DIMOSTRAZIONI CON IPOTESI NON TAUTOLOGICHE

Andrea Corradini e Francesca Levi

Dipartimento di Informatica

October 3, 2016

Esempi: Inferenze Corrette e Tautologie

- Il Calcolo Proposizionale permette di formalizzare semplici inferenze/deduzioni/dimostrazioni, e di verificarne la correttezza
- Esempio: **"Normalmente se piove non esco, ma ieri sono uscito, quindi non pioveva"**
- Formula proposizionale corrispondente:

$$(P \Rightarrow \neg E) \wedge E \Rightarrow \neg P$$

- **L'inferenza è corretta se e solo se la formula è una tautologia**
- In questo caso lo è, vediamo la dimostrazione:

$$\begin{array}{lll}
 & (P \Rightarrow \neg E) \wedge E & \\
\equiv & & \{(\text{Elim.-}\Rightarrow)\} \\
 & (\neg P \ \vee \neg E) \wedge E & \\
\equiv & & \{\ (\text{Complemento})\} \\
 & (\neg P \wedge E) & \\
\Rightarrow & & \{\ (\text{Sempl.-}\wedge)\} \\
 & \neg P &
\end{array}$$

Inferenze Corrette e Tautologie (2)

- Esempio: **"Normalmente se piove non esco, ma ieri non pioveva, quindi sono uscito"**
- Formula proposizionale corrispondente:

$$(P \Rightarrow \neg E) \wedge \neg P \Rightarrow E$$

- **L'inferenza è corretta se e solo se la formula è una tautologia**
- In questo caso no: trovare un controesempio!

$$\mathit{Soluzione}: \ \{E \rightarrow \mathbf{F}, P \rightarrow \mathbf{F}\}$$

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

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 $conn \in \{\equiv, \Rightarrow\}$:

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

- 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 che

$$P\ conn\ Q \;\Rightarrow\; R\ conn\ R[Q/P]$$

- Se $P\ conn\ Q$ è una legge (tautologia) allora

$$R\ conn\ R[Q/P]$$

Uso di Ipotesi come Giustificazioni: Esempio 1

- Vogliamo dimostrare che la formula $p \Rightarrow (p \wedge q \equiv q)$ è una tautologia
- Proviamo che $(p \wedge q \equiv q)$ è vera nell'ipotesi che p sia vera:

$$
\begin{array}{lll}
 & p \wedge q & \\
\equiv & & \{\mathbf{Ip}\text{: } p \equiv \mathbf{T}\} \\
 & \mathbf{T} \wedge q & \\
\equiv & & \{(\text{Unità})\} \\
 & q &
\end{array}
$$

- Nelle giustificazioni abbiamo indicato esplicitamente con "Ip: ..." il fatto che $p \equiv \mathbf{T}$ è un'ipotesi e non una tautologia (legge)

Schema Generale di Dimostrazione con Ipotesi

Lo schema di dimostrazione:

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

rappresenta una dimostrazione della seguente tautologia:

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

Commenti

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

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

- Otteniamo

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

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

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

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 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 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

$$
\begin{array}{lll}
 & p \wedge r & \\
\Rightarrow & & \{\textbf{Ip}\text{: } (p \Rightarrow (q \equiv r)),\ p \text{ occorre pos.}\} \\
 & (q \equiv r) \wedge r & \\
\equiv & & \{(\text{Elim.-}\equiv)\} \\
 & (q \Rightarrow r) \wedge (r \Rightarrow q) \wedge r & \\
\Rightarrow & & \{(\text{Modus Ponens}),\ (r \Rightarrow q) \wedge r \text{ occorre pos.}\} \\
 & (q \Rightarrow r) \wedge q & \\
\Rightarrow & & \{\text{Sempl.-}\wedge,\ (q \Rightarrow r) \wedge q \text{ occorre pos.}\} \\
 & q &
\end{array}
$$

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

- Vogliamo dimostrare la legge:

$$(p \Rightarrow q) \wedge (r \Rightarrow s) \Rightarrow (p \wedge r \Rightarrow q \wedge s)$$

- Dimostriamo $(p \wedge r \Rightarrow q \wedge s)$ usando le ipotesi $p \Rightarrow q$ e $r \Rightarrow s$

