

DIMOSTRAZIONE DI IMPLICAZIONI TAUTOLOGICHE

Corso di Logica per la Programmazione

A.A. 2010/11

Andrea Corradini

DIGRESSIONE: SULLA SINTASSI DEL CALCOLO PROPOSIZIONALE

- Abbiamo già presentato la grammatica del calcolo:

```
Prop ::=
    Prop ≡ Prop | Prop ∧ Prop | Prop ∨ Prop |
    Prop ⇒ Prop | Prop ⇐ Prop |
    Atom | ~Atom

Atom ::=
    T | F | Ide | (Prop)

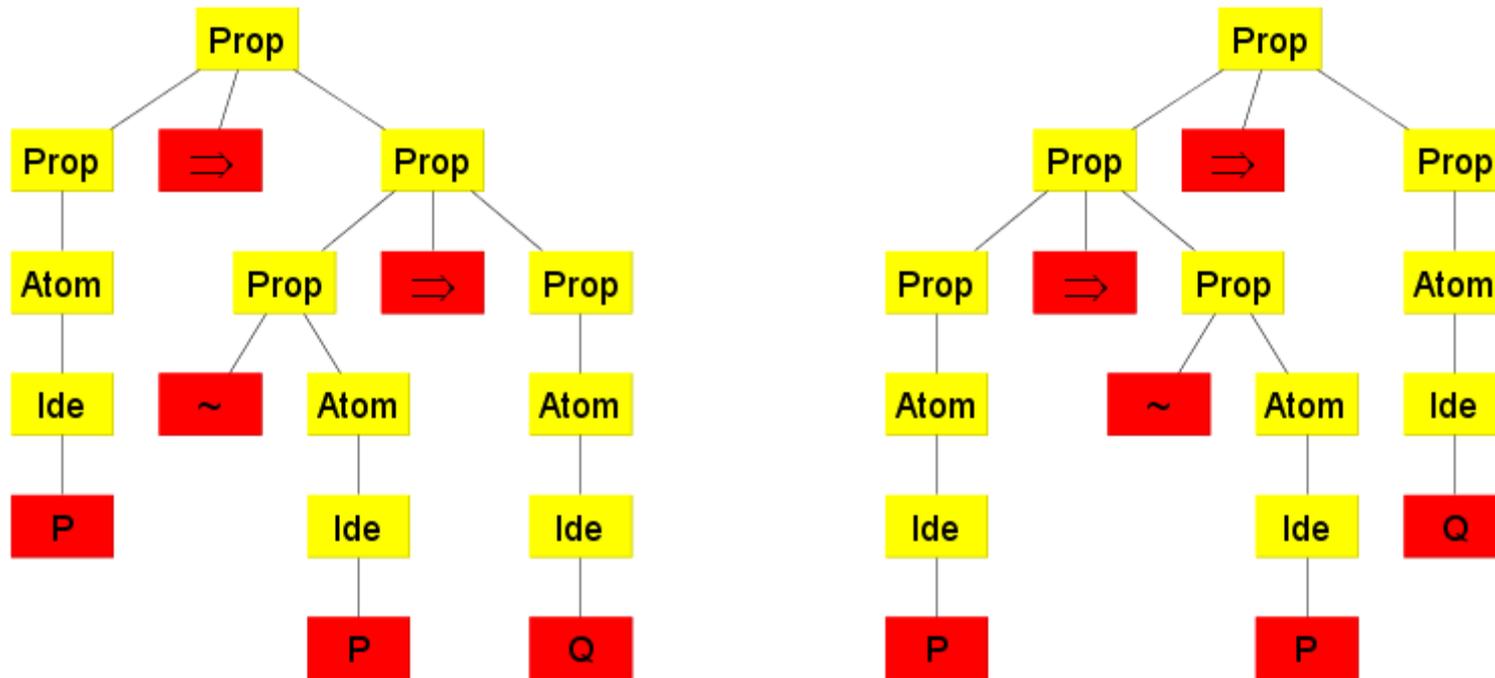
Ide ::=
    p | q | ... | P | Q | ...
```

- Questa grammatica è ambigua: ci sono proposizioni che hanno più di un albero di derivazione.
- Per esempio: $P \Rightarrow \sim P \Rightarrow Q$



