

Logica per la Programmazione

Lezione 5

- ▶ Dimostrazioni e Tautologie, Ipotesi non tautologiche
 - ▶ Tautologie come schemi di dimostrazione
 - ▶ Dimostrazioni con ipotesi non tautologiche

Tecniche di Dimostrazione come Tautologie:

Dimostrazione per Assurdo

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

$$P \equiv (\neg P \Rightarrow \mathbf{F})$$

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

$$P \Rightarrow Q \equiv (P \wedge \neg Q \Rightarrow \mathbf{F})$$

Mostriamo che sono tautologie

Dimostrazione per Assurdo come Tautologia

► $P \equiv (\neg P \Rightarrow \mathbf{F})$ (*Dimostrazione per Assurdo*)

$$\begin{aligned}
 & (\neg P \Rightarrow \mathbf{F}) \\
 \equiv & \quad \{(\text{Elim.} \Rightarrow) \text{ e } (\text{Doppia Neg.})\} \\
 & (P \vee \mathbf{F}) \\
 \equiv & \quad \{(\text{Unità})\} \\
 & P
 \end{aligned}$$

► $P \Rightarrow Q \equiv (P \wedge \neg Q \Rightarrow \mathbf{F})$ (*Dimostrazione per Assurdo (2)*)

$$\begin{aligned}
 & (P \wedge \neg Q \Rightarrow \mathbf{F}) \\
 \equiv & \quad \{(\text{Elim.} \Rightarrow)\} \\
 & \neg(P \wedge \neg Q) \vee \mathbf{F} \\
 \equiv & \quad \{(\text{De Morgan}) \text{ e } (\text{Doppia neg.})\} \\
 & (\neg P \vee Q) \vee \mathbf{F} \\
 \equiv & \quad \{(\text{Unità})\} \\
 & (\neg P \vee Q) \\
 \equiv & \quad \{(\text{Elim.} \Rightarrow)\} \\
 & P \Rightarrow Q
 \end{aligned}$$

Esempio di Dimostrazione per Assurdo

Dimostriamo per assurdo $(P \vee Q \Rightarrow R) \Rightarrow (P \Rightarrow R)$

Essendo un'implicazione, usiamo (Dimostrazione per Assurdo (2)), quindi dimostriamo $(P \vee Q \Rightarrow R) \wedge \neg(P \Rightarrow R) \Rightarrow \mathbf{F}$

$$\begin{aligned}
 & (P \vee Q \Rightarrow R) \wedge \neg(P \Rightarrow R) \\
 \equiv & \quad \{(\text{Elim.} \Rightarrow), (\neg \Rightarrow)^*\} \\
 & (\neg(P \vee Q) \vee R) \wedge (P \wedge \neg R) \\
 \equiv & \quad \{(\text{De Morgan})\} \\
 & ((\neg P \wedge \neg Q) \vee R) \wedge \neg R \wedge P \\
 \equiv & \quad \{(\text{Complemento})\} \\
 & (\neg P \wedge \neg Q) \wedge \neg R \wedge P \\
 \equiv & \quad \{ \text{“Riarrangiamento dei termini”} \} \\
 & (\neg P \wedge P) \wedge \neg Q \wedge \neg R \\
 \equiv & \quad \{(\text{Contraddizione}) \text{ e } (\text{Zero}) \} \\
 & \mathbf{F}
 \end{aligned}$$

(*) Legge $(\neg \Rightarrow)$: $\neg(A \Rightarrow B) \equiv \neg(\neg A \vee B) \equiv (A \wedge \neg B)$

Altre Tecniche di Dimostrazione come Tautologie

Dimostrazione per **Controposizione**:

Per dimostrare $P \Rightarrow Q$, basta mostrare che $\neg Q \Rightarrow \neg P$

$$\blacktriangleright P \Rightarrow Q \equiv \neg Q \Rightarrow \neg P \quad (\text{Controposizione})$$

