Logica per la Programmazione

Lezione 2

- Dimostrazione di tautologie
- Proof System

Un Problema di Deduzione Logica [da un test di ingresso]

- Tre amici, Antonio, Bruno e Corrado, sono incerti se andare al cinema. Si sa che:
  - Se Corrado va al cinema, allora ci va anche Antonio;
  - Condizione necessaria affinché Antonio vada al cinema è che ci vada Bruno
- Il giorno successivo possiamo affermare con certezza che:
  1. Se Corrado è andato al cinema, allora ci è andato anche Bruno
  2. Nessuno dei tre amici è andato al cinema
  3. Se Bruno è andato al cinema, allora ci è andato anche Corrado
  4. Se Corrado non è andato al cinema, allora non ci è andato nemmeno Bruno
- *Come si formalizza? Come si può usare una dimostrazione per rispondere alla domanda?*

Formalizzazione del Problema di Deduzione Logica

- Tre amici, Antonio, Bruno e Corrado, sono incerti se andare al cinema.
  - Introduciamo tre proposizioni:
    - $A \equiv$ "Antonio va al cinema"
    - $B \equiv$ "Bruno va al cinema'
    - $C \equiv$ "Corrado va al cinema"
- Formalizziamo le premesse
  - Se Corrado va al cinema, allora ci va anche Antonio:
    - $C \Rightarrow A$
- Condizione necessaria affinché Antonio vada al cinema è che ci vada Bruno
    - $A \Rightarrow B$

Calcolo Proposizionale per formalizzare Enunciati: Esempio (cont.)

- Formalizziamo anche le quattro possibili risposte:
  - Se Corrado è andato al cinema, allora ci è andato anche Bruno
    - $C \Rightarrow B$
  - Nessuno dei tre amici è andato al cinema
    - $(\neg A) \wedge (\neg B) \wedge (\neg C)$
  - Se Bruno è andato al cinema, allora ci è andato anche Corrado
    - $B \Rightarrow C$
  - Se Corrado non è andato al cinema, allora non ci è andato nemmeno Bruno
    - $(\neg C) \Rightarrow (\neg B)$
- Per rispondere alla domanda, dobbiamo capire quale di queste quattro proposizioni è **conseguenza logica** delle proposizioni precedenti

Come possiamo essere certi della risposta?

- Scriviamo una formula che formalizza il problema logico nei quattro casi (se la conclusione è conseguenza logica delle premesse):
    1. $((C \Rightarrow A) \wedge (A \Rightarrow B) \Rightarrow (C \Rightarrow B)$
    2. $((C \Rightarrow A) \wedge (A \Rightarrow B)) \Rightarrow ((\neg A) \wedge (\neg B) \wedge (\neg C))$
    3. $((C \Rightarrow A) \wedge (A \Rightarrow B)) \Rightarrow (B \Rightarrow C)$
    4. $((C \Rightarrow A) \wedge (A \Rightarrow B)))) \Rightarrow ((\neg C) \Rightarrow (\neg B))$
- Bisogna determinare quale quale delle seguenti formule è una tautologia (tramite tabelle di verità o trovando un controesempio)
- Chiaramente la (1) è una tautologia, mentre la (2), (3) e la (4) non lo sono !!!!
- Facciamo vedere il caso 3) e lasciamo le altre per esercizio

Come si vede che una Formula non è una Tautologia?

- Esempio: (3) $((C \Rightarrow A) \wedge (A \Rightarrow B)) \Rightarrow (B \Rightarrow C)$
- Basta trovare un'interpretazione che la rende falsa (un controesempio)
  - Determiniamo valori di verità per A, B e C che rendano falsa la formula
  - Poiché è un'implicazione, è falsa solo quando la premessa è vera e la conseguenza è falsa
  - Quindi $(B \Rightarrow C)$ deve essere falso, quindi

$$\{B \mapsto \mathbf{T}, C \mapsto \mathbf{F}\}$$

  - A questo punto si vede che per qualunque valore di A la premessa è vera. Quindi le seguenti interpretazioni rendono la formula falsa:

$$\{A \mapsto \mathbf{T}, B \mapsto \mathbf{T}, C \mapsto \mathbf{F}\} \qquad \{A \mapsto \mathbf{F}, B \mapsto \mathbf{T}, C \mapsto \mathbf{F}\}$$

