Logica per la Programmazione

Lezione 5

- Dimostrazioni e Tautologie, Ipotesi non tautologiche
  - Tautologie come schemi di dimostrazione
  - Dimostrazioni con ipotesi non tautologiche

Tecniche di Dimostrazione come Tautologie: Dimostrazione per Assurdo

Alcune tautologie schematizzano delle tecniche di dimostrazione valide (alcune conosciute dalla scuola)

Dimostrazione per Assurdo: *Per dimostrare P basta mostrare che negando P si ottiene una contraddizione*

$$P \equiv (\neg P \Rightarrow \mathbf{F})$$

Dimostrazione per Assurdo (2): *Per mostrare che P (ipotesi) implica Q (tesi) basta mostrare che se vale P e si nega Q si ottiene una contraddizione*

$$P \Rightarrow Q \equiv (P \ \wedge \neg Q \Rightarrow \mathbf{F})$$

Mostriamo che sono tautologie

Dimostrazione per Assurdo come Tautologia

- $P \equiv (\neg P \Rightarrow \mathbf{F})$ *(Dimostrazione per Assurdo)*

$$
\begin{array}{ll}
 & (\neg P \Rightarrow \mathbf{F}) \\
\equiv & \qquad \{(\text{Elim.-}\Rightarrow) \text{ e } (\text{Doppia Neg.})\} \\
 & (P \vee \mathbf{F}) \\
\equiv & \qquad \{(\text{Unità})\} \\
 & P
\end{array}
$$

- $P \Rightarrow Q \equiv (P \wedge \neg Q \Rightarrow \mathbf{F})$ *(Dimostrazione per Assurdo (2))*

$$
\begin{array}{ll}
 & (P \wedge \neg Q \Rightarrow \mathbf{F}) \\
\equiv & \qquad \{(\text{Elim.-}\Rightarrow)\} \\
 & \neg(P \wedge \neg Q) \vee \mathbf{F} \\
\equiv & \qquad \{(\text{De Morgan}) \text{ e } (\text{Doppia neg.})\} \\
 & (\neg P \vee Q) \vee \mathbf{F} \\
\equiv & \qquad \{(\text{Unità})\} \\
 & (\neg P \vee Q) \\
\equiv & \qquad \{(\text{Elim.-}\Rightarrow)\} \\
 & P \Rightarrow Q
\end{array}
$$

Esempio di Dimostrazione per Assurdo

Dimostriamo per assurdo $(P \vee Q \Rightarrow R) \Rightarrow (P \Rightarrow R)$
Essendo un'implicazione, usiamo (Dimostrazione per Assurdo (2)), quindi dimostriamo $(P \vee Q \Rightarrow R) \wedge \neg(P \Rightarrow R) \Rightarrow \mathbf{F}$

$$
\begin{array}{lll}
 & (P \vee Q \Rightarrow R) \wedge \neg(P \Rightarrow R) & \\
\equiv & & \{(\text{Elim.-}\Rightarrow),\ (\neg\text{-}\Rightarrow)^*\} \\
 & (\neg(P \vee Q) \vee R) \wedge (P \wedge \neg R) & \\
\equiv & & \{(\text{De Morgan})\} \\
 & ((\neg P \wedge \neg Q) \vee R) \wedge \neg R \wedge P & \\
\equiv & & \{(\text{Complemento})\} \\
 & (\neg P \wedge \neg Q) \wedge \neg R \wedge P & \\
\equiv & & \{\text{ ``Riarrangiamento dei termini'' }\} \\
 & (\neg P \wedge P) \wedge \neg Q \ \ \wedge \neg R & \\
\equiv & & \{(\text{Contraddizione})\text{ e }(\text{Zero})\ \} \\
 & \mathbf{F} &
\end{array}
$$

(*) Legge $(\neg\text{-}\Rightarrow)$: $\neg(A \Rightarrow B) \equiv \neg(\neg A \vee B) \equiv (A \wedge \neg B)$

