DIMOSTRAZIONI CON IPOTESI NON TAUTOLOGICHE

Corso di Logica per la Programmazione

A.A. 2010/11

Andrea Corradini, Paolo Mancarella

FORMALIZZAZIONE DEI PASSI DI DIMOSTRAZIONE

- Sia ***conn*** $\in$ { ≡, ⇒, ⇐ }
- Per il **Teorema di Deduzione** (che vedremo in seguito), il passo di dimostrazione

$$\begin{array}{ll} & \mathbf{P} \\ \boldsymbol{conn} & \{ \mathbf{G} \} \\ & \mathbf{Q} \end{array}$$

è un modo di esprimere che $\mathbf{G} \Rightarrow (\mathbf{P}\ \boldsymbol{conn}\ \mathbf{Q})$ è una ***tautologia***

- Analogamente,

$$\begin{array}{ll} & \mathbf{P} \\ \boldsymbol{conn}_1 & \{ \mathbf{G}_1 \} \\ & \mathbf{Q} \\ \boldsymbol{conn}_2 & \{ \mathbf{G}_2 \} \\ & \mathbf{R} \end{array}$$

corrisponde a $(\mathbf{G}_1 \Rightarrow (\mathbf{P}\ \boldsymbol{conn}_1\ \mathbf{Q})) \wedge (\mathbf{G}_2 \Rightarrow (\mathbf{Q}\ \boldsymbol{conn}_2\ \mathbf{R}))$

OVVERO

- Poiché $\mathbf{G}_1$ e $\mathbf{G}_2$ sono tautologie (e $P \equiv \mathbf{T} \Rightarrow P$), abbiamo

  $$(\mathbf{G}_1 \Rightarrow (\mathbf{P}\ \boldsymbol{conn}_1\ \mathbf{Q})) \wedge (\mathbf{G}_2 \Rightarrow (\mathbf{Q}\ \boldsymbol{conn}_2\ \mathbf{R}))$$

  $$\equiv$$

  $$(\mathbf{P}\ \boldsymbol{conn}_1\ \mathbf{Q}) \wedge (\mathbf{Q}\ \boldsymbol{conn}_2\ \mathbf{R})$$

- Se $\boldsymbol{conn}_1$ e $\boldsymbol{conn}_2$ sono lo stesso connettivo e il connettivo è transitivo (come lo sono $\equiv$ e $\Rightarrow$), dalla prova segue

  $$\mathbf{P}\ \boldsymbol{conn}\ \mathbf{R}$$

  come richiedeva la nostra intuizione

USO DI IPOTESI COME GIUSTIFICAZIONI

- Riassumendo: per dimostrare che da una ipotesi **P** segue una conseguenza **Q**, possiamo dimostrare che
  - $\mathbf{P} \Rightarrow \mathbf{Q}$ è una tautologia
  - $\mathbf{\sim Q} \Rightarrow \mathbf{\sim P}$ è una tautologia
  - $\mathbf{P} \wedge \mathbf{\sim Q} \Rightarrow \mathbf{F}$ è una tautologia
- ***Strategia alternativa***: per dimostrare $\mathbf{P} \Rightarrow \mathbf{Q}$, 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 1

- Teorema: $\mathbf{p \Rightarrow (p \wedge q \equiv q)}$
- Prova: dimostriamo che $\mathbf{(p \wedge q \equiv q)}$ è vera nell'ipotesi che **p** sia vera:

$$\mathbf{p \wedge q}$$
$$\equiv \{\ \mathbf{Ip}: p \equiv \mathbf{T}\ \}$$
$$\mathbf{T} \wedge \mathbf{q}$$
$$\equiv \{\text{unità}\}$$
$$\mathbf{q}$$

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

USO DI IPOTESI COME GIUSTIFICAZIONI: ESEMPIO 2

- Teorema: $\mathbf{(P \Rightarrow (Q \equiv R)) \Rightarrow (P \land R \Rightarrow Q)}$
- Prova: dimostriamo che vale $\mathbf{(P \land R \Rightarrow Q)}$ sotto l'ipotesi che valga $\mathbf{(P \Rightarrow (Q \equiv R))}$

$\mathbf{P \land R}$

$\Rightarrow$ {**Ip**: $P \Rightarrow (Q \equiv R)$, P occorre pos.}

$(Q \equiv R) \land R$

$\equiv$ {Elim- $\equiv$ }

$(Q \Rightarrow R) \land (R \Rightarrow Q) \land R$

$\Rightarrow$ {Modus Ponens, $(R \Rightarrow Q) \land R$ occorre pos.}

$(Q \Rightarrow R) \land Q$

$\Rightarrow$ {Sempl- $\land$ }

$\mathbf{Q}$

IN CONCLUSIONE

Lo schema di dimostrazione:

