



LOGICA DEL PRIMO ORDINE: PROOF SYSTEM

Corso di Logica per la Programmazione

A.A. 2013/14

Andrea Corradini

LOGICA DEL PRIMO ORDINE: RIASSUNTO

- Sintassi: grammatica libera da contesto (BNF), parametrica rispetto a un alfabeto $\mathbf{A} = (\mathbf{C}, \mathbf{F}, \mathbf{P}, \mathbf{V})$
- Interpretazione $\mathbf{I} = (\mathbf{D}, \boldsymbol{\alpha})$: fissa il significato dei simboli dell'alfabeto su un opportuno dominio
- Semantica: data una interpretazione $\mathbf{I} = (\mathbf{D}, \boldsymbol{\alpha})$ e una formula φ , le regole (S1)-(S9) permettono di calcolare $\mathbf{I}_\rho(\varphi)$, il valore di verità di φ in \mathbf{I} .



MODELLI

- Sia \mathbf{I} una interpretazione e φ una formula chiusa.
Se φ è vera in \mathbf{I} diciamo che \mathbf{I} è un **modello** di φ e scriviamo

$$\mathbf{I} \models \varphi$$

- Se Γ è un insieme di formule, con

$$\mathbf{I} \models \Gamma$$

intendiamo che \mathbf{I} è un modello per tutte le formule in Γ

- Se una formula è vera in almeno una interpretazione si dice che è **soddisfacibile** altrimenti è **insoddisfacibile**
- Se una formula è vera in tutte le interpretazioni si dice che è **valida** (estensione del concetto di **tautologia**) e scriviamo

$$\models \varphi$$



ESEMPI

- Formula **soddisfacibile**

$$p(a)$$

Con $D = \mathbb{N}$

$$a = 44$$

$p(x) = \mathbf{T}$ se x è pari, \mathbf{F} altrimenti

- Formula **valida**

$$(\forall x.p(x) \vee \sim p(x))$$

- Corrispondono alle **tautologie**

- Formula **insoddisfacibile**

$$p(a) \wedge \sim p(a)$$

- Corrispondono alle **contraddizioni**



CONSEGUENZA LOGICA

- Il concetto di **conseguenza logica** consente di **parametrizzare** la validità di una formula φ rispetto ad una teoria rappresentata da un insieme di formule Γ
- Diciamo che φ è una **conseguenza logica** di Γ e scriviamo

$$\Gamma \models \varphi$$

se e soltanto se φ è vera in tutti i modelli di Γ ,
ovvero tutte le interpretazioni che rendono vere le formule in Γ rendono vera anche φ



I SISTEMI DI DIMOSTRAZIONE (PROOF SYSTEMS)

- Dato un insieme di formule, un **sistema di dimostrazione** (o **proof system**) 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 $\varphi_1, \dots, \varphi_n$ 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
 - Scriviamo $\Gamma \vdash \varphi$ se esiste una dimostrazione di φ a partire da Γ



CALCOLO PROPOSIZIONALE COME PROOF SYSTEM

- Il **Calcolo Proposizionale** è un **proof system** sull'insieme delle proposizioni
- Le regole di inferenza sono
 - **il principio di sostituzione** per le dimostrazioni di equivalenza
 - **i principi di sostituzione per \Rightarrow** per le dimostrazioni di implicazioni
- Anche per il primo ordine ci limitiamo alle regole di inferenza che consentono di dimostrare teoremi del tipo:
 - $\varphi \equiv \psi$
 - $\varphi \Rightarrow \psi$



CORRETTEZZA E COMPLETEZZA DEI PROOF SYSTEMS

- Un proof system è **corretto** se quando esiste una dimostrazione di una formula φ da un insieme di premesse Γ allora φ è una conseguenza logica di Γ , cioè
se $\Gamma \vdash \varphi$ allora $\Gamma \models \varphi$
- Sia il Calcolo Proposizionale che il calcolo che vedremo per la Logica del Primo Ordine sono corretti
 - Non ha senso considerare proof systems non corretti!!
- Un proof system è **completo** se quando una formula φ è una conseguenza logica di un insieme di premesse Γ , allora esiste una dimostrazione di φ da Γ , cioè
se $\Gamma \models \varphi$ allora $\Gamma \vdash \varphi$
- Il Calcolo Proposizionale è completo.



