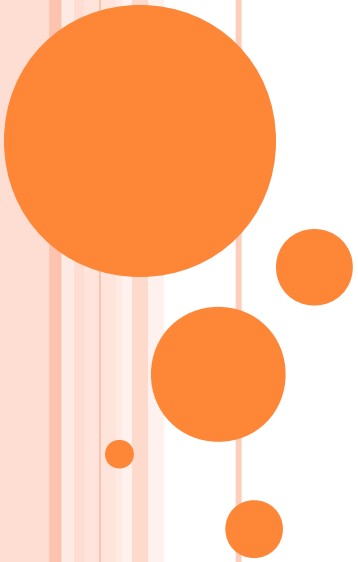

# DIMOSTRAZIONI DI TAUTOLOGIE

**Corso di Logica per la Programmazione**

**A.A. 2010/11**

***Andrea Corradini, Paolo Mancarella***

# DIMOSTRAZIONE DI TAUTOLOGIE

**Abbiamo detto che:** Per dimostrare che $p$ è una tautologia possiamo:

- Usare le tabelle di verità, sfruttando quelle dei connettivi
  - Del tutto meccanico, richiede di considerare $2^n$ casi, dove $n$ è il numero di variabili proposizionali in $p$
- Cercare di costruire una dimostrazione
  - Usando delle leggi (tautologie già dimostrate)
  - Usando opportune *regole di inferenza*
  - Si possono impostare vari tipi di dimostrazioni
- Mostrare che non è una tautologia
  - individuando valori delle variabili proposizionali che rendono falsa $p$

- Vediamo come si costruiscono le tabelle di verità

# Interpretazione di una formula proposizionale

- **Interpretazione:** funzione da variabili proposizionali a {T, F}
- Un'interpretazione determina il valore di verità di una formula
  - Formula $(P \wedge Q) \vee \neg R$
  - Interpretazione $\{P \mapsto T, Q \mapsto F, R \mapsto T\}$
  - Valore di verità usando una tabella (sfruttando quella dei connettivi):

| $P$ | $Q$ | $R$ | $(P$ | $\wedge$ | $Q)$ | $\vee$ | $\neg$ | $R$ |
|---|---|---|---|---|---|---|---|---|
| T | F | F | T | F | F | **T** | T | F |
| | | | (1) | (2) | (1) | **(3)** | (2) | (1) |

| $P$ | $Q$ | $\neg P$ | $P \wedge Q$ | $P \vee Q$ | $P \Rightarrow Q$ | $P \equiv Q$ | $P \Leftarrow Q$ |
|---|---|---|---|---|---|---|---|
| T | T | F | T | T | T | T | T |
| T | F | F | F | T | F | F | T |
| F | T | T | F | T | T | F | F |
| F | F | T | F | F | T | T | T |

# Tabella di Verità di una formula: raccoglie tutte le interpretazioni

- Un esempio:

| $P$ | $Q$ | $R$ | $(P$ | $\wedge$ | $Q)$ | $\vee$ | $\neg$ | $R$ |
|---|---|---|---|---|---|---|---|---|
| T | T | T | T | T | T | **T** | F | T |
| T | T | F | T | T | T | **T** | T | F |
| T | F | T | T | F | F | **F** | F | T |
| T | F | F | T | F | F | **T** | T | F |
| F | T | T | F | F | T | **F** | F | T |
| F | T | F | F | F | T | **T** | T | F |
| F | F | T | F | F | F | **F** | F | T |
| F | F | F | F | F | F | **T** | T | F |
| | | | (1) | (2) | (1) | (3) | (2) | (1) |

# DIMOSTRAZIONE DI TAUTOLOGIE

**Abbiamo detto che:** Per dimostrare che $p$ è una tautologia possiamo:

- Usare le tabelle di verità, sfruttando quelle dei connettivi
  - Del tutto meccanico, richiede di considerare $2^n$ casi, dove $n$ è il numero di variabili proposizionali in $p$
- Cercare di costruire una dimostrazione
  - Usando delle leggi (tautologie già dimostrate)
  - Usando opportune *regole di inferenza*
  - Si possono impostare vari tipi di dimostrazioni
- Mostrare che non è una tautologia
  - individuando valori delle variabili proposizionali che rendono falsa $p$

