Logica per la Programmazione

Lezione 8

- Formule Valide, Conseguenza Logica
- Proof Systems
- Proof System per la Logica del Primo Ordine
- Leggi per i Quantificatori

Logica del Primo Ordine: riassunto

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

Modelli

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

$$\mathcal{I} \models \phi$$

- Se Γ ("Gamma") è un insieme di formule, con

$$\mathcal{I} \models \Gamma$$

  intendiamo che $\mathcal{I}$ è un **modello** di tutte le formule in Γ
- Se una formula ϕ è vera in tutte le interpretazioni si dice che è **valida** (estensione del concetto di tautologia) e scriviamo

$$\models \phi$$

- Se una formula ϕ è vera in almeno una interpretazione si dice che è **soddisfacibile** altrimenti è **insoddisfacibile**

Esempi

- Formula **soddisfacibile**: $p(a)$
  - Basta trovare un'interpretazione che la renda vera. Per esempio: $\mathcal{I} = (\mathcal{D}, \alpha)$, con $\mathcal{D} = \mathbb{N}$ e
    - $\alpha(\mathbf{a}) = 44$
    - $\alpha(\mathbf{p})(\mathbf{x}) = \mathbf{T}$ se $\mathbf{x}$ è pari, $\mathbf{F}$ altrimenti
- Formula **valida** (corrispondono alle **tautologie**):

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

- Formula **insoddisfacibile** (corrispondono alle **contraddizioni**):

$$p(a) \wedge \neg p(a)$$

Conseguenza Logica

- Il concetto di conseguenza logica consente di parametrizzare la validità di una formula ϕ rispetto a un insieme di formule Γ
- Diciamo che ϕ è una conseguenza logica di Γ e scriviamo

$$\Gamma \models \phi$$

se e soltanto se ϕ **è vera in tutti i modelli di** Γ.
In altre parole, se un'interpretazione $\mathcal{I}$ rende vere tutte le formule in Γ (ovvero $\mathcal{I} \models \Gamma$), allora $\mathcal{I}$ rende vera anche ϕ (ovvero $\mathcal{I} \models \phi$)
- Caso Particolare: $\boxed{\emptyset \models \phi}$ se e solo se $\boxed{\models \phi}$, cioè se ϕ è valida

I Sistemi di Dimostrazione (Proof Systems)

- Dato un insieme di formule Φ, un **sistema di dimostrazione** (o **proof system**) per Φ è un insieme di **Regole di Inferenza**
- Ciascuna **Regola di Inferenza** consente di derivare una formula (**conseguenza**) da un insieme di formule dette le (**premesse**)
- Una **Regola di Inferenza** ha la forma

$$\frac{\phi_1, \ldots, \phi_k}{\phi}$$

dove $\phi_1, \ldots, \phi_k$ sono le premesse e ϕ è la conseguenza, e sono tutte formule in Φ

Dimostrazioni

- Una **dimostrazione** di una formula ϕ a partire da un insieme di premesse Γ è una sequenza di formule $\phi_1, \ldots, \phi_n$ tale che
  - Ogni formula $\phi_\mathbf{i}$ è un elemento di Γ oppure è ottenuta applicando una regola di inferenza a partire dalle premesse Γ e $\phi_1, \ldots \phi_{i-1}$
  - ϕ_n coincide con ϕ
- Scriviamo

$$\Gamma \vdash \phi$$

se esiste una dimostrazione di ϕ a partire da Γ

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 $\Gamma \vdash \phi$ allora $\Gamma \models \phi$

- 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 $\Gamma \models \phi$ allora $\Gamma \vdash \phi$

- Quindi completezza e correttezza mettono in relazione un concetto puramente sintattico ($\Gamma \vdash \phi$) con uno semantico ($\Gamma \models \phi$)
- Non ha senso considerare proof system non corretti!!

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 l'implicazione**
- Il Calcolo Proposizionale è corretto ed anche completo, ma non vediamo le dimostrazioni

CP come Proof System: dimostrazione del Complemento

- Quindi: una **dimostrazione** di ϕ a partire da un insieme di premesse Γ è una sequenza $\phi_1, \ldots, \phi_n = \phi$ dove $\phi_i \in \Gamma$ oppure è ottenuta applicando una regola di inferenza a partire da Γ e $\phi_1, \ldots \phi_{i-1}$
- Vediamo come "leggere" le nostre dimostrazioni in questo modo. Γ sono le leggi già dimostrate.