COSA VEDREMO DEL CALCOLO DEL PRIMO ORDINE

- Rivedremo le **regole di inferenza** del Calcolo Proporzionale in forma più generale (con premesse)
 - Per i connettivi logici useremo le **leggi** del CP
- Introdurremo **nuove leggi e nuove regole di inferenza** per i quantificatori
- Vedremo esempi di dimostrazione di validità di formule del primo ordine, usando le tecniche di dimostrazione viste
- Le regole di inferenza che introdurremo **non** formano un proof system **completo** per LP1: questo sarebbe impossibile
- **Teorema di Incompletezza di Gödel (1931)**: nella logica del primo ordine sui naturali, esistono formule vere che non sono dimostrabili



LEGGI GENERALI E IPOTESI (1)

- Anche nel calcolo del primo ordine useremo **formule valide** come leggi generali (corrispondenti alle tautologie nel calcolo proposizionale)
- L'uso di formule valide garantisce la **validità** del risultato. Vediamo perché:
 - 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 la dimostrazione garantisce che

$$\Gamma_2 \models \varphi$$



GENERALIZZAZIONE DEL PRINCIPIO DI SOSTITUZIONE PER \equiv

- Nota: La generalizzazione consiste nel far riferimento a un insieme delle premesse Γ

$$\frac{(Q \equiv R) \in \Gamma}{\Gamma \vdash P \equiv P[Q/R]}$$

- “Se Q e R sono logicamente equivalenti nelle premesse Γ , allora il fatto che P e $P[Q/R]$ sono equivalenti è conseguenza logica di Γ ”



GENERALIZZAZIONE DEI PRINCIPI DI SOSTITUZIONE PER \Rightarrow

- Dobbiamo estendere il concetto di **occorrenza positiva** o **negativa** alle formule quantificate
 - **P** occorre **positivamente** in $(\forall x. P)$
 - **P** occorre **positivamente** in $(\exists x. P)$

$$\frac{(Q \Rightarrow R) \in \Gamma \quad Q \text{ occorre } \mathbf{positivamente} \text{ in } P}{\Gamma \vdash P \Rightarrow P[R/Q]}$$

$$\frac{(Q \Rightarrow R) \in \Gamma \quad Q \text{ occorre } \mathbf{negativamente} \text{ in } P}{\Gamma \vdash P[R/Q] \Rightarrow P}$$



ESEMPI

$$(\forall x. P \vee R) \wedge (\exists x. \sim P)$$

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

$$(\forall x. Q \vee R) \wedge (\exists x. \sim P)$$

Corretto, perché la prima P occorre positivamente

$$(\forall x. P \vee R) \wedge (\exists x. \sim P)$$

~~$$\Rightarrow \{ I_p: P \Rightarrow Q \}$$~~

$$(\forall x. P \vee R) \wedge (\exists x. \sim Q)$$

Sbagliato, perché la seconda P occorre negativamente



TEOREMA DI DEDUZIONE

- Sappiamo dal CP che per dimostrare che $P \Rightarrow Q$ è una tautologia, basta dimostrare Q usando P come ipotesi
- Ora che abbiamo introdotto le **premesse** di una dimostrazione, possiamo giustificare questa tecnica con il **Teorema di Deduzione**:

$$\begin{array}{c} \Gamma \vdash P \Rightarrow Q \\ \text{se e soltanto se} \\ \Gamma, P \vdash Q \end{array}$$

- Ovvero per dimostrare una implicazione

$$P \Rightarrow Q$$

è possibile costruire una dimostrazione per Q usando sia le leggi generali (formule valide) che P come ipotesi



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 di validità, oppure una dimostrazione che usi solo premesse valide
- Ricordiamo che 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 libere di x in P 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**

- $(\forall x.P) \Rightarrow P[t/x]$ (**elim- \forall**) [t chiuso]
- Poiché non abbiamo visto altre leggi, usiamo la definizione di validità: **elim- \forall** deve essere vera in qualunque interpretazione
- Per assurdo: sia $I = (D, \alpha)$ tale che $I_\rho(\mathbf{elim-}\forall) = F$ (ρ qualunque)
- Per (S6), $I_\rho(\mathbf{elim-}\forall) = F$ sse $I_\rho((\forall x.P)) = T$ e $I_\rho(P[t/x]) = F$
- Se $I_\rho((\forall x.P)) = T$, per (S8) abbiamo: $I_{\rho[d/x]}(P) = T$ per qualunque d in D ...
- ... e quindi in particolare $I_{\rho[\underline{d}/x]}(P) = T$ con $\underline{d} = \alpha_\rho(t)$.
- Ma allora $I_\rho(P[t/x]) = T$, e abbiamo ottenuto una contraddizione
[Abbiamo usato $I_\rho(P[t/x]) = I_{\rho[\underline{d}/x]}(P(x))$, che si può dimostrare per induzione strutturale su t]



LEGGI PER I QUANTIFICATORI (2)

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

○ Esempio

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

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

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

○ **Esercizio:** Dimostrare la validità di (intro- \exists) utilizzando la definizione di validità di una formula, come visto per (elim- \forall).