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

rappresenta una dimostrazione della seguente tautologia:

$$(\mathbf{G_1} \Rightarrow (\mathbf{P_1}\ \boldsymbol{conn_1}\ \mathbf{P_2}) \wedge (\mathbf{G_2} \Rightarrow (\mathbf{P_2}\ \boldsymbol{conn_2}\ \mathbf{P_3})) \wedge \ldots$$

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

- Supponiamo poi che le proprietà di $\boldsymbol{conn}_1$ **...** $\boldsymbol{conn}_{n-1}$, consentono di dimostrare $(\mathbf{P}_1\ \boldsymbol{conn}\ \mathbf{P}_n)$

- Se le giustificazioni $\mathbf{G}_1, \ldots, \mathbf{G}_{n-1}$ sono tutte tautologie, allora abbiamo una dimostrazione di

$$\mathbf{P}_1\ \boldsymbol{conn}\ \mathbf{P}_n$$

- Se le giustificazioni $\mathbf{G}_1, \ldots, \mathbf{G}_{n-1}$ non sono tautologie, ma ipotesi, allora abbiamo una dimostrazione di

$$\mathbf{G}_1 \wedge \ldots \wedge \mathbf{G}_{n-1} \Rightarrow (\mathbf{P}_1\ \boldsymbol{conn}\ \mathbf{P}_n)$$

- Se poi **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 prova di

$$\mathbf{H} \Rightarrow (\mathbf{P}_1\ \boldsymbol{conn}\ \mathbf{P}_n)$$

Ancora esempi...

- Dimostrare le seguenti tautologie usando giustificazioni non tautologiche

- $(p \vee q) \wedge (p \Rightarrow r) \wedge (q \Rightarrow s) \;\; \Rightarrow (r \vee s)$
  (Sillogismo disgiuntivo)

- $(p \Rightarrow q) \wedge (r \Rightarrow s) \Rightarrow (p \wedge r \;\; \Rightarrow q \wedge s)$
  (Sempl.-$\Rightarrow$)

Ancora esempi...

$p \vee q$

$\Rightarrow \quad \{\textbf{Ip: } p \Rightarrow r,\ p+\}$

$r \vee q$

$\Rightarrow \quad \{\textbf{Ip: } q \Rightarrow s,\ q+\}$

$r \vee s$

- In realtà abbiamo dimostrato

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

che, grazie alla legge (Sempl. Sinistra-$\Rightarrow$), equivale al Sillogismo Disgiuntivo

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

Ancora esempi...

$p \wedge r$

$\Rightarrow$ $\{$**Ip:** $p \Rightarrow q,\ p+\}$

$q \wedge r$

$\Rightarrow$ $\{$**Ip:** $r \Rightarrow s,\ r+\}$

$q \wedge s$

- Abbiamo dimostrato

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

(Sempl.-$\Rightarrow$)

ALTRE TECNICHE DI DIMOSTRAZIONE

DIMOSTRAZIONE PER ASSURDO

- Corrisponde all'uso della legge (ovvia tautologia)

$$(\sim p \Rightarrow F) \equiv p$$

- Se $p \equiv q \Rightarrow r$ la prova per assurdo diventa

$\sim(q \Rightarrow r) \Rightarrow F$

$\equiv$

$\sim(\sim q \vee r) \Rightarrow F$

$\equiv$

$(q \wedge \sim r) \Rightarrow F$

ESEMPIO: $((P \vee Q) \Rightarrow R) \Rightarrow (P \Rightarrow R)$

Prova per assurdo

$((p \vee q) \Rightarrow r) \wedge \sim(p \Rightarrow r)$

$\equiv$ {elim- $\Rightarrow$, DeMorgan}

$(\sim(p \vee q) \vee r) \wedge (p \wedge \sim r)$

$\equiv$ {DeMorgan}

$((\sim p \wedge \sim q) \vee r) \wedge (p \wedge \sim r)$

$\equiv$ {complemento}

$(\sim p \wedge \sim q) \wedge p \wedge \sim r$

$\equiv$ {contraddizione e zero}

F

DIMOSTRAZIONE PER CASI

- Corrisponde all'uso della tautologia:

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

- Ovvero per dimostrare p è sufficiente provare le due implicazioni:
  - $q \Rightarrow p$
  - $\sim q \Rightarrow p$
- q e ~q costituiscono un contesto che facilita la dimostrazione.
- I due casi (q e ~q) insieme naturalmente garantiscono un contesto sempre vero.

ESEMPIO DI PROVA PER CASI

- $((p \vee q) \Rightarrow r) \Rightarrow (p \Rightarrow r)$
- Caso q

$(p \vee q) \Rightarrow r$

$\equiv$ {**Ip**: q, Zero}

$T \Rightarrow r$

$\equiv$ {Elim- $\Rightarrow$, Unità}

r

$\Rightarrow$ {Intro- $\vee$}

$\sim p \vee r$

$\equiv$ {Elim- $\Rightarrow$}

$p \Rightarrow r$

- Caso ~q

$(p \vee q) \Rightarrow r$

$\equiv$ {**Ip**: ~q ,Unità}

$p \Rightarrow r$