AMBIGUITA' DELLA GRAMMATICA: UN ESEMPIO

- Due alberi di derivazione per $P \Rightarrow \sim P \Rightarrow Q$



$P \Rightarrow [\sim P \Rightarrow Q]$

$[P \Rightarrow \sim P] \Rightarrow Q$

- Esercizio: mostrare che la prima è una tautologia, la seconda no

PRECEDENZA TRA CONNETTIVI

- Stabiliamo i seguenti livelli di precedenza tra connettivi logici, per disambiguare le proposizioni:

operatore	livello di precedenza
\equiv	0
\Rightarrow, \Leftarrow	1
\wedge, \vee	2
\neg	3

- Per esempio,
 - $(P \Rightarrow (Q \wedge R)) \equiv ((P \Rightarrow Q) \wedge (P \Rightarrow R))$ si può scrivere
 - $P \Rightarrow Q \wedge R \equiv (P \Rightarrow Q) \wedge (P \Rightarrow R)$
- **Attenzione:** proposizioni come $P \wedge Q \vee R$ o $P \Rightarrow Q \Rightarrow R$ restano **ambigue**. Se non sono disambiguate con parentesi, vengono considerate **sintatticamente errate**



VERSO ALTRE TECNICHE DI DIMOSTRAZIONE DI TAUTOLOGIE

- Abbiamo visto dimostrazioni di equivalenze
(del tipo $\mathbf{p} \equiv \mathbf{q}$) usando una catena di equivalenze:

$$\mathbf{p} \equiv \dots \equiv \mathbf{q}$$

- Se la formula \mathbf{p} da dimostrare non è un'equivalenza, si può mostrare equivalente a \mathbf{T} : $\mathbf{p} \equiv \dots \equiv \mathbf{T}$

- Se la formula è del tipo $\mathbf{p} \Rightarrow \mathbf{q}$, si può dimostrare anche usando una catena di equivalenze/implicazioni:

$$\mathbf{p} \equiv \dots \Rightarrow \dots \equiv \dots \Rightarrow \mathbf{q}$$

usando per giustificazioni, equivalenze o implicazioni tautologiche. Vediamo come...



ALCUNE IMPORTANTI LEGGI DERIVATE

- Hanno un'implicazione come connettivo principale
- Usate come giustificazioni in prove di implicazioni
- *Diamo anche forma disambiguata con parentesi*

- $\mathbf{p \wedge (p \Rightarrow q) \Rightarrow q}$ (Modus Ponens)

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

- $\mathbf{p \wedge q \Rightarrow p}$ (Sempl.- \wedge)

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

- $\mathbf{p \Rightarrow p \vee q}$ (Intro.- \vee)

$$p \Rightarrow (p \vee q)$$



CORRETTEZZA DI MODUS PONENS E SEMPL- \wedge

$$\begin{aligned} & \mathbf{p \wedge (p \Rightarrow q) \Rightarrow q} && \mathbf{(Modus Ponens)} \\ \equiv & && \{Elim-\Rightarrow\} \\ & \mathbf{p \wedge (\sim p \vee q) \Rightarrow q} \\ \equiv & && \{Complemento\} \\ & \mathbf{p \wedge q \Rightarrow q} && \mathbf{(Sempl.-\wedge)} \\ \equiv & && \{Elim-\Rightarrow\} \\ & \mathbf{\sim(p \wedge q) \vee q} \\ \equiv & && \{DeMorgan\} \\ & \mathbf{\sim p \vee \sim q \vee q} \\ \equiv & && \{TerzoEscluso, Zero\} \\ & \mathbf{T} \end{aligned}$$



VERSO LA DIMOSTRAZIONE DI IMPLICAZIONI TAUTOLOGICHE

- Posso impostare la dimostrazione che $P_1 \Rightarrow P_k$ così:

P_1	
\equiv	{giustificazione ₁ }
	...
\equiv	{giustificazione _h }
P	
\Rightarrow	{ $P \Rightarrow Q$ }
Q	
\equiv	{giustificazione _{h+1} }
	...
\equiv	{giustificazione _{k-1} }
P_k	



ESEMPIO - TOLLENDO PONENS

- Usando la legge possiamo dimostrare

$$p \wedge q \Rightarrow q \text{ (Sempl-}\wedge\text{)}$$

$$(p \vee q) \wedge \sim p \Rightarrow q \text{ (Tollendo Ponens)}$$

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

$$\equiv \{ \text{Doppia Negazione e Complemento} \}$$

$$q \wedge \sim p$$

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

$$q$$

- Si noti che abbiamo applicato (Sempl- \wedge) all'intera proposizione $q \wedge \sim p$



VALE UN PRINCIPIO DI SOSTITUZIONE PER L'IMPLICAZIONE ?