Dimostrazione (Sempl.-$\Rightarrow$) con Ipotesi

$$
\begin{array}{lll}
 & p \wedge r & \\
\Rightarrow & & \{\textbf{Ip}:\ p \Rightarrow q,\ \text{p occorre pos.}\} \\
 & q \wedge r & \\
\Rightarrow & & \{\textbf{Ip}:\ r \Rightarrow s,\ \text{r occorre pos.}\} \\
 & q \wedge s &
\end{array}
$$

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 contrapposizione

Dimostrazione per Assurdo

- Dimostrazione per Assurdo (1):
  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

$$p \Rightarrow q \equiv (p \ \wedge \neg q \Rightarrow \mathbf{F})$$

- Esercizio: mostrare che sono tautologie

Dimostrazioni per assurdo: prova delle leggi

- $p \equiv (\neg p \Rightarrow \mathbf{F})$

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

- $p \Rightarrow q \equiv (p \ \wedge \neg q \Rightarrow \mathbf{F})$

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

Esempio di Dimostrazione per Assurdo

Dimostriamo per assurdo che $((p \vee q) \;\Rightarrow\; r)) \;\Rightarrow\; (p \Rightarrow r)$

$$
\begin{array}{lll}
 & ((p \vee q) \Rightarrow r) \wedge \neg(p \Rightarrow r) & \\
\equiv & & \{(\text{Elim.-}\Rightarrow),\ (\neg - \Rightarrow)\} \\
 & (\neg(p \vee q) \vee r) \wedge (p \;\wedge \neg r) & \\
\equiv & & \{(\text{De Morgan})\} \\
 & ((\neg p \;\wedge \neg q) \vee r) \wedge (\neg r \;\wedge p) & \\
\equiv & & \{(\text{Complemento})\} \\
 & (\neg p \;\wedge \neg q) \;\wedge \neg r \;\wedge p & \\
\equiv & & \{\ (\text{Comm.})\ \text{e}\ (\text{Ass.})\ \} \\
 & (\neg p \wedge p) \;\wedge \neg q \;\wedge \neg r & \\
\equiv & & \{(\text{Contraddizione})\ \text{e}\ (\text{Zero})\ \} \\
 & \mathbf{F} &
\end{array}
$$

Dimostrazione per Controposizione

- $\boxed{\begin{array}{c}\textit{Per dimostrare } p \Rightarrow q \\ \textit{si può dimostrare che } \neg q \Rightarrow \neg p\end{array}}$
- In formule otteniamo

$$p \Rightarrow q \equiv \neg q \Rightarrow \neg p$$

- Esercizio: dimostare la legge

Dimostrazione per Casi

- Dimostrazione per Casi:
  Per dimostrare q, basta mostrare che per un certo p, valgono sia $p \Rightarrow q$ che $\neg p \Rightarrow q$

$$(p \Rightarrow q) \wedge (\neg p \Rightarrow q) \equiv q$$

- Dimostrazione per Casi:
  Per dimostrare che $p \wedge r \Rightarrow q \wedge s$, basta fornire due prove separate per $p \Rightarrow q$ e per $r \Rightarrow s$

$$(p \Rightarrow q) \wedge (r \Rightarrow s) \equiv p \wedge r \Rightarrow q \wedge s$$

- Esercizio: mostrare che sono tautologie

Esempio: Prova per Casi

- Dimostrare $((p \vee q) \Rightarrow r) \Rightarrow (p \Rightarrow r)$ per casi su q
- Caso $q \equiv \mathbf{T}$

$$
\begin{array}{lll}
 & (p \vee q) \Rightarrow r & \\
\equiv & & \{ \textbf{Ip}\text{: } q \equiv \mathbf{T}, \text{(Zero)} \} \\
 & \mathbf{T} \Rightarrow r & \\
\equiv & & \{ \text{(Elim.-}\Rightarrow\text{) e (Unità)} \} \\
 & r & \\
\Rightarrow & & \{ \text{(Intro.-}\vee\text{)} \} \\
 & \neg p \vee r & \\
\equiv & & \{ \text{(Elim.-}\Rightarrow\text{)} \} \\
 & p \Rightarrow r &
\end{array}
$$

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

$$
\begin{array}{lll}
 & (p \vee q) \Rightarrow r & \\
\equiv & & \{ \textbf{Ip}\text{: } q \equiv \mathbf{F}, \text{(Unità)} \} \\
 & p \Rightarrow r &
\end{array}
$$

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