Dimostrazione di Tautologie

Per dimostrare che una formula è una tautologia possiamo:

- costruire la tabella di verità, sfruttando quella dei connettivi
  - del tutto meccanico, considerando 2^n interpretazioni
- esiste anche un approccio alternativo basato sulla costruzione di una dimostrazione formale usando un proof system
  - la dimostrazione si ottiene applicando delle regole di inferenza
  - esistono vari tipi di proof system in ogni caso la costruzione di una dimostrazione non è un procedimento automatico

Dimostrazione di Tautologie

- Il sistema di dimostrazioni che presenteremo è ispirato alla struttura delle dimostrazioni dell'aritmetica
- Si usano delle leggi che sono tautologie della forma
  - $p \equiv q$ (equivalenze tautologiche)
  - $p \Rightarrow q$ (implicazioni tautologiche)
- *Regola di Inferenza*: il Principio di Sostituzione
- Ma come è strutturata una dimostrazione?
- Cominciamo dall'aritmetica rivisitando una semplice dimostrazione ed analizzandone la struttura

Dimostrazioni: cominciamo dall'Aritmetica

- Mostriamo che $(\mathbf{a}+\mathbf{b})(\mathbf{a}-\mathbf{b}) = \mathbf{a}^2 - \mathbf{b}^2$
  $(\mathbf{a}+\mathbf{b})(\mathbf{a}-\mathbf{b})$
  $=$ {(distributività $(x+y)z = xz + yz$) con a al posto di y, b al posto di z e $(a-b)$ al posto di x}
  $\underline{\mathbf{a}(\mathbf{a}-\mathbf{b})} + \underline{\mathbf{b}(\mathbf{a}-\mathbf{b})}$
  $=$ {(distributività $x(y-z) = xy - xz$), due volte, la prima volta applicata la prima volta con $x = a$, $y = a$, $z = b$ e la seconda con $x = b$, $y = a$, $z = b$}
  $(\underline{\mathbf{aa}} - \mathbf{ab}) + (\mathbf{ba} - \underline{\mathbf{bb}})$
  $=$ {(quadrato $xx = x^2$), due volte, e (associatività) della somma
  $\mathbf{a}^2 \underline{-\mathbf{ab} + \mathbf{ba}} - \mathbf{b}^2$}
  $=$ (commutatività) del prodotto, e (differenza $-x + x = 0$)
  $\underline{\mathbf{a}^2 + \mathbf{0}} - \mathbf{b}^2$
  $=$ {(elemento neutro $x + 0 = x$)}
  $\mathbf{a}^2 - \mathbf{b}^2$

Struttura di una semplice Dimostrazione

- Nella dimostrazione vista abbiamo
  - una sequenza di eguaglianze
    - es: $\mathbf{a^2 + 0 - b^2 = a^2 - b^2}$
- Ogni eguaglianza ha come giustificazione una o più **leggi** (dell'aritmetica)
  - es: $x + 0 = x$ (Elemento neutro)
- La correttezza di ogni eguaglianza è basata su una **regola di inferenza**: il principio di sostituzione. Informalmente:

  "Sostituendo eguali con eguali il valore non cambia"

  - es: instanziando la legge sappiamo che $\mathbf{a^2 + 0 = a^2}$
  - sostituendo $\mathbf{a^2 + 0}$ con $\mathbf{a^2}$ in $\mathbf{a^2 + 0 - b^2}$ otteniamo $\mathbf{a^2 - b^2}$

Principio di Sostituzione: eguaglianza

- Esprime una proprietà fondamentale dell' **eguaglianza**
- Consente di trasformare le espressioni usando le ben note **leggi algebriche**
- **"Se $p = q$ allora il valore di una espressione r in cui compare p non cambia se p è sostituito con q"**
- In formule:

$$r = r[q/p]$$

- Qui $\mathbf{p} = \mathbf{q}$ è una istanza di una legge e $\mathbf{r} = \mathbf{r}[\mathbf{q}/\mathbf{p}]$ è l'eguaglianza da essa giustificata

