DIMOSTRAZIONI E TAUTOLOGIE, IPOTESI NON TAUTOLOGICHE

Corso di Logica per la Programmazione

A.A. 2013/14

Andrea Corradini

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:

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

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

$$
\begin{array}{ll}
 & (P \Rightarrow \sim E) \wedge E \\
\equiv & \{(\text{elim-}\Rightarrow)\} \\
 & (\sim P \vee \sim E) \wedge E \\
\equiv & \{(\text{complemento})\} \\
 & \sim P \wedge E \\
\Rightarrow & \{(\text{sempl-}\wedge)\} \\
 & \sim P
\end{array}
$$

INFERENZE CORRETTE E TAUTOLOGIE (2)

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

$$((P \Rightarrow \sim E) \land \sim P) \Rightarrow E$$

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

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

- In generale, possiamo rapprensentare con delle formule proposizionali delle **tecniche di dimostrazione**: saranno corrette se e solo se la formula è una tautologia

TECNICHE DI DIMOSTRAZIONE COME TAUTOLOGIE

- 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*

- $p \equiv (\sim p \Rightarrow F)$ (Dimostrazione per Assurdo)

> 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*

- $p \Rightarrow q \equiv (p \wedge \sim q \Rightarrow F)$ (Dimostrazione per Assurdo)
- Esercizio: mostrare che sono tautologie

ESEMPIO DI DIMOSTRAZIONE PER ASSURDO: $((P \vee Q) \Rightarrow R) \Rightarrow (P \Rightarrow R)$

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

$\equiv$ {(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

TECNICHE DI DIMOSTRAZIONE COME TAUTOLOGIE (2)

Dimostrazione per Controposizione:

Per dimostrare che $p \Rightarrow q$

si può dimostrare che $\sim q \Rightarrow \sim p$

- $p \Rightarrow q \equiv \sim q \Rightarrow \sim p$ (Controposizione)

Dimostrazione per casi:

Per dimostrare q *è sufficiente dimostrare che,*

per un certo p, *valgono sia* $p \Rightarrow q$ che $\sim p \Rightarrow q$

- $(p \Rightarrow q) \wedge (\sim p \Rightarrow q) \Rightarrow q$ (Dim. per casi)

Per dimostrare che $p \wedge r \Rightarrow q \wedge s$ *è sufficiente*

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.-$\Rightarrow$)
- Esercizio: mostrare che sono tautologie

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)}

$p \Rightarrow r$

ALTRE TAUTOLOGIE CHE RAPPRESENTANO TECNICHE DI DIMOSTRAZIONE

- $(p \Rightarrow \sim p) \equiv \sim p$ (Riduzione ad Assurdo)
- $p \wedge q \Rightarrow r \equiv p \wedge \sim r \Rightarrow \sim q$ (Scambio)
- $((p \Rightarrow q) \wedge \sim q) \Rightarrow \sim p$ (Tollendo Tollens)
- $(p \equiv q) \equiv (p \wedge q) \vee (\sim p \wedge \sim q)$ (Elim-≡-bis)
- $(p \Rightarrow q) \wedge (p \Rightarrow r) \equiv (p \Rightarrow q \wedge r)$ (Sempl.Destra-⇒)
- $(p \Rightarrow q) \vee (p \Rightarrow r) \equiv (p \Rightarrow q \vee r)$
- $(p \Rightarrow r) \vee (q \Rightarrow r) \equiv (p \wedge q \Rightarrow r)$ (Sempl.Sinistra-⇒)
- $(p \Rightarrow r) \wedge (q \Rightarrow r) \equiv (p \vee q \Rightarrow r)$
- $p \Rightarrow (q \Rightarrow r) \equiv (p \wedge q \Rightarrow r)$ (Sempl.Sinistra-2 ⇒)

- **Esercizio:** dimostrare che sono tautologie

DA DIMOSTRAZIONI A TAUTOLOGIE

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

$$\boxed{\begin{array}{l} \quad P \\ \equiv \ \{ G \} \\ \quad Q \end{array}}$$

- 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, $G \equiv T$, da cui segue che $\boxed{(P \equiv Q)}$ è una tautologia (perché?)
- Analogamente,

$$\boxed{\begin{array}{l} \quad P \\ \Rightarrow \ \{ G \} \\ \quad Q \end{array}} \quad \text{sse} \quad \boxed{G \Rightarrow (P \Rightarrow Q)} \quad \text{sse} \quad \boxed{(P \Rightarrow Q)}$$

