Logica per la Programmazione

Lezione 2

- Dimostrazione di Tautologie
  - Tabelle di Verità
  - Dimostrazioni per sostituzione
  - Leggi del Calcolo Proposizionale
- Insiemi funzionalmente completi di connettivi

Dimostrazione di Tautologie

Abbiamo detto che: Per dimostrare che P è una tautologia possiamo:

- Usare le tabelle di verità, sfruttando quelle dei connettivi
  - Del tutto meccanico, richiede di considerare 2^n casi, dove n è il numero di variabili proposizionali in P
- Cercare di costruire una dimostrazione
  - Usando delle leggi (tautologie già dimostrate)
  - Usando opportune *regole di inferenza*
  - Si possono impostare vari tipi di dimostrazioni
- Mostrare che non è una tautologia
  - individuando valori delle variabili proposizionali che rendono falsa P

Vediamo come si costruiscono le tabelle di verità

Interpretazione di una Formula Proposizionale

- **Interpretazione**: funzione da variabili proposizionali a $\{0, 1\}$
  Nota: useremo F e T nelle formule, ma **0** e **1** per *falso* e *vero* nella semantica
- Esempio: $\Rightarrow$ LAVAGNA
  - Formula $(P \wedge Q) \vee \neg R$
  - Interpretazione $\{P \mapsto 1, Q \mapsto 0, R \mapsto 0\}$
- Si può calcolare il valore di verità della formula nell'interpretazione usando le tavole di verità dei connettivi logici:

P	Q	R	$((P$	$\wedge$	$Q)$	$\vee$	$\neg$	$R)$
1	0	0	1	0	0	**1**	1	0
			(1)	(2)	(1)	**(3)**	(2)	(1)

P	Q	$\neg P$	$P \wedge Q$	$P \vee Q$	$P \Rightarrow Q$	$P \equiv Q$	$P \Leftarrow Q$
1	1	0	1	1	1	1	1
1	0	0	0	1	0	0	1
0	1	1	0	1	1	0	0
0	0	1	0	0	1	1	1

Tabella di verità di una formula proposizionale

- La tabella di verità raccoglie tutte le possibili interpretazioni
- Un esempio: $((P \wedge Q) \vee \neg R)$

P	Q	R	$((P$	$\wedge$	$Q)$	$\vee$	$\neg$	$R)$
1	1	1	1	1	1	**1**	0	1
1	1	0	1	1	1	**1**	1	0
1	0	1	1	0	0	**0**	0	1
1	0	0	1	0	0	**1**	1	0
0	1	1	0	0	1	**0**	0	1
0	1	0	0	0	1	**1**	1	0
0	0	1	0	0	0	**0**	0	1
0	0	0	0	0	0	**1**	1	0
			(1)	(2)	(1)	(3)	(2)	(1)

Dimostrazione di Tautologie

Abbiamo detto che: Per dimostrare che P è una tautologia possiamo:

- Usare le tabelle di verità, sfruttando quelle dei connettivi
  - Del tutto meccanico, richiede di considerare 2^n casi, dove n è il numero di variabili proposizionali in P
- **Cercare di costruire una dimostrazione**
  - **Usando delle leggi (tautologie già dimostrate)**
  - **Usando opportune regole di inferenza**
  - **Si possono impostare vari tipi di dimostrazioni**
- Mostrare che non è una tautologia
  - individuando valori delle variabili proposizionali che rendono falsa P

Dimostrazioni per Sostituzione: cominciamo dall'Aritmetica

- Mostriamo che $(\mathbf{a}+\mathbf{b})(\mathbf{a}-\mathbf{b}) = \mathbf{a}^2 - \mathbf{b}^2$ $\Rightarrow$ LAVAGNA

  $(\mathbf{a}+\mathbf{b})(\mathbf{a}-\mathbf{b})$

  $=$ (distributività $(x+y)z = xz + yz$) con sostituzione $\{\, x \mapsto a, y \mapsto b, z \mapsto (a-b) \,\}$