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)
- $(\exists x. (\exists y.P)) \equiv (\exists y. (\exists x.P))$

Le seguenti leggi valgono solo se si assume che il dominio di interpretazione non sia vuoto:

- $(\forall x.P) \equiv P$ se x non occorre in P (costante)
- $(\exists x.P) \equiv P$ se x non occorre in P
- **Esercizio:** dimostrare la validità delle leggi presentate



LEGGI PER I QUANTIFICATORI (4)

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

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

- $(\forall x.P \vee Q) \equiv (\forall x.P) \vee Q$ se x non compare in Q (Distrib.)
- $(\exists x.P \wedge Q) \equiv (\exists x.P) \wedge Q$ se x non compare in Q (Distrib.)

- **Esercizio:** dimostrare la validità delle leggi presentate



ALTRE LEGGI PER QUANTIFICATORI, DA DIMOSTRARE

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

- $(\forall x.P \vee Q \Rightarrow R) \equiv (\forall x.P \Rightarrow R) \wedge (\forall x.Q \Rightarrow R)$ (Dominio)

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

[suggerimento: sfruttare la legge precedente usando De Morgan]

Le seguenti leggi (Distrib) valgono solo se si assume che il dominio di interpretazione non sia vuoto:

- $(\forall x.P \wedge Q) \equiv (\forall x.P) \wedge Q$ se x non compare in Q (Distrib)

- $(\exists x.P \vee Q) \equiv (\exists x.P) \vee Q$ se x non compare in Q (Distrib)

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

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



LINGUAGGI DEL PRIMO ORDINE CON UGUAGLIANZA

- Considereremo sempre linguaggi del primo ordine **con uguaglianza**, cioè con il simbolo speciale di predicato binario “=” (quindi $= \in P$)
- Il significato di “=” è fissato: per qualunque interpretazione, la formula $\mathbf{t} = \mathbf{t}'$ è vera se e solo se \mathbf{t} e \mathbf{t}' denotano lo stesso elemento del dominio di interesse
- Più formalmente: data un'interpretazione $\mathbf{I} = (\mathbf{D}, \alpha)$ e un assegnamento $\rho: V \rightarrow \mathbf{D}$, abbiamo $\mathbf{I}_\rho(\mathbf{t} = \mathbf{t}') = \mathbf{T}$ (la formula $\mathbf{t} = \mathbf{t}'$ è vera) se $\alpha_\rho(\mathbf{t}) = \alpha_\rho(\mathbf{t}')$ (cioè se le semantiche di \mathbf{t} e \mathbf{t}' coincidono)



LEGGI PER L'UGUAGLIANZA

- Per il predicato di uguaglianza così definito valgono le seguenti leggi:

1) $(\forall x. (\forall y. x = y \Rightarrow (P \equiv P[y/x])))$ (Leibniz)

2) $(\forall x. (\forall y. (x = y \wedge P) \equiv (x = y \wedge P[y/x])))$

3) $(\forall x. (\forall y. (x = y \wedge P) \Rightarrow P[y/x]))$

- $(\forall y. (\forall x. x = y \Rightarrow P) \equiv P[y/x])$ (singoletto)

- $(\forall y. (\exists x. x = y \wedge P) \equiv P[y/x])$

- **Esercizio:** dimostrare che $(1) \equiv (2)$ e $(1) \Rightarrow (3)$



LEGGI PER L'UGUAGLIANZA (2)

- **Attenzione:** spesso (e nella dispensa) queste leggi sono scritte informalmente senza quantificazioni:
- $x = y \Rightarrow (P \equiv P[y/x])$ (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)
- $(\exists x. x = y \wedge P) \equiv P[y/x]$

- **Esercizio:** dimostrare la validità delle leggi presentate usando la definizione del predicato di uguaglianza



REGOLE DI INFERENZA: LA REGOLA DI GENERALIZZAZIONE

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

$$\frac{\Gamma \vdash P[d/x], \text{ con } d \text{ nuova costante}}{\Gamma \vdash (\forall x.P)}$$

- Intuitivamente, d rappresenta un generico elemento del dominio sul quale non possiamo fare alcuna assunzione



REGOLE DI INFERENZA: LA REGOLA DI SKOLEMIZZAZIONE

- Se sappiamo che $(\exists x.P)$ è vera, possiamo usarla per provare una formula Q nella forma $P[d/x]$, dove d è una costante nuova, che non compare in Q :

$$\frac{(\exists x.P) \in \Gamma \quad \Gamma, P[d/x] \vdash Q, \text{ con } d \text{ nuova costante, } d \text{ non occorre in } Q}{\Gamma \vdash Q}$$

- Intuitivamente, è come se chiamassimo d un ipotetico elemento del dominio che testimonia la verità di $(\exists x.P)$

