$

$$\Gamma \vdash (\forall x.P)$$


Esercizi

- Si dimostri che le seguenti formule sono valide
- $(\forall x.P) \Rightarrow (\exists x.P)$
- $(\exists x.P \Rightarrow (\forall x.P))$
- $((\forall x.P \Rightarrow R) \wedge (\exists x.P)) \Rightarrow (\exists x.R)$



Esempi: proprietà di operazioni su insiemi

- Dimostrare, usando come premesse le formule di *Ins* che definiscono le operazioni su insiemi, che:
- $(\forall C, D . C \cup D = D \cup C)$
- $(\forall A, B, C . A \cup (B \cap C) = (A \cup B) \cap (A \cup C))$