Principio di Sostituzione: equivalenza

- Nel Calcolo Proposizionale vale una proprietà analoga per l'**equivalenza** ($\equiv$)
- **"Se $P \equiv Q$ allora il valore di una formula R in cui compare P non cambia se P è sostituito con Q"**
- In formule:

$$\mathbf{R \equiv R[Q/P]}$$

dove $P \equiv Q$ è una legge logica (tautologia) e $R[Q/P]$ indica la formula R in cui P viene sostituito con Q

Dimostrazioni di Equivalenze Tautologiche (1)

- Sfruttando il Principio di Sostituzione possiamo fare un passo di dimostrazione
- Se $P \equiv Q$ è una istanza di una legge (tautologia)

$$\begin{array}{ll} & \mathbf{R} \\ \equiv & \{P \equiv Q\} \\ & \mathbf{R[Q/P]} \end{array}$$

- Il passo è corretto Principio di Sostituzione

Dimostrazioni di Equivalenze Tautologiche (2)

- Come per equazioni algebriche si può provare $\mathbf{P_1} \equiv \mathbf{P_n}$ nel modo seguente:

$$
\begin{array}{ll}
 & \mathbf{P_1} \\
\equiv & \quad \{\text{giustificazione}\} \\
 & \mathbf{P_2} \\
 & \ldots \\
 & \mathbf{P_{n-1}} \\
\equiv & \quad \{\text{giustificazione}\} \\
 & \mathbf{P_n}
\end{array}
$$

- Ad ogni passo applichiamo una istanza di una legge (tautologia)
- Ogni passo è corretto per il Principio di Sostituzione patto che la legge applicata sia una (tautologia)

Leggi del Calcolo Proposizionale

- Una **legge** è una tautologia
- Di solito una tautologia viene chiamata "legge" quando descrive importanti proprietà di uno o più connettivi logici e delle relazioni tra loro
- Per ogni legge che introduciamo bisognerebbe verificare che sia una tautologia
  - a volte è ovvio
  - a volte lo mostreremo con tabelle di verità
  - a volte presenteremo una dimostrazione in cui usiamo **solo leggi introdotte in precedenza**
  - spesso lo lasceremo come esercizio...

Leggi per l'Equivalenza

- $P \equiv P$ (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)
- Esempio di dimostrazione: (Unità)

P	$(P$	$\equiv$	$\mathbf{T})$	$\equiv$	P
T	T	T	T	**T**	T
F	F	F	T	**T**	F
	(1)	(2)	(1)	(3)	(1)

Leggi per Congiunzione e Disgiunzione (1)

$$(P \vee Q) \equiv (Q \vee P) \qquad \text{(Commutatività)}$$
$$(P \wedge Q) \equiv (Q \wedge P)$$

$$(P \vee (Q \vee R)) \equiv ((P \vee Q) \vee R) \qquad \text{(Associatività)}$$
$$(P \wedge (Q \wedge R)) \equiv ((P \wedge Q) \wedge R)$$

$$(P \wedge (Q \vee R)) \equiv ((P \wedge Q) \vee (P \wedge R)) \qquad \text{(Distributività)}$$
$$(P \vee (Q \wedge R)) \equiv ((P \vee Q) \wedge (P \vee R))$$

- Esercizio: dimostrare la (Distributività) con le tabelle di verità

Leggi per Congiunzione e Disgiunzione (2)

$$(P \vee P) \equiv P \quad \text{(Idempotenza)}$$
$$(P \wedge P) \equiv P$$

$$(P \wedge \mathbf{T}) \equiv P \quad \text{(Unità)}$$
$$(P \vee \mathbf{F}) \equiv P$$

$$(P \wedge \mathbf{F}) \equiv \mathbf{F} \quad \text{(Zero) (Dominanza)}$$
$$(P \vee \mathbf{T}) \equiv \mathbf{T}$$

