IL CALCOLO DEL PRIMO ORDINE

Corso di Logica per la Programmazione

A.A. 2010/11

Andrea Corradini, Paolo Mancarella

ANCORA SU 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 $\boldsymbol{\varphi}$ a partire da un insieme di premesse $\boldsymbol{\Gamma}$ è una sequenza di $\boldsymbol{\varphi_1, \ldots, \varphi_n}$ tale che
  - Ogni formula $\boldsymbol{\varphi_i}$ è un elemento di $\boldsymbol{\Gamma}$ oppure è ottenuta applicando una regola di inferenza a partire dalle premesse $\boldsymbol{\Gamma}$ e $\boldsymbol{\varphi_1, \ldots, \varphi_{i-1}}$
  - $\boldsymbol{\varphi_n}$ coincide con $\boldsymbol{\varphi}$
  - Scriviamo $\boldsymbol{\Gamma \vdash \varphi}$ se esiste una dimostrazione di $\boldsymbol{\varphi}$ a partire da $\boldsymbol{\Gamma}$

CALCOLO PROPOSIZONALE 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 princìpi 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 $\boldsymbol{\varphi}$ da un insieme di premesse $\boldsymbol{\Gamma}$ allora $\boldsymbol{\varphi}$ è una conseguenza logica di $\boldsymbol{\Gamma}$, 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 $\boldsymbol{\varphi}$ è una conseguenza logica di un insieme di premesse $\boldsymbol{\Gamma}$, allora esiste una dimostrazione di $\boldsymbol{\varphi}$ da $\boldsymbol{\Gamma}$, 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 Proposizionale 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 ≡

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

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

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)**

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

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

ESEMPI

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

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

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

corretto

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

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

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

sbagliato!

TEOREMA DI DEDUZIONE

- Sappiamo dal CP che per dimostrare che $\mathbf{P \Rightarrow Q}$ 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**:

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

- Ovvero per dimostrare una implicazione

$$P \Rightarrow Q$$

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

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 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 con t
- Esempi:

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

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

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

  $(\forall x.uomo(x) \Rightarrow mortale(x))$

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

  $uomo(Socrate) \Rightarrow mortale(Socrate)$

VALIDITA' DELLA LEGGE **ELIM-∀**

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

  [Abbiamo usato $\mathbf{I}_\rho(P[t/x]) = \mathbf{I}_{\rho[\underline{d}/x]}(P(x))$, 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

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

  $\Rightarrow$ {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 libera in P (costante)
- $(\exists x.P) \equiv P$ se x non occorre libera 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 è libera in Q (Distrib.)
- $(\exists x.P \wedge Q) \equiv (\exists x.P) \wedge Q$ se x non è libera 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 è libera in Q (Distrib)
- $(\exists x.P \vee Q) \equiv (\exists x.P) \vee Q$ se x non è libera in Q (Distrib)

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

LINGUAGGI DEL PRIMO ORDINE CON UGUAGLIANZA

- Considereremo sempre linguaggi del primo ordine **con uguaglianza**, cioè con il simbolo speciale di predicato binario "=" (quindi $= \in \boldsymbol{P}$)

- Il significato di "=" è fissato: per qualunque interpretazione, la formula $\mathbf{t} = \mathbf{t'}$ è vera se e solo se **t** e **t'** denotano lo stesso elemento del dominio di interesse

- Più formalmente: data un'interpretazione $\mathbf{I} = (\boldsymbol{D},\alpha)$ e un assegnamento ρ: $V \rightarrow \boldsymbol{D}$, 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 **t** e **t'** coincidono)

LEGGI PER L'UGUAGLIANZA (=)

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

- $x = y \quad \Rightarrow \quad (P \equiv P[y/x])$ (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]**

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

- 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 **(∃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**:

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

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