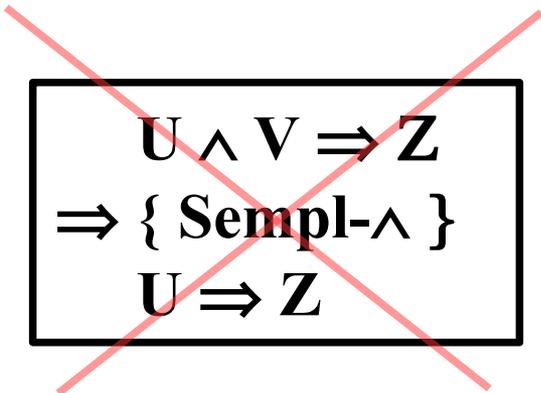
- Il principio di sostituzione stabilisce che se $P \equiv Q$, allora $R \equiv R[Q/P]$
- E' valido un analogo principio di sostituzione per l'implicazione?

“Se $P \Rightarrow Q$, allora $R \Rightarrow R[Q/P]$ ” (???)

- In generale **NO**. Infatti:

$$\begin{array}{l} Z \Rightarrow U \wedge V \\ \Rightarrow \{ \text{Sempl-}\wedge \} \\ Z \Rightarrow U \end{array}$$

OK


$$\begin{array}{l} U \wedge V \Rightarrow Z \\ \Rightarrow \{ \text{Sempl-}\wedge \} \\ U \Rightarrow Z \end{array}$$

NO



ANALOGIA CON DISUGUAGLIANZE ALGEBRICHE

- Una situazione del tutto analoga si incontra nella dimostrazione di disuguaglianze algebriche
- Quali delle seguenti deduzioni sono corrette?

$$\begin{array}{l} \mathbf{a - c} \\ \leq \quad \{ \mathbf{a \leq b} \} \\ \mathbf{b - c} \end{array}$$

OK

$$\begin{array}{l} \mathbf{a - c} \\ \leq \quad \{ \mathbf{c \leq d} \} \\ \mathbf{a - d} \end{array}$$

NO

$$\begin{array}{l} \mathbf{a - c} \\ \geq \quad \{ \mathbf{c \leq d} \} \\ \mathbf{a - d} \end{array}$$

OK

- Si noti che **a** compare *positivamente* in **(a - c)**, ma **c** vi compare *negativamente*. Per questo nel secondo caso il segno di disuguaglianza va invertito.



OCCORRENZE POSITIVE E NEGATIVE

- Diciamo che **p** occorre *positivamente* in

$$\mathbf{p} \quad \mathbf{p} \vee \mathbf{q} \quad \mathbf{p} \wedge \mathbf{q} \quad \mathbf{q} \Rightarrow \mathbf{p}$$

- mentre **p** occorre *negativamente* in

$$\sim \mathbf{p} \\ \mathbf{p} \Rightarrow \mathbf{q} \quad (\text{si ricordi che } \mathbf{p} \Rightarrow \mathbf{q} \equiv \sim \mathbf{p} \vee \mathbf{q})$$

- Se **p** compare in **Q** a livello più profondo, si contano le **occorrenze negative** da **p** fino alla radice di **Q**:
 - se sono pari, **p** occorre *positivamente* in **Q**
 - se sono dispari **p** occorre *negativamente* in **Q**
- Attenzione: **p** può occorrere sia negativamente che positivamente in **Q**