Altre Tecniche di Dimostrazione come Tautologie

Dimostrazione per **Controposizione:**
Per dimostrare $P \Rightarrow Q$, basta mostrare che $\neg Q \Rightarrow \neg P$

- $P \Rightarrow Q \equiv \neg Q \Rightarrow \neg P$ (Controposizione)

Dimostrazione per **Casi:**
Per dimostrare Q, basta mostrare che per un certo P, valgono sia $P \Rightarrow Q$ che $\neg P \Rightarrow Q$

- $(P \Rightarrow Q) \wedge (\neg P \Rightarrow Q) \equiv Q$ (Dim. per casi)

Per dimostrare che $P \wedge R \Rightarrow Q \wedge S$, basta fornire due prove separate per $P \Rightarrow Q$ e per $R \Rightarrow S$

- $(P \Rightarrow Q) \wedge (R \Rightarrow S) \Rightarrow (P \wedge R \Rightarrow Q \wedge S)$ (Sempl-$\Rightarrow$)

Tautologie corrispondenti a Tecniche di Dimostrazione

- $(P \Rightarrow Q) \equiv (\neg Q \Rightarrow \neg P)$ *(Controposizione)*

$$
\begin{array}{cll}
 & \neg Q \Rightarrow \neg P & \\
\equiv & & \{(\text{Elim.-}\Rightarrow) \text{ e } (\text{Doppia Neg.})\} \\
 & Q \vee \neg P & \\
\equiv & & \{(\text{Elim.-}\Rightarrow)\} \\
 & P \Rightarrow Q &
\end{array}
$$

- $(P \Rightarrow Q) \wedge (\neg P \Rightarrow Q) \equiv Q$ *(Dimostrazione per Casi)*

$$
\begin{array}{cll}
 & (P \Rightarrow Q) \wedge (\neg P \Rightarrow Q) & \\
\equiv & & \{(\text{Elim.-}\Rightarrow) \text{ e } (\text{Doppia Neg.})\} \\
 & (\neg P \vee Q) \wedge (P \vee Q) & \\
\equiv & & \{(\text{Distr.}), \text{ al contrario}\} \\
 & (\neg P \wedge P) \vee Q & \\
\equiv & & \{(\text{Contrad.}) \text{ e } (\text{Unità})\} \\
 & Q &
\end{array}
$$

Tautologie corrispondenti a Tecniche di Dimostrazione (2)

- $(P \Rightarrow Q) \wedge (R \Rightarrow S) \Rightarrow (P \wedge R \Rightarrow Q \wedge S)$ *(Sempl-⇒)*

$$
\begin{array}{ll}
 & (P \Rightarrow Q) \wedge (R \Rightarrow S) \\
\equiv & \{(\text{Elim-}\Rightarrow),\ 2\ \text{volte}\} \\
 & (\neg P \vee Q) \wedge (\neg R \vee S) \\
\Rightarrow & \{(\text{Intro-}\vee),\ \text{due volte, occorrenze positive}\} \\
 & (\neg P \vee \neg R \vee Q) \wedge (\neg P \vee \neg R \vee S) \\
\equiv & \{(\text{Distributività}),\ \text{al contrario}\} \\
 & (\neg P \vee \neg R) \vee (Q \wedge S) \\
\equiv & \{(\text{De Morgan}),\ \text{al contrario}\} \\
 & \neg(P \wedge R) \vee (Q \wedge S) \\
\equiv & \{(\text{Elim.-}\Rightarrow),\ \text{al contrario}\} \\
 & P \wedge R \Rightarrow Q \wedge S
\end{array}
$$