- Esercizio: dimostrare alcune leggi con tabelle di verità

Leggi della Negazione

$\neg(\neg P) \equiv P$	(Doppia Negazione)
$(P \vee \neg P) \equiv \mathbf{T}$	(Terzo Escluso)
$(P \wedge \neg P) \equiv \mathbf{F}$	(Contraddizione)
$\neg\mathbf{T} \equiv \mathbf{F}$	(**T: F**)
$\neg\mathbf{F} \equiv \mathbf{T}$	(**F: T**)
$\neg(P \wedge Q) \equiv (\neg P \vee \neg Q)$	(De Morgan)
$\neg(P \vee Q) \equiv (\neg P \wedge \neg Q)$	

- Mostriamo il caso delle leggi di De Morgan tramite tabelle di verità

Esempio: prova delle leggi di De Morgan

- $$\neg(P \wedge Q) \equiv (\neg P \vee \neg Q) \quad \text{(De Morgan)}$$
  $$\neg(P \vee Q) \equiv (\neg P \wedge \neg Q)$$
- Tabella

P	Q	$\neg$	$(P$	$\wedge$	$Q)$	$\equiv$	$(\neg$	P	$\vee$	$\neg$	$Q)$
T	T	F	T	T	T	T	F	T	F	F	T
T	F	T	T	F	F	T	F	T	T	T	F
F	T	T	F	F	T	T	T	F	T	F	T
F	F	T	F	F	F	T	T	F	T	T	F
		(3)	(1)	(2)	(1)	(4)	(2)	(1)	(3)	(2)	(1)

Leggi della Implicazione (1)

- $$(P \Rightarrow Q) \equiv (\neg P \vee Q) \quad \text{(Elim- } \Rightarrow\text{)}$$

- Tabella

P	Q	$(P$	$\Rightarrow$	$Q\ )$	$\equiv$	$(\ \neg$	P	$\vee$	$Q\ )$
T	T	T	T	T	T	F	T	T	T
T	F	T	F	F	T	F	T	F	F
F	T	F	T	T	T	T	F	T	T
F	F	F	T	F	T	T	F	T	F
		(1)	(2)	(1)	(4)	(2)	(1)	(3)	(1)

Leggi della Implicazione (2)

- $$(P \Rightarrow Q) \equiv (\neg P \vee Q) \quad \text{(Elim-} \Rightarrow\text{)}$$
- $$(P \equiv Q) \equiv (P \Rightarrow Q) \wedge (Q \Rightarrow P) \quad \text{(Elim-} \equiv\text{)}$$
- $$(P \Leftarrow Q) \equiv (Q \Rightarrow P) \quad \text{(Elim-} \Leftarrow\text{)}$$

Una Semplice Dimostrazione

Teorema: $(p \vee (q \vee r)) \equiv ((p \vee q) \vee (p \vee r))$

$$
\begin{array}{ll}
 & \underline{(p \vee q)} \vee (p \vee r) \\
\equiv & \quad \{\ (\text{Commutatività})\} \\
 & \underline{(q \vee p) \vee (p \vee r)} \\
\equiv & \quad \{(\text{Associatività})\} \\
 & q \vee (\underline{(p \vee p)} \vee r)) \\
\equiv & \quad \{(\text{Idempotenza})\} \\
 & \underline{q \vee (p \vee r)} \\
\equiv & \quad \{(\text{Associatività})\} \\
 & \underline{(q \vee p)} \vee r \\
\equiv & \quad \{(\text{Commutatività})\} \\
 & \underline{(p \vee q) \vee r} \\
\equiv & \quad \{(\text{Associatività})\} \\
 & p \vee (q \vee r)
\end{array}
$$

Commenti

- La dimostrazione fatta usando le leggi garantisce la correttezza della dimostrazione grazie al *Principio di Sostituzione*
- Nel seguito semplificheremo le dimostrazioni, saltando passi ovvi come l'applicazione di Associatività, Commutatività e Idempotenza

La (1) è una Tautologia (Transitività dell'implicazione)