  $\underline{\mathbf{a}(\mathbf{a}-\mathbf{b})} + \underline{\mathbf{b}(\mathbf{a}-\mathbf{b})}$

  $=$ (distributività $x(y-z) = xy - xz$), due volte, la prima volta con sostituzione $\{\, x \mapsto a, y \mapsto a, z \mapsto b \,\}$ e la seconda con $\{\, x \mapsto b, y \mapsto a, z \mapsto b \,\}$

  $(\underline{\mathbf{aa}} - \mathbf{ab}) + (\mathbf{ba} - \underline{\mathbf{bb}})$

  $=$ (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: $\mathbf{a}^2 + \mathbf{0} - \mathbf{b}^2 = \mathbf{a}^2 - \mathbf{b}^2$
- ogni eguaglianza ha come giustificazione una o più **leggi** (dell'aritmetica)
  - es: $x + 0 = x$
- 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: dalla legge (con sostituzione $\{x \mapsto \mathbf{a}^2\}$) sappiamo che $\mathbf{a}^2 + \mathbf{0} = \mathbf{a}^2$
  - quindi per il principio di sostituzione abbiamo $\underline{\mathbf{a}^2 + \mathbf{0}} - \mathbf{b}^2 = \underline{\mathbf{a}^2} - \mathbf{b}^2$

Principio di Sostituzione

- Esprime una proprietà fondamentale dell'**eguaglianza**.
- **"Se sappiamo che $A = B$, allora il valore di una espressione C in cui compare A non cambia se A è sostituito con B"**
- in formule, $$\frac{A = B}{C = C[^B/_A]}$$
- Qui $A = B$ è una legge, e $C = C[B/A]$ è l'eguaglianza da essa giustificata, grazie al principio di sostituzione
- Nel Calcolo Proposizionale esprime una proprietà dell'**equivalenza**:

$$\boxed{\frac{P \equiv Q}{R \equiv R[^Q/_P]}}$$

- A volte scriviamo R_P^Q per $R[^Q/_P]$

Leggi del Calcolo Proposizionale

- Una **legge** è una tautologia.
- Di solito una tautologia viene chiamata “legge” quando descrive una proprietà di uno o più connettivi logici, o quando è usata come giustificazione nelle dimostrazioni.
- 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)
- $(p \equiv q) \wedge (q \equiv r) \Rightarrow (p \equiv r)$ (Transitività)
- Esempio di dimostrazione: (Unità), (Transitività)

P	$(P$	$\equiv$	$\mathbf{T})$	$\equiv$	P
1	1	1	1	**1**	1
0	0	0	1	**1**	0
	(1)	(2)	(1)	(3)	(1)

Leggi per Congiunzione e Disgiunzione

$p \vee q \equiv q \vee p$	(Commutatività)
$p \wedge q \equiv q \wedge p$	
$p \vee (q \vee r) \equiv (p \vee q) \vee r$	(Associatività)
$p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$	
$p \vee p \equiv p$	(Idempotenza)
$p \wedge p \equiv p$	
$p \wedge \mathbf{T} \equiv p$	(Unità)
$p \vee \mathbf{F} \equiv p$	
$p \wedge \mathbf{F} \equiv \mathbf{F}$	(Zero) (Dominanza)
$p \vee \mathbf{T} \equiv \mathbf{T}$	
$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	(Distributività)
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	

- Esercizio: dimostrare alcune leggi con tabelle di verità

Dimostrazioni di Equivalenze Tautologiche

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

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

- dove ogni passo ha la seguente forma, in cui $P \equiv Q$ è una legge:

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

- Ogni passo è corretto per il *Principio di Sostituzione*

Una Semplice Dimostrazione ⇒ Lavagna

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

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

Commenti

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

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)
$\neg(p \wedge q) \equiv \neg p \vee \neg q$	(De Morgan)
$\neg(p \vee q) \equiv \neg p \wedge \neg q$	
$\neg\mathbf{T} \equiv \mathbf{F}$	(**T: F**)
$\neg\mathbf{F} \equiv \mathbf{T}$	(**F: T**)