Da Dimostrazioni a Tautologie

- Vediamo come le dimostrazioni che abbiamo introdotto corrispondono a tautologie
- Consideriamo un generico passo di dimostrazione:

$$\boxed{\begin{array}{lll} & P & \\ \equiv & & \{G\} \\ & Q & \end{array}}$$

- Il passo è corretto se e solo se la formula $\boxed{G \Rightarrow (P \equiv Q)}$ è una **tautologia** (usando il **Teorema di Deduzione**, che vedremo)
- Poiché G è una legge, $G \equiv \mathbf{T}$, da cui segue che $\boxed{P \equiv Q}$ è una tautologia. (Si verifichi la legge $\mathbf{T} \Rightarrow A \equiv A$)
- Analog., $\boxed{\begin{array}{lll} & P & \\ \Rightarrow & & \{G\} \\ & Q & \end{array}}$ sse $\boxed{G \Rightarrow (P \Rightarrow Q)}$ sse $\boxed{P \Rightarrow Q}$

Da Dimostrazioni a Tautologie (2)

- E se abbiamo più passi di dimostrazione?
- Sia $conn_i \in \{\equiv, \Rightarrow\}$. Allora $\boxed{\begin{array}{lcl} & P & \\ conn_1 & & \{G_1\} \\ & Q & \\ conn_2 & & \{G_2\} \\ & R & \end{array}}$ sse

  $\boxed{(G_1 \Rightarrow (P\ conn_1\ Q)) \wedge (G_2 \Rightarrow (Q\ conn_2\ R))}$
- Poiché G_1 e G_2 sono tautologie (e $(\mathbf{T} \Rightarrow A \equiv A)$), abbiamo $(G_1 \Rightarrow (P\ conn_1\ Q)) \wedge (G_2 \Rightarrow (Q\ conn_2\ R)) \equiv (P\ conn_1\ Q) \wedge (Q\ conn_2\ R)$
- Se $conn_1$ e $conn_2$ rappresentano lo stesso connettivo e il connettivo è transitivo (come lo sono $\equiv$ e $\Rightarrow$), dalla prova segue che

$$P\ conn\ R$$

come richiedeva la nostra intuizione

Uso di Ipotesi non Tautologiche come Giustificazioni

- Riassumendo: per dimostrare che da una ipotesi P segue una conseguenza Q, possiamo dimostrare che
  - $P \Rightarrow Q$ è una tautologia
  - $\neg Q \Rightarrow \neg P$ è una tautologia
  - $P \wedge \neg Q \Rightarrow \mathbf{F}$ è una tautologia
- **Strategia alternativa**: per dimostrare $P \Rightarrow Q$, partiamo da Q e cerchiamo di dimostrare che è vero sotto l'ipotesi, da usare come giustificazione in qualche passaggio, che P sia vero.
- Ricordiamoci infatti che il caso critico dell'implicazione $P \Rightarrow Q$ è dimostrare che Q è vero quando P è vero. Quando P è falso l'implicazione vale sempre.

Uso di Ipotesi come Giustificazioni: Esempio 1

- Teorema: $P \Rightarrow (P \wedge Q \equiv Q)$
- Dimostrazione: proviamo che $(P \wedge Q \equiv Q)$ è vera nell'ipotesi che P sia vera:

$$
\begin{array}{cll}
 & P \wedge Q & \\
\equiv & & \{\textbf{Ip}: P\} \\
 & \mathbf{T} \wedge Q & \\
\equiv & & \{(\text{Unità})\} \\
 & Q &
\end{array}
$$

- Nelle giustificazioni abbiamo indicato esplicitamente con "**Ip**: ..." il fatto che P è un'ipotesi e non una tautologia