	$((C \Rightarrow A) \wedge (A \Rightarrow B)) \Rightarrow (C \Rightarrow B)$	
$\equiv$		$\{(\text{Elim.-}\Rightarrow)\}$
	$\neg((C \Rightarrow A) \wedge (A \Rightarrow B)) \vee (C \Rightarrow B)$	
$\equiv$		$\{(\text{Elim.-}\Rightarrow)$, 3 volte$\}$
	$\neg((\neg C \vee A) \wedge (\neg A \vee B)) \vee (\neg C \vee B)$	
$\equiv$		$\{$(De Morgan)$\}$
	$(\neg(\neg C \vee A) \vee \neg(\neg A \vee B)) \vee (\neg C \vee B)$	
$\equiv$		$\{$(De Morgan) 2 volte, (Doppia Neg.)$\}$
	$(C \wedge \neg A) \vee (A \wedge \neg B) \vee (\neg C \vee B)$	
$\equiv$		$\{$(Comm.), (Assoc.)$\}$
	$((C \wedge \neg A) \vee \neg C) \vee ((A \wedge \neg B) \vee B)$	
$\equiv$		$\{$(Distr.) 2 volte$\}$
	$((C \vee \neg C) \wedge (\neg A \vee \neg C)) \vee ((A \vee B) \wedge (\neg B \vee B))$	
$\equiv$		$\{$(Terzo Escluso) 2 volte$\}$
	$(\mathbf{T} \wedge (\neg A \vee \neg C)) \vee ((A \vee B) \wedge \mathbf{T})$	
$\equiv$		$\{$(Unità)$\}$
	$(\neg A \vee \neg C) \vee (A \vee B)$	
$\equiv$		$\{$(Terzo Escluso), (Assoc.)$\}$
	$\mathbf{T} \vee \neg C \vee B$	
$\equiv$		$\{$(Zero)$\}$
	$\mathbf{T}$	

Commenti

- Si può mostrare che tutte le tautologie del Calcolo Proposizionale sono dimostrabili a partire dall'insieme delle leggi visto sinora
- Naturalmente la tecnica non automatizza le dimostrazioni. Rimane a carico nostro la scelta delle leggi da usare, da quale membro della equivalenza partire, l'organizzazione della sequenza dei passaggi
- Conviene comunque, per motivi di espressività e compattezza delle definizioni, introdurre altre leggi derivate che sono molto utili in pratica

Esercizi Proposti: (1)

Dimostrare tramite una dimostrazione per sostituzione che le seguenti formule sono tautologie:

- $(P \Rightarrow Q) \equiv (\neg Q \Rightarrow \neg P)$ (Contropositiva)
- $\neg(P \Rightarrow Q) \equiv P \wedge \neg Q$ ($\neg$-$\Rightarrow$)
- $\neg(P \equiv Q) \equiv (P \equiv \neg Q)$ ($\neg$-$\equiv$)
- $(P \Rightarrow \neg P) \equiv \neg P$
- $((Q \Rightarrow P) \Rightarrow R) \equiv ((P \Rightarrow R) \wedge (\neg Q \Rightarrow R))$

Attenzione: alcune di queste tautologie sono importati leggi logiche derivate che useremo nelle lezioni successive

Esercizi Proposti: (2)

Dimostrare tramite una dimostrazione per sostituzione che le seguenti formule sono tautologie:

- $(P \wedge Q) \Rightarrow Q$ (Sempl-$\wedge$)
- $P \Rightarrow (P \vee Q)$ (Intro-$\vee$)
- $(P \wedge (P \Rightarrow Q)) \Rightarrow Q$ (Modus Ponens)
- $(\neg Q \wedge (P \Rightarrow Q)) \Rightarrow \neg P$ (Modus Tollens)
- $((Q \vee S) \wedge (Q \Rightarrow \neg P)) \Rightarrow (P \Rightarrow S)$
- $((P \equiv Q) \wedge (Q \equiv R)) \Rightarrow (P \equiv R)$ (Proprieta Transitiva)
- $((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)$ (Proprieta Transitiva)

Attenzione: alcune di queste tautologie sono importati leggi logiche che useremo nelle lezioni successive

Esercizi: Formalizzazione di Enunciati

Formalizzare i seguenti asserti (introducendo opportune variabili proposizionali):

- Piove e fa freddo
- Fa freddo ma non piove
- Se ci sono le nuvole e non c'è vento, allora piove
- Piove solo se ci sono le nuvole e non c'è vento
- Piove se ci sono le nuvole e non c'è vento
- Se piove e non hai l'ombrello, ti bagni
- Se piove allora hai l'ombrello oppure ti bagni