Dimostrazione per **Casi**:

Per dimostrare Q , basta mostrare che per un certo P , valgono sia $P \Rightarrow Q$ che $\neg P \Rightarrow Q$

$$\blacktriangleright (P \Rightarrow Q) \wedge (\neg P \Rightarrow Q) \equiv Q \quad (\text{Dim. per casi})$$

Per dimostrare che $P \wedge R \Rightarrow Q \wedge S$, basta fornire due prove separate per $P \Rightarrow Q$ e per $R \Rightarrow S$

$$\blacktriangleright (P \Rightarrow Q) \wedge (R \Rightarrow S) \Rightarrow (P \wedge R \Rightarrow Q \wedge S) \quad (\text{Sempl} \Rightarrow)$$

Tautologie corrispondenti a Tecniche di Dimostrazione

► $(P \Rightarrow Q) \equiv (\neg Q \Rightarrow \neg P)$ *(Controposizione)*

$$\begin{aligned} & \neg Q \Rightarrow \neg P \\ \equiv & \quad \{(\text{Elim.} \Rightarrow) \text{ e } (\text{Doppia Neg.})\} \\ & Q \vee \neg P \\ \equiv & \quad \{(\text{Elim.} \Rightarrow)\} \\ & P \Rightarrow Q \end{aligned}$$

► $(P \Rightarrow Q) \wedge (\neg P \Rightarrow Q) \equiv Q$ *(Dimostrazione per Casi)*

$$\begin{aligned} & (P \Rightarrow Q) \wedge (\neg P \Rightarrow Q) \\ \equiv & \quad \{(\text{Elim.} \Rightarrow) \text{ e } (\text{Doppia Neg.})\} \\ & (\neg P \vee Q) \wedge (P \vee Q) \\ \equiv & \quad \{(\text{Distr.}), \text{ al contrario}\} \\ & (\neg P \wedge P) \vee Q \\ \equiv & \quad \{(\text{Contrad.}) \text{ e } (\text{Unit\`a})\} \\ & Q \end{aligned}$$

Tautologie corrispondenti a Tecniche di Dimostrazione (2)

► $(P \Rightarrow Q) \wedge (R \Rightarrow S) \Rightarrow (P \wedge R \Rightarrow Q \wedge S)$ (Sempl- \Rightarrow)

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

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

$$(\neg P \vee Q) \wedge (\neg R \vee S)$$

$$\Rightarrow \{(\text{Intro-}\vee), \text{due volte}\}$$

$$(\neg P \vee \neg R \vee Q) \wedge (\neg P \vee \neg R \vee S)$$

$$\equiv \{(\text{Distributività}), \text{al contrario}\}$$

$$(\neg P \vee \neg R) \vee (Q \wedge S)$$

$$\equiv \{(\text{De Morgan}), \text{al contrario}\}$$

$$\neg(P \wedge R) \vee (Q \wedge S)$$

$$\equiv \{(\text{Elim.-}\Rightarrow), \text{al contrario}\}$$

$$P \wedge R \Rightarrow Q \wedge S$$

Da Dimostrazioni a Tautologie

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

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

- ▶ Il passo è corretto se e solo se la formula $G \Rightarrow (P \equiv Q)$ è una **tautologia** (usando il **Teorema di Deduzione**, che vedremo)
- ▶ Poiché G è una legge, $G \equiv \mathbf{T}$, da cui segue che $P \equiv Q$ è una tautologia. (Si verifichi la legge $\mathbf{T} \Rightarrow A \equiv A$)

- ▶ Analog., $\begin{array}{c} P \\ \Rightarrow \\ Q \end{array} \quad \{G\}$ sse $G \Rightarrow (P \Rightarrow Q)$ sse $P \Rightarrow Q$

Da Dimostrazioni a Tautologie (2)