Uso di Ipotesi come Giustificazioni: Esempio 2

- Teorema: $(P \Rightarrow (Q \equiv R)) \Rightarrow (P \wedge R \Rightarrow Q)$
- Dimostrazione: proviamo che $(P \wedge R \Rightarrow Q)$ è vera nell'ipotesi che $(P \Rightarrow (Q \equiv R))$ sia vera:

$$
\begin{array}{lll}
 & P \wedge R & \\
\Rightarrow & & \{\textbf{Ip}: (P \Rightarrow (Q \equiv R)),\ P \text{ occorre pos.}\} \\
 & (Q \equiv R) \wedge R & \\
\equiv & & \{(\text{Elim.-}\equiv)\} \\
 & (Q \Rightarrow R) \wedge (R \Rightarrow Q) \wedge R & \\
\Rightarrow & & \{(\text{Modus Ponens}),\ (R \Rightarrow Q) \wedge R \text{ occ. pos.}\} \\
 & (Q \Rightarrow R) \wedge Q & \\
\Rightarrow & & \{\text{Sempl.-}\wedge\text{, occ. pos.}\} \\
 & Q &
\end{array}
$$

In conclusione

Lo schema di dimostrazione:

$$
\begin{array}{lll}
 & P_1 & \\
conn_1 & & \{G_1\} \\
 & P_2 & \\
conn_2 & & \{G_2\} \\
 & \ldots & \\
 & P_{n-1} & \\
conn_{n-1} & & \{G_{n-1}\} \\
 & P_n &
\end{array}
$$

rappresenta una dimostrazione della seguente tautologia:

$$
(G_1 \Rightarrow (P_1 \ conn_1 \ P_2)) \wedge (G_2 \Rightarrow (P_2 \ conn_2 \ P_3)) \wedge \ldots
$$

$$
\wedge (G_{n-1} \Rightarrow (P_{n-1} \ conn_{n-1} \ P_n))
$$

In conclusione (cont.)

- Supponiamo poi che le proprietà di $conn_1$, ... $conn_{n-1}$, consentono di dimostrare $(P_1 \ conn \ P_n)$
- Allora abbiamo

$$(G_1 \Rightarrow (P_1 \ conn_1 \ P_2)) \wedge (G_2 \Rightarrow (P_2 \ conn_2 \ P_3)) \wedge \ldots$$

$$\wedge (G_{n-1} \Rightarrow (P_{n-1} \ conn_{n-1} \ P_n))$$

$$\Rightarrow (G_1 \wedge \ldots \wedge G_{n-1} \Rightarrow P_1 \ conn \ P_n)$$

- Se H implica la (o è equivalente alla) congiunzione di tutte le ipotesi usate come giustificazioni, ovvero $H \Rightarrow G_1 \wedge \ldots \wedge G_{n-1}$, abbiamo una dimostrazione di

$$H \Rightarrow P_1 \ conn \ P_n$$

- Se le giustificazioni G_1, ... , G_{n-1} sono tutte tautologie, allora abbiamo una dimostrazione di

$$P_1 \ conn \ P_n$$

Esempio: Sillogismo Disgiuntivo

Dimostrare la seguente tautologia usando giustificazioni non tautologiche

- $(P \vee Q) \wedge (P \Rightarrow R) \wedge (Q \Rightarrow S) \Rightarrow (R \vee S)$ (Sillogismo disgiuntivo)

Anticipiamo la legge

$$\boxed{A \Rightarrow (B \Rightarrow C) \equiv (A \wedge B \Rightarrow C) \qquad \text{(Sempl. Sinistra 2-}\Rightarrow\text{)}}$$

Quindi è sufficiente dimostrare che

$$(P \Rightarrow R) \wedge (Q \Rightarrow S) \Rightarrow ((P \vee Q) \Rightarrow (R \vee S))$$

$$\begin{array}{lll}
 & P \vee Q & \\
\Rightarrow & & \{\textbf{Ip}\text{: } (P \Rightarrow R),\ P^{+} \text{ (cioè } P \text{ occorre pos.)}\} \\
 & R \vee Q & \\
\Rightarrow & & \{\textbf{Ip}\text{: } (Q \Rightarrow S),\ Q^{+} \text{ (cioè } Q \text{ occorre pos.)}\} \\
 & R \vee S &
\end{array}$$

