Logica per la Programmazione

Lezione 8

- Formule Valide, Conseguenza Logica
- Proof System per la Logica del Primo Ordine

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 ρ, 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 è un insieme di formule, con

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

  intendiamo $\mathcal{I}$ è un **modello** di per 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**: $\boxed{(\exists x . p(x))}$
  - Basta trovare un'interpretazione che la renda vera. Per esempio: $\mathcal{I} = (\mathcal{D}, \alpha)$, con $\mathcal{D} = \mathbb{N}$ e
    - $\alpha(p)(\mathbf{x}) = \mathbf{T}$ se $\mathbf{x}$ è pari, $\mathbf{F}$ altrimenti
- Formula **valida** (corrispondono alle **tautologie**): $\boxed{(\forall x . p(x) \ \vee \neg p(x))}$
- Formula **insoddisfacibile** (corrispondono alle **contraddizioni**): $\boxed{p(a) \ \wedge \neg p(a)}$

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, ovvero **tutte le interpretazioni** $\mathcal{I}$ che rendono vere tutte le formule in Γ **rendono vera** anche ϕ. Formalmente, se $\mathcal{I} \models \Gamma$ allora $\mathcal{I} \models \phi$
- Caso Particolare: se $\Gamma = \emptyset$ allora $\models \phi$

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 (**conseguenza**) da un insieme di formule dette le (**premesse**)

Una Dimostrazione con Premesse

- 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 ϕ_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 $\Gamma \vdash \phi$

- 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** $\Rightarrow$ le dimostrazioni
- Il Calcolo Proposizionale è corretto ed anche completo

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
  - Introdurremo **nuove leggi** e **nuove regole di inferenza** per i quantificatori
  - Le regole di inferenza che introdurremo formano un proof system **corretto** per LPO ma non **completo**: 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 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 in Γ

- quindi se $\Gamma = \Gamma_1 \cup \Gamma_2$, dove Γ_1 sono formule valide e Γ_2 sono ipotesi, allora la dimostrazione garantisce che

$$\Gamma_2 \models \phi$$

- Ogni interpretazione $\mathcal{I}$ è modello di tutte le formule di $\Gamma_1 \cup \Gamma_2$ sse è modello di tutte le formule di Γ_2

Generalizzazione del Principio di Sostituzione per $\equiv$

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

- 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 conseguenza logica di Γ"

Esempio di dimostrazione nel CP: 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)**

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

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

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

  Corretto perché la prima P occorre positivamente

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

  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