DA DIMOSTRAZIONI A TAUTOLOGIE

- E se abbiamo più passi di dimostrazione?
- Sia $conn_i \in \{\equiv, \Rightarrow\}$. Allora,

$$\boxed{\begin{array}{ll} \quad P & \\ conn_1 & \{ G_1 \} \\ \quad Q & \\ conn_2 & \{ G_2 \} \\ \quad R & \end{array}} \qquad \text{sse} \qquad \boxed{\begin{array}{l} (G_1 \Rightarrow (P \; conn_1 \; Q)) \land \\ (G_2 \Rightarrow (Q \; conn_2 \; R)) \end{array}}$$

- Poiché G_1 e G_2 sono tautologie (e $(T \Rightarrow R) \equiv R$), abbiamo

$$(G_1 \Rightarrow (P \; conn_1 \; Q)) \land (G_2 \Rightarrow (Q \; conn_2 \; R)) \quad \equiv$$
$$(P \; conn_1 \; Q) \land (Q \; conn_2 \; R)$$

- Se $conn_1$ e $conn_2$ sono lo stesso connettivo e il connettivo è transitivo (come lo sono $\equiv$ e $\Rightarrow$), dalla prova segue

$$P \;\; conn \;\; R$$

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:

$$
\begin{aligned}
& \mathbf{p \wedge q} \\
\equiv\ & \{\ \mathbf{Ip}\text{: } p \equiv \mathbf{T}\ \} \\
& \mathbf{T} \wedge \mathbf{q} \\
\equiv\ & \{\text{unità}\} \\
& \mathbf{q}
\end{aligned}
$$

- Nelle giustificazioni abbiamo indicato esplicitamente con "**Ip: ...**" il fatto che p ≡ **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 $\mathbf{(P \Rightarrow (Q \equiv R))}$

$$\mathbf{P \land R}$$
$$\Rightarrow \{\mathbf{Ip}: P \Rightarrow (Q \equiv R), \text{P occorre pos.}\}$$
$$(Q \equiv R) \land R$$
$$\equiv \quad \{\text{Elim-} \equiv\}$$
$$(Q \Rightarrow R) \land (R \Rightarrow Q) \land R$$
$$\Rightarrow \{\text{Modus Ponens, } (R \Rightarrow Q) \land R \text{ occorre pos.}\}$$
$$(Q \Rightarrow R) \land Q$$
$$\Rightarrow \{\text{Sempl-} \land\}$$
$$\mathbf{Q}$$

IN CONCLUSIONE

Lo schema di dimostrazione:

$$\begin{array}{ll} & \mathbf{P_1} \\ \boldsymbol{conn_1} & \{\, \mathbf{G_1} \,\} \\ & \mathbf{P_2} \\ \boldsymbol{conn_2} & \{\, \mathbf{G_2} \,\} \\ \multicolumn{2}{l}{\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots} \\ & \mathbf{P_{n-1}} \\ \boldsymbol{conn_{n-1}} & \{\, \mathbf{G_{n-1}} \,\} \\ & \mathbf{P_n} \end{array}$$

rappresenta una dimostrazione della seguente tautologia:

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

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

- 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.-$\Rightarrow$)

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

(Sillogismo disgiuntivo)

$p \vee q$

$\Rightarrow$ $\{$**Ip:** $p \Rightarrow r, p+\}$ [indichiamo che p occorre

$r \vee q$ positivamente con p+]

$\Rightarrow$ $\{$**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 2-$\Rightarrow$), equivale al Sillogismo Disgiuntivo

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

$p \Rightarrow (q \Rightarrow r) \equiv (p \wedge q \Rightarrow r)$	(Sempl. Sinistra 2-$\Rightarrow$)

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

(Sempl.-$\Rightarrow$)

$p \wedge r$

$\Rightarrow$ {**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.-$\Rightarrow$)