# DIMOSTRAZIONI: COMINCIAMO DALL'ARITMETICA

- Mostriamo che $(a+b)(a-b) = a^2-b^2$

$(a + b)(a - b)$

= {distributività della moltiplicazione rispetto all'addizione, ovvero, in formule, $(y+z)x = yx+zx$ applicata con $a$ al posto di $y$, $b$ al posto di $z$ e $(a-b)$ al posto di $x$}

$a(a - b) + b(a - b)$

= {distributività della moltiplicazione rispetto alla sottrazione, due volte, ovvero, in formule, $x(y-z) = xy-xz$ applicata la prima volta con $x=a$, $y=a$, $z=b$ e la seconda con $x=b$, $y=a$, $z=b$}

$(aa - ab) + (ba - bb)$

= { $xx=x^2$, e associatività dell'addizione }

$a^2 - ab + ba - b^2$

= { commutatività della moltiplicazione, e $-x+x=0$ }

$a^2 + 0 - b^2$

= { $x + 0 = x$ }

$a^2 - b^2$

# STRUTTURA DI UNA SEMPLICE DIMOSTRAZIONE

- Nella dimostrazione vista abbiamo
  - una sequenza di eguaglianze
    - es: $a^2 + 0 - b^2 = a^2 - b^2$
  - ogni eguaglianza ha come giustificazione una o più ***leggi*** (dell'aritmetica)
    - es: $\{ x + 0 = x \}$
  - La correttezza di ogni eguaglianza è basata su una ***regola di inferenza***: il principio di sostituzione.

    Informalmente:

**"Sostituendo eguali con eguali il valore non cambia"**

- es: dalla legge sappiamo che $a^2 + 0 = a^2$
- sostituendo $a^2 + 0$ con $a^2$ in $a^2 + 0 - b^2$ otteniamo $a^2 - b^2$

# IL PRINCIPIO DI SOSTITUZIONE

- Esprime una proprietà fondamentale dell'***eguaglianza***.
- Nel Calcolo Proposizionale esprime una proprietà dell'***equivalenza***.

- **"Se *p* = *q* allora il valore di una espressione *r* in cui compare *p* non cambia se *p* è sostituito con *q*"**

- In formule, $r = r[q/p]$ o $r = r^{q}_{p}$

- Qui $p = q$ è una legge, e $r = r[q/p]$ è l'eguaglianza da essa giustificata, grazie al principio di sostituzione

# LEGGI DEL CALCOLO PROPOSIZIONALE

- Una ***legge*** è una tautologia.
- Di solito una tautologia viene chiamata "legge" quando descrive una proprietà di uno o più connetttivi logici, o quando è usata come giustificazione nelle dimostrazioni.
- Per ogni legge che introduciamo, bisognerebbe verificare che sia una tautologia
  - a volte è ovvio
  - a volte lo mostreremo con tabelle di verità
  - a volte presenteremo una dimostrazione in cui usiamo ***solo leggi introdotte in precedenza***
  - spesso lo lasceremo come esercizio...

# LEGGI PER L'EQUIVALENZA ( ≡ )

- $p \equiv p$ (Riflessività)
- $(p \equiv q) \equiv (q \equiv p)$ (Simmetria)
- $((p \equiv q) \equiv r) \equiv (p \equiv (q \equiv r))$ (Associatività)
- $(p \equiv \mathbf{T}) \equiv p$ (Unità)
- $((p \equiv q) \wedge (q \equiv r)) \Rightarrow (p \equiv r)$ (Transitività)

- Esempio di dimostrazione:

(Unità)

| $P$ | $(P$ | $\equiv$ | $T)$ | $\equiv$ | $P$ |
|---|---|---|---|---|---|
| T | T | T | T | **T** | T |
| F | F | F | T | **T** | F |
| | (1) | (2) | (1) | (3) | (1) |