Dimostrazione di $p \vee (\neg p \wedge q) \equiv p \vee q$ (Complemento)

	$p \vee (\neg p \wedge q)$	$\phi_1 = p \vee (\neg p \wedge q) \equiv \underline{p \vee (\neg p \wedge q)}$
$\equiv$	{(Distr.)}	{Regola: (Sost-$\equiv$), applicata a ϕ_1 e (Distr.)}
	$(p \vee \neg p) \wedge (p \vee q)$	$\phi_2 = p \vee (\neg p \wedge q) \equiv \underline{(p \vee \neg p)} \wedge (p \vee q)$
$\equiv$	{(Terzo Escluso)}	{(Sost-$\equiv$), applicata a ϕ_2 e (Terzo Escluso)}
	$\mathbf{T} \wedge (p \vee q)$	$\phi_3 = p \vee (\neg p \wedge q) \equiv \underline{\mathbf{T} \wedge (p \vee q)}$
$\equiv$	{(Unità)}	{(Sost-$\equiv$), applicata a ϕ_3 e (Unità)}
	$(p \vee q)$	$\phi_4 = p \vee (\neg p \wedge q) \equiv (p \vee q)$

- Quindi le nostre dimostrazioni sono una notazione più compatta della definizione generale.

Cosa vedremo del Calcolo del Primo Ordine

- Rivedremo le **Regole di Inferenza** del Calcolo Proposizionale in forma più generale (come proof system con premesse)
  - Per i connettivi logici useremo le leggi del CP
- Estenderemo il proof system alla Logica del Primo Ordine
  - Anche per il primo ordine ci limiteremo alle regole di inferenza che consentono di dimostrare la validità di formule del tipo:
    - $\phi \equiv \psi$
    - $\phi \Rightarrow \psi$
  - Introdurremo **nuove leggi** e **nuove regole di inferenza** per i quantificatori
  - Le regole di inferenza che introdurremo formano un proof system **corretto** per LPO
  - per LPO esistono diversi proof systems **corretti e completi** (come la *deduzione naturale* e il *calcolo dei sequenti*)

Leggi Generali e Ipotesi (1)

- Anche nel calcolo del primo ordine useremo come leggi generali **formule valide** (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:
  $$\Gamma \vdash \phi$$
  - se $\Gamma \vdash \phi$ allora per la correttezza di $\vdash$, $\Gamma \models \phi$, ovvero ϕ è vera in ogni modello $\mathcal{I}$ di Γ
  - poiché ogni interpretazione $\mathcal{I}$ è modello di Γ, ϕ è vera in ogni interpretazione $\mathcal{I}$
  - quindi è **valida**, ovvero
  $$\models \phi$$

Leggi Generali e Ipotesi (2)

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

$$\Gamma \vdash \phi$$

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 sono ipotesi, allora la dimostrazione garantisce che

$$\Gamma_2 \models \phi$$

Generalizzazione del Principio di Sostituzione per $\equiv$

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

- Nota: La generalizzazione consiste nel far riferimento ad un insieme di premesse Γ
- "Se P e Q sono logicamente equivalenti nelle premesse Γ, allora il fatto che R e $R[Q/P]$ sono equivalenti è dimostrabile da Γ"

Generalizzazione dei Principi di Sostituzione per $\Rightarrow$

- Dobbiamo estendere il concetto di occorrenza positiva o negativa alle formule quantificate
  - P occorre positivamente in $(\forall x.P)$ ed in $(\exists x.P)$
-
$$\frac{(P \Rightarrow Q) \in \Gamma \quad P \text{ occorre positivamente in } R}{\Gamma \vdash R \Rightarrow R[Q/P]}$$
-
$$\frac{(P \Rightarrow Q) \in \Gamma \quad P \text{ occorre negativamente in } R}{\Gamma \vdash R[Q/P] \Rightarrow R}$$

Esempi

$$\begin{array}{ll} & (\forall x.P \vee R) \wedge (\exists x.\neg P) \\ \Rightarrow & \{\mathrm{Ip} : P \Rightarrow Q\} \\ & (\forall x.Q \vee R) \wedge (\exists x.\neg P) \end{array}$$

Corretto perché la prima P occorre positivamente

$$\begin{array}{ll} & (\forall x.P \vee R) \wedge (\exists x.\neg P) \\ \Rightarrow & \{\mathrm{Ip} : P \Rightarrow Q\} \\ & (\forall x.Q \vee R) \wedge (\exists x.\neg Q) \end{array}$$

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**:

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

se e solo se

$$\Gamma, P \vdash Q$$

- 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 LPO 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 $(\forall x.P)$ (risp. $(\exists x.P)$) la portata di $\forall x$ (risp. $\exists x$) è la sottoformula P.