- ▶ 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

$$(G_1 \Rightarrow (P \text{ conn}_1 Q)) \wedge (G_2 \Rightarrow (Q \text{ conn}_2 R))$$

- ▶ Poiché G_1 e G_2 sono tautologie (e $(\mathbf{T} \Rightarrow A \equiv A)$), abbiamo $(G_1 \Rightarrow (P \text{ conn}_1 Q)) \wedge (G_2 \Rightarrow (Q \text{ conn}_2 R)) \equiv (P \text{ conn}_1 Q) \wedge (Q \text{ conn}_2 R)$
- ▶ Se $conn_1$ e $conn_2$ rappresentano lo stesso connettivo e il connettivo è transitivo (come lo sono \equiv e \Rightarrow), dalla prova segue che

$$P \text{ conn } R$$

come richiedeva la nostra intuizione

Uso di Ipotesi non Tautologiche come Giustificazioni

- ▶ Riassumendo: per dimostrare che da una ipotesi P segue una conseguenza Q , possiamo dimostrare che
 - ▶ $P \Rightarrow Q$ è una tautologia
 - ▶ $\neg Q \Rightarrow \neg P$ è una tautologia
 - ▶ $P \wedge \neg Q \Rightarrow \mathbf{F}$ 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 $P \Rightarrow Q$ 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: $P \Rightarrow (P \wedge Q \equiv Q)$
- ▶ Dimostrazione: proviamo che $(P \wedge Q \equiv Q)$ è vera nell'ipotesi che P sia vera:

$$\begin{aligned}
 & P \wedge Q \\
 \equiv & \quad \{ \text{Ip: } P \} \\
 & \mathbf{T} \wedge Q \\
 \equiv & \quad \{ (\text{Unità}) \} \\
 & Q
 \end{aligned}$$

- ▶ Nelle giustificazioni abbiamo indicato esplicitamente con “**Ip:** ...” il fatto che P è un'ipotesi e non una tautologia

Uso di Ipotesi come Giustificazioni: Esempio 2

- ▶ Teorema: $(P \Rightarrow (Q \equiv R)) \Rightarrow (P \wedge R \Rightarrow Q)$
- ▶ Dimostrazione: proviamo che $(P \wedge R \Rightarrow Q)$ è vera nell'ipotesi che $(P \Rightarrow (Q \equiv R))$ sia vera:

$P \wedge R$	
\Rightarrow	{Ip: $(P \Rightarrow (Q \equiv R))$, P occorre pos.}
$(Q \equiv R) \wedge R$	
\equiv	{(Elim.- \equiv)}
$(Q \Rightarrow R) \wedge (R \Rightarrow Q) \wedge R$	
\Rightarrow	{(Modus Ponens), $(R \Rightarrow Q) \wedge R$ occorre pos}
$(Q \Rightarrow R) \wedge Q$	
\Rightarrow	{Sempl.- \wedge , occ. pos.}
Q	

In conclusione

Lo schema di dimostrazione:

$$\begin{array}{ccc}
 & P_1 & \\
 \text{conn}_1 & & \{G_1\} \\
 & P_2 & \\
 \text{conn}_2 & & \{G_2\} \\
 & \dots & \\
 & P_{n-1} & \\
 \text{conn}_{n-1} & & \{G_{n-1}\} \\
 & P_n &
 \end{array}$$

rappresenta una dimostrazione della seguente tautologia:

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

In conclusione (cont.)

