Logica per la Programmazione

Lezione 6

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

Tecniche di Dimostrazione come Tautologie

- Alcune ben note tecniche di dimostrazione possono essere formalizzate come tautologie (alcune conosciute dalla scuola)
- Dimostrazione per assurdo e per casi
- Dimostrazione per contraposizione

Tecniche di Dimostrazione come Tautologie: Dimostrazione per Assurdo

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)*

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

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

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

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)*

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

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

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

Tautologie corrispondenti a Tecniche di Dimostrazione (2)

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

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

Dimostrazioni con Ipotesi Non Tautologiche

- Vedremo come il sistema di dimostrazioni che abbiamo presentato possa essere esteso utilizzando nei passaggi deduttivi formule che non sono leggi (tautologie)
- Tali formule diventano le Ipotesi non Tautologiche della dimostrazione
- Intuitivamente questa tecnica di prova si usa per dimostrare implicazioni tautologiche della forma:

$$H_1 \wedge \ldots \wedge H_n \;\Rightarrow\; G$$

Un Passo di Dimostrazione

- Consideriamo un generico passo di dimostrazione con $conn \in \{\equiv, \Rightarrow\}$:

$$\begin{array}{lll} & R & \\ conn & & \{P \; conn \; Q\} \\ & R[Q/P] & \end{array}$$

- Usiamo una legge (tautologia) P conn Q quindi $R \; conn \; R[Q/P]$ è una tautologia
- Abbiamo dimostrato $\boxed{R \; conn \; R[Q/P]}$
- Per garantire il *Principio di Sostituzione* assumiamo che P occorra positivamente in R (Il caso di $\Leftarrow$ è analogo a quello di $\Rightarrow$)

Un Passo di Dimostrazione con Ipotesi

- Consideriamo un passo di dimostrazione con $conn \in \{\equiv, \Rightarrow\}$:

$$
\begin{array}{lll}
 & R & \\
conn & & \{P\ conn\ Q\} \\
 & R[Q/P] &
\end{array}
$$

- La formula P conn Q non è una legge (tautologia)!!
- Cosa abbiamo dimostrato?????
- Se $P\ conn\ Q$ fosse vera allora $R\ conn\ R[Q/P]$ sarebbe vera!!!
- Il passaggio deduttivo è valido sotto l'ipotesi $P\ conn\ Q$
- Formalmente: $\boxed{P\ conn\ Q \ \Rightarrow\ R\ conn\ R[Q/P]}$

Un Passo di Dimostrazione: caso generale

- Consideriamo un passo di dimostrazione con $conn \in \{\equiv, \Rightarrow\}$:

$$\begin{array}{lll} & R & \\ conn & & \{P\ conn\ Q\} \\ & R[Q/P] & \end{array}$$

- Abbiamo dimostrato che
  $\boxed{P\ conn\ Q \ \Rightarrow\ R\ conn\ R[Q/P]}$
- Se $P\ conn\ Q$ è una legge (tautologia) allora abbiamo che $P\ conn\ Q \equiv \mathbf{T}$ e quindi abbiamo dimostrato
  $\boxed{R\ conn\ R[Q/P]}$

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:

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

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

Schema Generale di Dimostrazione con Ipotesi

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:

$$(\mathbf{G_1} \Rightarrow (\mathbf{P_1}\ \mathbf{conn_1}\ \mathbf{P_2})) \wedge \ldots \wedge (\mathbf{G_{n-1}} \Rightarrow (\mathbf{P_{n-1}}\ \mathbf{conn_{n-1}}\ \mathbf{P_n}))$$

Commenti

- Supponiamo poi che le proprietà di $\mathbf{conn_1}$, ... $\mathbf{conn_{n-1}}$ consentono di dimostrare

$$\mathbf{P_1} \ \mathbf{conn} \ \mathbf{P_n}$$

- Allora abbiamo

$$G_1 \Rightarrow (P_1 \ conn_1 \ P_2)) \wedge \ldots (G_{n-1} \Rightarrow (P_{n-1} \ conn_{n-1} \ P_n)) \ \Rightarrow (G_1 \wedge \ldots \wedge G_{n-1} \Rightarrow \mathbf{P_1} \ \mathbf{conn} \ \mathbf{P_n})$$

