



# **DIMOSTRAZIONI E TAUTOLOGIE, IPOTESI NON TAUTOLOGICHE**

**Corso di Logica per la Programmazione**

# 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:

$$\begin{aligned} & (P \Rightarrow \sim E) \wedge E \\ \equiv & \quad \{(\text{elim-}\Rightarrow)\} \\ & (\sim P \vee \sim E) \wedge E \\ \equiv & \quad \{(\text{complemento})\} \\ & \sim P \wedge E \\ \Rightarrow & \quad \{(\text{semp1-}\wedge)\} \\ & \sim P \end{aligned}$$



## INFERENZE CORRETTE E TAUTOLOGIE (2)

- Esempio “*Normalmente se piove non esco, ma ieri non pioveva, quindi sono uscito*”
- Formula proposizionale corrispondente:
$$((P \Rightarrow \sim E) \wedge \sim P) \Rightarrow E$$
- **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 rappresentare 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: $((P \vee Q) \Rightarrow R) \Rightarrow (P \Rightarrow R)$

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

$$\equiv \{(\text{elim-} \Rightarrow), (\text{DeMorgan})\}$$

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

$$\equiv \{(\text{DeMorgan})\}$$

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

$$\equiv \{(\text{complemento})\}$$

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

$$\equiv \{(\text{contraddizione}) \text{ e } (\text{zero})\}$$

F



# TECNICHE DI DIMOSTRAZIONE COME TAUTOLOGIE (2)

Dimostrazione per Controposizione:

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

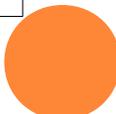
- $p \Rightarrow q \equiv \sim q \Rightarrow \sim p$  (Controposizione)

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  $q$

$$\begin{aligned} & (p \vee q) \Rightarrow r \\ \equiv & \quad \{\mathbf{Ip}: q, (\text{Zero})\} \\ & \quad T \Rightarrow r \\ \equiv & \quad \{(\text{Elim-} \Rightarrow), (\text{Unità})\} \\ & \quad r \\ \Rightarrow & \quad \{(\text{Intro-}\vee)\} \\ & \quad \sim p \vee r \\ \equiv & \quad \{(\text{Elim-} \Rightarrow)\} \\ & \quad p \Rightarrow r \end{aligned}$$

○ Caso  $\sim q$

$$\begin{aligned} & (p \vee q) \Rightarrow r \\ \equiv & \quad \{\mathbf{Ip}: \sim q, (\text{Unità})\} \\ & \quad p \Rightarrow r \end{aligned}$$



# 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- $\equiv$ -bis)
- $(p \Rightarrow q) \wedge (p \Rightarrow r) \equiv (p \Rightarrow q \wedge r)$  (Sempl.Destra- $\Rightarrow$ )
- $(p \Rightarrow q) \vee (p \Rightarrow r) \equiv (p \Rightarrow q \vee r)$
- $(p \Rightarrow r) \vee (q \Rightarrow r) \equiv (p \wedge q \Rightarrow r)$  (Sempl.Sinistra- $\Rightarrow$ )
- $(p \Rightarrow r) \wedge (q \Rightarrow r) \equiv (p \vee q \Rightarrow r)$
- $p \Rightarrow (q \Rightarrow r) \equiv (p \wedge q \Rightarrow r)$  (Sempl.Sinistra-2  $\Rightarrow$ )
  
- **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:

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

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

$$\boxed{\begin{array}{c} P \\ \Rightarrow \{ G \} \\ Q \end{array}}$$

sse

$$\boxed{G \Rightarrow (P \Rightarrow Q)}$$

sse

$$\boxed{(P \Rightarrow Q)}$$



# DA DIMOSTRAZIONI A TAUTOLOGIE

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

P	
$conn_1$	$\{ G_1 \}$
Q	
$conn_2$	$\{ G_2 \}$
R	

sse

$(G_1 \Rightarrow (P \text{ } conn_1 \text{ } Q)) \wedge$ $(G_2 \Rightarrow (Q \text{ } conn_2 \text{ } R))$
---

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

$$(G_1 \Rightarrow (P \text{ } conn_1 \text{ } Q)) \wedge (G_2 \Rightarrow (Q \text{ } conn_2 \text{ } R)) \equiv$$

$$(P \text{ } conn_1 \text{ } Q) \wedge (Q \text{ } conn_2 \text{ } R)$$

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

$$P \text{ } conn \text{ } R$$

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
  - $P \Rightarrow Q$  è una tautologia
  - $\sim Q \Rightarrow \sim P$  è una tautologia
  - $P \wedge \sim Q \Rightarrow F$  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 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:  $p \Rightarrow (p \wedge q \equiv q)$
- Prova: dimostriamo che  $(p \wedge q \equiv q)$  è vera nell'ipotesi che  $p$  sia vera:

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

- 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:  $(P \Rightarrow (Q \equiv R)) \Rightarrow (P \wedge R \Rightarrow Q)$
- Prova: dimostriamo che vale  $(P \wedge R \Rightarrow Q)$  sotto l'ipotesi che valga  $(P \Rightarrow (Q \equiv R))$

**$P \wedge R$**

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

$(Q \equiv R) \wedge R$

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

$(Q \Rightarrow R) \wedge (R \Rightarrow Q) \wedge R$

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

$(Q \Rightarrow R) \wedge Q$

$\Rightarrow \{\text{Sempl- } \wedge \}$

**$Q$**



# IN CONCLUSIONE

Lo schema di dimostrazione:

$P_1$   
 $conn_1 \{ G_1 \}$

$P_2$   
 $conn_2 \{ G_2 \}$

.....

$P_{n-1}$   
 $conn_{n-1} \{ G_{n-1} \}$

$P_n$

rappresenta una dimostrazione della seguente tautologia:

$$(G_1 \Rightarrow (P_1 \textit{ conn}_1 P_2)) \wedge (G_2 \Rightarrow (P_2 \textit{ conn}_2 P_3)) \wedge \dots \\ \dots \wedge (G_{n-1} \Rightarrow (P_{n-1} \textit{ conn}_{n-1} P_n))$$



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

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

$$P_1 \text{ conn } P_n$$

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

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

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

$$H \Rightarrow (P_1 \text{ conn } P_n)$$



## 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)

- Per la legge (Sempl. Sinistra  $2\text{-}\Rightarrow$ ) è sufficiente dimostrare  
 $(p \Rightarrow r) \wedge (q \Rightarrow s) \Rightarrow ((p \vee q) \Rightarrow (r \vee s))$

$P \Rightarrow (Q \Rightarrow R) \equiv (P \wedge Q \Rightarrow R)$  (Sempl. Sinistra  $2\text{-}\Rightarrow$ )

$p \vee q$   
 $\Rightarrow$  {**Ip**:  $p \Rightarrow r, p^+$ } [indichiamo che  $p$  occorre  
 $r \vee q$  positivamente con  $p^+$ ]  
 $\Rightarrow$  {**Ip**:  $q \Rightarrow s, q^+$ }  
 $r \vee s$



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

(Sempl.- $\Rightarrow$ )

$$p \wedge r$$
$$\Rightarrow \quad \{\mathbf{Ip}: p \Rightarrow q, p^+\}$$

$$q \wedge r$$
$$\Rightarrow \quad \{\mathbf{Ip}: r \Rightarrow s, r^+\}$$

$$q \wedge s$$

○ Abbiamo dimostrato

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

(Sempl.- $\Rightarrow$ )