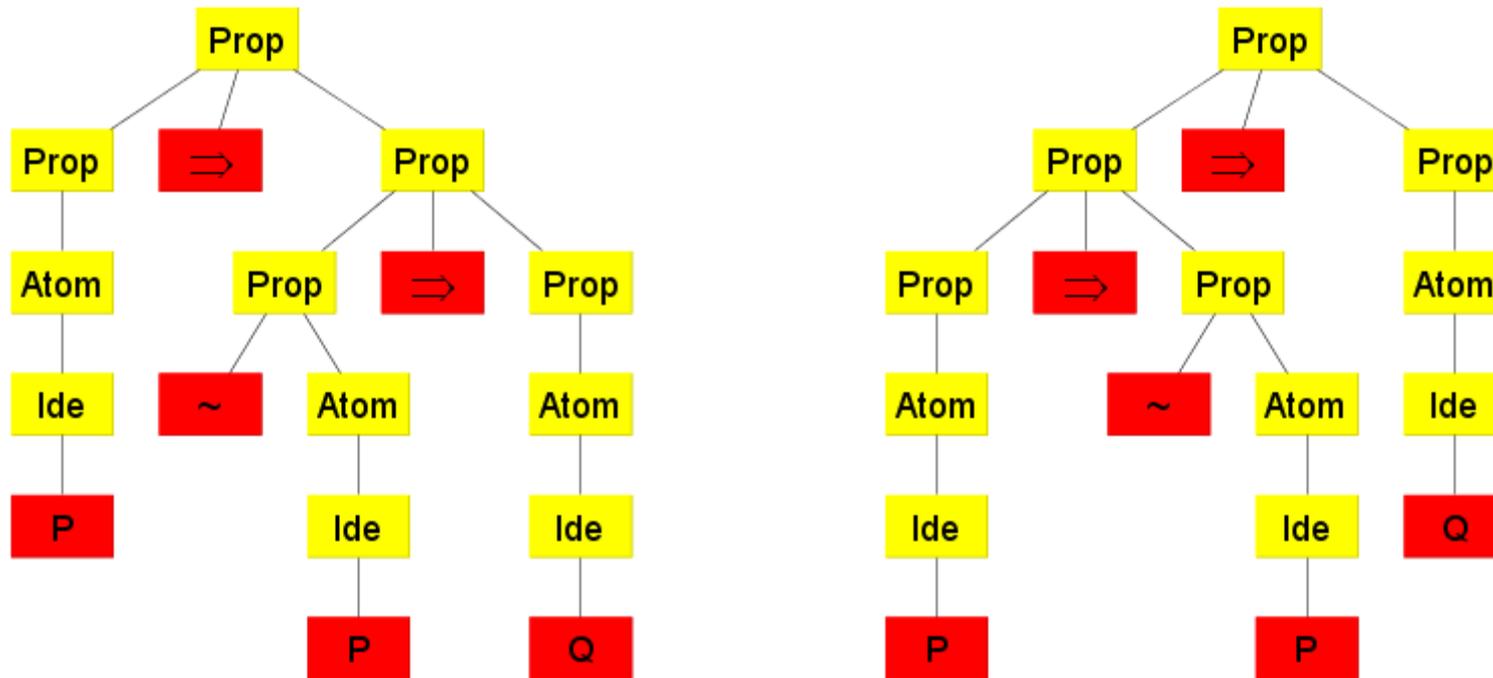
OCCORRENZE POSITIVE E NEGATIVE: ESEMPI

- Come occorre **p** nelle seguenti proposizioni?
 - $(q \wedge p \wedge r) \vee s$
 - $q \Rightarrow \sim(p \wedge r)$
 - $(\sim p \wedge q \Rightarrow r) \Rightarrow s$
 - $\sim p \wedge q \Rightarrow (r \Rightarrow s)$
 - $p \wedge q \Rightarrow p \vee q$
- Se ci sono più occorrenze di **p**, indicheremo esplicitamente quale ci interessa.
 - $\mathbf{p} \Rightarrow (q \vee p \Rightarrow q \vee \sim s)$
 - $p \Rightarrow (q \vee \mathbf{p} \Rightarrow q \vee \sim s)$



OCCORRENZE POSITIVE E NEGATIVE: ESEMPI CON ALBERI DI DERIVAZIONE

- Consideriamo gli alberi di derivazione per $P \Rightarrow \sim P \Rightarrow Q$



$P \Rightarrow [\sim P \Rightarrow Q]$

$[P \Rightarrow \sim P] \Rightarrow Q$

- Esercizio: P e Q compaiono positivamente o negativamente?