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

$$\mathbf{H} \Rightarrow \mathbf{P}_1 \ conn \ \mathbf{P}_n$$

Commenti

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

$$\mathbf{P_1} \textbf{ conn } \mathbf{P_n}$$

- Se le giustificazioni $\mathbf{G_1}$, ... , $\mathbf{G_{n-1}}$ non sono tautologie, ma ipotesi, allora abbiamo una dimostrazione di

$$\mathbf{G_1} \wedge \ldots \wedge \mathbf{G_{n-1}} \Rightarrow \mathbf{P_1} \textbf{ conn } \mathbf{P_n}$$

- Se poi $\mathbf{H}$ è la congiunzione di tutte le ipotesi usate come giustificazioni abbiamo una dimostrazione di

$$\mathbf{H} \Rightarrow \mathbf{P_1} \textbf{ conn } \mathbf{P_n}$$

Uso di Ipotesi come Giustificazioni

- **Strategia intuitiva**: 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 è dimostrare che Q è vero quando P è vero. Quando$P$ è falso l'implicazione vale sempre.

Uso di Ipotesi come Giustificazioni: Esempio 2

- Teorema: $(P \Rightarrow (Q \equiv R)) \Rightarrow (P \wedge R \Rightarrow Q)$
- Strategia: proviamo che $(P \wedge R \Rightarrow Q)$ è vera nell'ipotesi che $(P \Rightarrow (Q \equiv R))$ sia vera
- Partiamo dalla premessa $P \wedge R$ per arrivare a Q usando l'ipotesi $(P \Rightarrow (Q \equiv R))$

Dimostrazione con Ipotesi: Esempio 2

$$
\begin{array}{ll}
 & \underline{P} \wedge R \\
\Rightarrow & \{\mathbf{Ip}: P \Rightarrow (Q \equiv R),\ P \text{ occ. pos.}\} \\
 & \underline{(Q \equiv R)} \wedge R \\
\equiv & \{(\text{Elim-}\equiv)\} \\
 & (Q \Rightarrow R) \wedge \underline{(R \Rightarrow Q) \wedge R} \\
\Rightarrow & \{(\text{Modus Ponens}),\ (R \Rightarrow Q) \wedge R \text{ occ. pos.} \\
 & \underline{(Q \Rightarrow R) \wedge Q} \\
\Rightarrow & \{\text{Semp.-}\wedge,\ (Q \Rightarrow R) \wedge Q \text{ occ. pos.}\} \\
 & Q
\end{array}
$$

Ancora Esempi: (Sempl.-$\Rightarrow$)

- Vogliamo dimostrare la legge:
  $(P \Rightarrow Q) \land (R \Rightarrow S) \Rightarrow (P \land R \Rightarrow Q \land S)$
- Dimostriamo $(P \land R \Rightarrow Q \land S)$ usando le ipotesi $P \Rightarrow Q$ e $R \Rightarrow S$

$$\begin{array}{ll} & \underline{P} \land R \\ \Rightarrow & \{\textbf{Ip}\text{: P} \Rightarrow \text{Q, P occorre pos.}\} \\ & Q \land \underline{R} \\ \Rightarrow & \{\textbf{Ip}\text{: R} \Rightarrow \text{S, R occorre pos.}\} \\ & Q \land S \end{array}$$

Esempio: Prova per Casi

- Dimostrare $(P \vee Q \Rightarrow R) \Rightarrow (P \Rightarrow R)$ per casi su Q
- Caso $Q \equiv \mathbf{T}$

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

- Caso $Q \equiv \mathbf{F}$

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

Esercizio

- Dimostrare la seguente tautologia

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

- Si fornisca una dimostrazione per sostituzione partendo dalla premessa $(\neg P \vee Q \;\Rightarrow\; \neg R) \wedge ((\neg P \vee \neg Q) \wedge P \;\Rightarrow\; \neg S)$ ed arrivando alla conseguenza $(R \;\Rightarrow\; \neg S)$
- Si fornisca una dimostrazione per sostituzione usando le ipotesi non tautologiche

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-$\Rightarrow$)
- $(p \Rightarrow q) \vee (p \Rightarrow r) \equiv (p \Rightarrow q \vee r)$
- $(p \Rightarrow q) \wedge (p \Rightarrow r) \equiv (p \wedge q \Rightarrow r)$ (Sempl.Sinistra-$\Rightarrow$)
- $(p \Rightarrow q) \vee (p \Rightarrow r) \equiv (p \vee q \Rightarrow r)$
- $p \Rightarrow (q \Rightarrow r) \equiv (p \wedge q \Rightarrow r)$ (Sempl.Sinistra-2–$\Rightarrow$)
- Esercizio: dimostrare che sono tautologie