Esempio: (Sempl.-$\Rightarrow$)

Dimostrare la seguente tautologia usando giustificazioni non tautologiche

- $(P \Rightarrow Q) \wedge (R \Rightarrow S) \Rightarrow (P \wedge R \Rightarrow Q \wedge S)$ (Sempl.-$\Rightarrow$)

$$
\begin{array}{ll}
 & P \wedge R \\
\Rightarrow & \qquad \{\textbf{Ip}:\ (P \Rightarrow Q),\ P^{+}\} \\
 & Q \wedge R \\
\Rightarrow & \qquad \{\textbf{Ip}:\ (R \Rightarrow S),\ R^{+}\} \\
 & Q \wedge S
\end{array}
$$

Esempio: Dimostrazione per Casi

Dimostrare $(P \vee Q \Rightarrow R) \Rightarrow (P \Rightarrow R)$.
Per (Dimostrazione per Casi), basta mostrare separatamente
$Q \Rightarrow((P \vee Q \Rightarrow R) \Rightarrow (P \Rightarrow R))$ e $\neg Q \Rightarrow((P \vee Q \Rightarrow R) \Rightarrow (P \Rightarrow R))$.
Lo facciamo usando Q e $\neg Q$ come ipotesi non tautologiche.

Caso Q

$$
\begin{array}{lll}
 & P \vee Q \Rightarrow R & \\
\equiv & & \{ \textbf{Ip}\text{: } Q \} \\
 & P \vee \mathbf{T} \Rightarrow R & \\
\equiv & & \{ \text{(Zero), (Elim.-}\Rightarrow\text{)} \} \\
 & \neg \mathbf{T} \vee R & \\
\equiv & & \{ (\mathbf{T}\text{:}\mathbf{F}), \text{(Unità)} \} \\
 & R & \\
\Rightarrow & & \{ \text{(Intro.-}\vee\text{)} \} \\
 & \neg P \vee R & \\
\equiv & & \{ \text{(Elim.-}\Rightarrow\text{)} \} \\
 & P \Rightarrow R &
\end{array}
$$

Caso $\neg Q$

$$
\begin{array}{lll}
 & P \vee Q \Rightarrow R & \\
\equiv & & \{ \textbf{Ip}\text{: } \neg Q \} \\
 & P \vee \mathbf{F} \Rightarrow R & \\
\equiv & & \{ \text{(Unità)} \} \\
 & P \Rightarrow R &
\end{array}
$$

Altre Tautologie che rappresentano Tecniche di Dimostrazione

- $(P \Rightarrow \neg P) \equiv \neg P$ (Riduzione ad Assurdo)
- $P \wedge Q \Rightarrow R \equiv P \wedge \neg R \Rightarrow \neg Q$ (Scambio)
- $((P \Rightarrow Q) \wedge \neg Q) \Rightarrow \neg P$ (Tollendo Tollens)
- $(P \equiv Q) \equiv (P \wedge Q) \vee (\neg P \wedge \neg Q)$ (Elim.-$\equiv$-bis)
- $(P \Rightarrow Q) \wedge (P \Rightarrow R) \equiv (P \Rightarrow Q \wedge R)$ (Sempl.Destra-$\Rightarrow$)
- $(P \Rightarrow Q) \vee (P \Rightarrow R) \equiv (P \Rightarrow Q \vee R)$
- $(P \Rightarrow R) \wedge (Q \Rightarrow R) \equiv (P \vee Q \Rightarrow R)$ (Sempl.Sinistra-$\Rightarrow$)
- $(P \Rightarrow R) \vee (Q \Rightarrow R) \equiv (P \wedge Q \Rightarrow R)$
- $P \Rightarrow (Q \Rightarrow R) \equiv (P \wedge Q \Rightarrow R)$ (Sempl.Sinistra-2–$\Rightarrow$)
- Esercizio: dimostrare che sono tautologie