PRINCIPIO DI SOSTITUZIONE PER L'IMPLICAZIONE

○ Se abbiamo stabilito

- $p \Rightarrow q$
 - p occorre *positivamente* in r
- allora vale

$$r \Rightarrow r [q/p]$$

○ Se abbiamo stabilito

- $p \Rightarrow q$
 - p occorre *negativamente* in r
- allora vale

$$r \Leftarrow r [q/p]$$



DIMOSTRAZIONE DI IMPLICAZIONI: ESEMPI

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

$$p \Rightarrow q \wedge r$$

\Rightarrow { (Sempl.- \wedge), $q \wedge r$ occorre positivamente }

$$p \Rightarrow q$$

$$p \wedge q \Rightarrow q \text{ (Sempl.-}\wedge\text{)}$$

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

Partiamo dalla conseguenza:

$$(p \Rightarrow r)$$

\Leftarrow { (Intro.- \vee), p occorre negativamente }

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

$$p \Rightarrow p \vee q \text{ (Intro.-}\vee\text{)}$$



ALTRE TECNICHE DI DIMOSTRAZIONE

- Alcune tautologie schematizzano delle tecniche di dimostrazione valide (alcune conosciute dalla scuola)

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

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

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

*Per dimostrare p basta mostrare
che negando p si ottiene una contraddizione*

- $p \Rightarrow q \equiv (p \wedge \sim q \Rightarrow \mathbf{F})$ (Dimostrazione per Assurdo)



ALTRE TECNICHE DI DIMOSTRAZIONE

- Dimostrazione per casi:

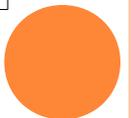
$$(p \Rightarrow q) \wedge (\sim p \Rightarrow q) \Rightarrow q \quad (1)$$

Per dimostrare q è sufficiente dimostrare che, per un certo p , valgono sia $p \Rightarrow q$ che $\sim p \Rightarrow q$

$$(p \vee r) \Rightarrow ((p \Rightarrow q) \wedge (r \Rightarrow q) \Rightarrow q) \quad (2)$$

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

Per dimostrare che $p \wedge r \Rightarrow q \wedge s$ è sufficiente fornire due prove separate per $p \Rightarrow q$ e per $r \Rightarrow s$



ALTRE TAUTOLOGIE UTILI

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



FORME NORMALI

- Usando le leggi ogni proposizione può essere trasformata in una *forma normale*. Si considerano due tipi:

- Forma normale congiuntiva

$$(p_1 \vee p_2 \vee \dots) \wedge (q_1 \vee q_2 \vee \dots) \wedge \dots$$

- Forma normale disgiuntiva

$$(p_1 \wedge p_2 \wedge \dots) \vee (q_1 \wedge q_2 \wedge \dots) \vee \dots$$

dove $p_1 p_2 \dots q_1 q_2 \dots$ sono variabili proposizionali, eventualmente negate

- Utili per dimostrare equivalenza di formule, riducendole in forma normale e verificando se sono equivalenti
- Spesso ridurre a forma normale aumenta la dimensione della formula, perché bisogna usare distributività



IL PRINCIPIO DI RISOLUZIONE

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

Questa legge permette di semplificare una formula in *forma normale congiuntiva*. E' il meccanismo di calcolo alla base della *programmazione logica*.

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

$$\equiv \quad \{\text{Elim-} \Rightarrow, 2 \text{ volte}\}$$

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

$$\Rightarrow \quad \{\text{Transitività-} \Rightarrow \}$$

$$\sim q \Rightarrow r$$

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

$$q \vee r$$



ESEMPIO

- La mia *conoscenza*:
 - *regole*
 - $r \Rightarrow p$
 - $q \Rightarrow r$
 - *fatti*
 - r
 - q
- Vorrei provare che p è una *conseguenza logica* della mia conoscenza
- *Strategia*: faccio vedere che aggiungendo $\sim p$ alla mia conoscenza cado in contraddizione (dimostrazione per assurdo: $p \Rightarrow q \equiv (p \wedge \sim q \Rightarrow \mathbf{F})$)
- Uso la risoluzione per applicare le regole



CALCOLO

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

$$\equiv \quad \{\text{Elim.-} \Rightarrow, 2 \text{ volte}\}$$

$$\underline{(\sim r \vee p)} \wedge (\sim q \vee r) \wedge r \wedge q \wedge \sim p$$

$$\Rightarrow \quad \{\text{Risoluzione applicata ai fattori sottolineati (si noti che entrambi occorrono positivamente, e che } r \equiv r \vee \mathbf{F})\}$$

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

$$\equiv \quad \{\text{Contraddizione}\}$$

$$\mathbf{F} \wedge (\sim q \vee r) \wedge q$$

$$\equiv \quad \{\text{zero}\}$$

$$\mathbf{F}$$