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

- ▶ Allora abbiamo

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

- ▶ Se 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 dimostrazione di

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

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

$$P_1 \text{ conn } P_n$$

Esempio: Sillogismo Disgiuntivo

Dimostrare la seguente tautologia usando giustificazioni non tautologiche

- ▶ $(P \vee Q) \wedge (P \Rightarrow R) \wedge (Q \Rightarrow S) \Rightarrow (R \vee S)$ (Sillogismo disgiuntivo)

Anticipiamo la legge

$$A \Rightarrow (B \Rightarrow C) \equiv (A \wedge B \Rightarrow C) \quad (\text{Sempl. Sinistra } 2\text{-}\Rightarrow)$$

Quindi è sufficiente dimostrare che

$$(P \Rightarrow R) \wedge (Q \Rightarrow S) \Rightarrow ((P \vee Q) \Rightarrow (R \vee S))$$

$$\begin{aligned} & P \vee Q \\ \Rightarrow & \quad \{\text{Ip: } (P \Rightarrow R), P^+ \text{ (cioè } P \text{ occorre pos.)}\} \\ & R \vee Q \\ \Rightarrow & \quad \{\text{Ip: } (Q \Rightarrow S), Q^+ \text{ (cioè } Q \text{ occorre pos.)}\} \\ & R \vee S \end{aligned}$$

Esempio: (Sempl.- \Rightarrow)

Dimostrare la seguente tautologia usando giustificazioni non tautologiche

$$\blacktriangleright (P \Rightarrow Q) \wedge (R \Rightarrow S) \Rightarrow (P \wedge R \Rightarrow Q \wedge S) \quad (\text{Sempl.-}\Rightarrow)$$

$$\begin{array}{l} \Rightarrow P \wedge R \\ \Rightarrow \quad \quad \quad \{ \text{Ip: } (P \Rightarrow Q), P^+ \} \\ \Rightarrow Q \wedge R \\ \Rightarrow \quad \quad \quad \{ \text{Ip: } (R \Rightarrow S), R^+ \} \\ \Rightarrow Q \wedge S \end{array}$$

Esempio: Dimostrazione per Casi

Dimostrare $(P \vee Q \Rightarrow R) \Rightarrow (P \Rightarrow R)$.

Per (Dimostrazione per Casi), basta mostrare separatamente

$Q \Rightarrow ((P \vee Q \Rightarrow R) \Rightarrow (P \Rightarrow R))$ e $\neg Q \Rightarrow ((P \vee Q \Rightarrow R) \Rightarrow (P \Rightarrow R))$.

Lo facciamo usando Q e $\neg Q$ come ipotesi non tautologiche.

Caso Q

$$\begin{array}{l}
 P \vee Q \Rightarrow R \\
 \equiv \\
 P \vee \mathbf{T} \Rightarrow R \quad \{ \text{Ip: } Q \} \\
 \equiv \\
 \neg \mathbf{T} \vee R \quad \{ (\text{Zero}), (\text{Elim.} \Rightarrow) \} \\
 \equiv \\
 R \quad \{ (\mathbf{T:F}), (\text{Unità}) \} \\
 \Rightarrow \\
 \neg P \vee R \quad \{ (\text{Intro.} \vee) \} \\
 \equiv \\
 P \Rightarrow R \quad \{ (\text{Elim.} \Rightarrow) \}
 \end{array}$$

Caso $\neg Q$

$$\begin{array}{l}
 P \vee Q \Rightarrow R \\
 \equiv \\
 P \vee \mathbf{F} \Rightarrow R \quad \{ \text{Ip: } \neg Q \} \\
 \equiv \\
 P \Rightarrow R \quad \{ (\text{Unità}) \}
 \end{array}$$

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)
- ▶ $(P \Rightarrow Q) \vee (P \Rightarrow R) \equiv (P \Rightarrow Q \vee R)$
- ▶ $(P \Rightarrow R) \wedge (Q \Rightarrow R) \equiv (P \vee Q \Rightarrow R)$ (Sempl.Sinistra- \Rightarrow)
- ▶ $(P \Rightarrow R) \vee (Q \Rightarrow R) \equiv (P \wedge Q \Rightarrow R)$
- ▶ $P \Rightarrow (Q \Rightarrow R) \equiv (P \wedge Q \Rightarrow R)$ (Sempl.Sinistra-2- \Rightarrow)
- ▶ Esercizio: dimostrare che sono tautologie