- Esercizio: dimostrare alcune leggi con tabelle di verità

Leggi di eliminazione

- $(p \Rightarrow q) \equiv (\neg p \vee q)$ (Elim-$\Rightarrow$)
- $\neg(p \Rightarrow q) \equiv (p \wedge \neg q)$ ($\neg$-$\Rightarrow$)

- $(p \equiv q) \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$ (Elim-$\equiv$)
- $(p \equiv q) \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$ (Elim-$\equiv$-bis)

- $(p \Leftarrow q) \equiv (q \Rightarrow p)$ (Elim- $\Leftarrow$)

Sulle Leggi del Calcolo Proposizionale

- Abbiamo visto le leggi per l'equivalenza ($\equiv$), la congiunzione ($\wedge$), la disgiunzione ($\vee$), la negazione ($\neg$)
- Poi abbiamo visto le leggi per eliminare implicazione ($\Rightarrow$), conseguenza ($\Leftarrow$) ed equivalenza ($\equiv$)
- Si può mostrare che tutte le tautologie del Calcolo Proposizionale sono dimostrabili a partire dall'insieme delle leggi visto sinora
- Conviene comunque, per motivi di espressività e compattezza delle definizioni, introdurre altre leggi che corrispondono, per esempio, ad assodate tecniche di dimostrazione

Insiemi Funzionalmente Completi di Connettivi Logici

- Abbiamo introdotto 6 diversi connettivi logici:

Connettivo	Forma simbolica	Operazione corrispondente
not	$\neg p$	*negazione*
and, *e*	$p \wedge q$	*congiunzione*
or, *o*	$p \vee q$	*disgiunzione*
se p allora q	$p \Rightarrow q$	*implicazione*
p se e solo se q	$p \equiv q$	*equivalenza*
p se q	$p \Leftarrow q$	*conseguenza*

- Alcuni possono essere definiti in termini di altri.
- Molti sottoinsiemi sono "funzionalmente completi" cioè permettono di derivare tutti gli altri.
- Vediamo che $\{\wedge, \neg\}$ è funzionalmente completo.
- Esercizio: dimostrare che anche $\{\vee, \neg\}$ e $\{\Rightarrow, \neg\}$ sono funzionalmente completi.

L'Insieme $\{\wedge, \neg\}$ è funzionalmente completo

- Occorre mostrare che una qualunque formula proposizionale è equivalente a una formula che contiene solo $\{\wedge, \neg\}$.
- Per induzione strutturale sulla sintassi delle formule
  - Ricordiamo la sintassi:

$$\begin{array}{lcl} Prop & ::= & Prop \equiv Prop \mid Prop \wedge Prop \mid Prop \vee Prop \mid \\ & & Prop \Rightarrow Prop \mid Prop \ \Leftarrow \ Prop \\ & & Atom \mid \neg Atom \\ Atom & ::= & \mathbf{T} \mid \mathbf{F} \mid Ide \mid (Prop) \\ Ide & ::= & p \mid q \mid \ldots \mid P \mid Q \mid \ldots \end{array}$$

  - implicazione ($\Rightarrow$), conseguenza ($\Leftarrow$) ed equivalenza ($\equiv$): facile!
  - disgiunzione:

$$\begin{array}{ll} & p \vee q \\ \equiv & \qquad\qquad \{(\text{Doppia Neg.})\} \\ & \neg\neg(p \vee q) \\ \equiv & \qquad\qquad \{(\text{De Morgan})\} \\ & \neg(\neg p \wedge \neg q) \end{array}$$

Il Connettivo "NAND"

- Si consideri il connettivo proposizionale binario **nand** la cui semantica è definita dalla seguente tabella di verità:

P	Q	P **nand** Q
0	0	1
0	1	1
1	0	1
1	1	0

- Esercizio: si provi che l'insieme $\{$**nand**$\}$ è **funzionalmente completo**.