Leggi per i Quantificatori: (1)

- (elim-∀)

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

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:

$$\begin{array}{ll} & (\forall x.pari(x) \wedge x > 2 \Rightarrow \neg primo(x)) \\ \Rightarrow & \{(\text{elim} - \forall)\} \\ & pari(7) \wedge 7 > 2 \Rightarrow \neg primo(7) \end{array}$$

$$\begin{array}{ll} & (\forall x.uomo(x) \Rightarrow mortale(x)) \\ \Rightarrow & \{(\text{elim} - \forall)\} \\ & uomo(Socrate) \Rightarrow mortale(Socrate) \end{array}$$

Validità della Legge (elim-$\forall$)

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

Leggi per i Quantificatori (2)

- (intro-$\exists$)

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

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

- Esempio:

$$pari(10) \wedge 10 > 2$$

$$\Rightarrow \qquad \{(\text{intro} - \exists)\}$$

$$(\exists x.pari(x) \wedge x > 2)$$

- **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)

- $$\neg(\forall x.P) \equiv (\exists x.\neg P) \quad \text{(De Morgan)}$$
  $$\neg(\exists x.P) \equiv (\forall x.\neg P)$$

- $$(\forall x.(\forall y.P)) \equiv (\forall y.(\forall x.P)) \quad \text{(Annidamento)}$$
  $$(\exists x.(\exists y.P)) \equiv (\exists y.(\exists x.P))$$

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

  $$(\forall x.P) \equiv P \quad \text{se } x \text{ non occorre in } P$$

  $$(\exists x.P) \equiv P \quad \text{se } x \text{ non occorre in } P$$

- **Esercizio**: Dimostrare la validità delle leggi presentate.

Leggi per i Quantificatori (4)

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

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

- $$(\forall x.P \vee Q) \equiv (\forall x.P) \vee Q \text{ se } x \text{ non occorre in } Q \quad (\textit{Distrib.})$$
  $$(\exists x.P \wedge Q) \equiv (\exists x.P) \wedge Q \text{ se } x \text{ non occorre in } Q \quad (\textit{Distrib.})$$

- **Esercizio**: Dimostrare la validità delle leggi presentate.

Altre Leggi per i Quantificatori, da dimostrare

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

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

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

$$(\forall x.P \wedge Q) \equiv (\forall x.P) \wedge Q \text{ se } x \text{ non occorre in } Q \quad (Distrib.)$$
$$(\exists x.P \vee Q) \equiv (\exists x.P) \vee Q \text{ se } x \text{ non occorre in } Q \quad (Distrib.)$$

- Per esercizio:

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

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

Linguaggio del Primo Ordine con Uguaglianza

- Considereremo sempre linguaggi del primo ordine con uguaglianza, cioè con il simbolo speciale di predicato binario "$=$" (quindi $= \in \mathcal{P}$)
- 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 una interpretazione $\mathcal{I} = (\mathcal{D}, \alpha)$ e un assegnamento $\rho : \mathcal{V} \to \mathcal{D}$, abbiamo $\mathcal{I}_\rho(\mathbf{t} = \mathbf{t}') = \mathbf{T}$ se $\alpha_\rho(\mathbf{t}) = \alpha_\rho(\mathbf{t}')$ (cioè se le semantiche di $\mathbf{t}$ e $\mathbf{t}'$ coincidono), $\mathbf{F}$ altrimenti

Leggi per l'Uguaglianza

- Per il predicato di uguaglianza valgono le seguenti leggi:

$$(1) \quad (\forall x\,.\,(\forall y.x = y \Rightarrow (P \equiv P[y/x]))) \qquad (\textit{Leibniz})$$

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

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

$$(\forall y\,.\,(\forall x.x = y \Rightarrow P) \equiv P[y/x]) \qquad (\textit{singoletto})$$

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

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

Leggi per l'Uguaglianza (2)

- Attenzione: spesso (e nella dispensa) queste leggi sono scritte informalmente *senza* quantificazioni:

$$x = y \Rightarrow (P \equiv P[y/x]) \qquad (\textit{Leibniz})$$

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

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

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 ipotesi

Regole di Inferenza: La Regola di Skolemizzazione

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

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

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