# LEGGI PER CONGIUNZIONE E DISGIUNZIONE

| | |
|---|---|
| $p \vee q \equiv q \vee p$ | (Commutatività) |
| $p \wedge q \equiv q \wedge p$ | |
| $p \vee (q \vee r) \equiv (p \vee q) \vee r$ | (Associatività) |
| $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$ | |
| $p \vee p \equiv p$ | (Idempotenza) |
| $p \wedge p \equiv p$ | |
| $p \wedge \mathbf{T} \equiv p$ | (Unità) |
| $p \vee \mathbf{F} \equiv p$ | |
| $p \wedge \mathbf{F} \equiv \mathbf{F}$ | (Zero) (Dominanza) |
| $p \vee \mathbf{T} \equiv \mathbf{T}$ | |
| $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ | (Distributività) |
| $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ | |

- Esercizio: dimostrare alcune leggi con tabelle di verità

# DIMOSTRAZIONI DI EQUIVALENZE TAUTOLOGICHE

- Come per equazioni algebriche si può provare $\mathbf{P_1 \equiv P_n}$ così:

  $\mathbf{P_1}$

  $\equiv$ {giustificazione$_1$}

  $P_2$

  .....

  $\equiv$ {giustificazione$_{n-1}$}

  $\mathbf{P_n}$

- dove ogni passo ha la forma

  **R**

  **$\equiv$ { P $\equiv$ Q }**

  **R[Q/P]**

- Ogni passo è corretto per il *Principio di Sostituzione*

# UNA SEMPLICE DIMOSTRAZIONE

**Teorema:** $p \vee (q \vee r) \equiv (p \vee q) \vee (p \vee r)$

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

$\equiv$ { $p \vee q \equiv q \vee p$ (Commutatività)}

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

$\equiv$ {Associatività}

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

$\equiv$ {Associatività}

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

$\equiv$ {Idempotenza}

$q \vee (p \vee r)$

$\equiv$ {Associatività}

$(q \vee p) \vee r$

$\equiv$ {Commutavità}

$(p \vee q) \vee r$

$\equiv$ {Associatività}

$p \vee (q \vee r)$

# COMMENTI

- La dimostrazione fatta usando le leggi garantisce la correttezza della dimostrazione grazie al Principio di Sostituzione

- Naturalmente la tecnica non automatizza le dimostrazioni. Rimane a carico nostro la scelta delle leggi da usare, da quale membro della equivalenza partire, l'organizzazione della sequenza dei passaggi

- Nel seguito semplificheremo le dimostrazioni, saltando passi ovvi come l'applicazione di Associatività, Commutatività e Idempotenza

# LEGGI DELLA NEGAZIONE

| | |
|---|---|
| $\sim(\sim p) \equiv p$ | (Doppia negazione) |
| $p \vee \sim p \equiv \mathbf{T}$ | (Terzo escluso) |
| $p \wedge \sim p \equiv \mathbf{F}$ | (Contraddizione) |
| $\sim(p \wedge q) \equiv \sim p \vee \sim q$ | (De Morgan) |
| $\sim(p \vee q) \equiv \sim p \wedge \sim q$ | |
| $\sim\mathbf{T} \equiv \mathbf{F}$ | (**T**:**F**) |
| $\sim\mathbf{F} \equiv \mathbf{T}$ | (**F**:**T**) |

- Esercizio: dimostrare alcune leggi con tabelle di verità

# LEGGI DELL'IMPLICAZIONE

- $(p \Rightarrow q) \equiv (\sim p \vee q)$ (elim- $\Rightarrow$)

| $P$ | $Q$ | $(P$ | $\Rightarrow$ | $Q)$ | $\equiv$ | $(\neg$ | $P$ | $\vee$ | $Q)$ |
|---|---|---|---|---|---|---|---|---|---|
| T | T | T | T | T | **T** | F | T | T | T |
| T | F | T | F | F | **T** | F | T | F | F |
| F | T | F | T | T | **T** | T | F | T | T |
| F | F | F | T | F | **T** | T | F | T | F |
| | | (1) | (2) | (1) | (4) | (2) | (1) | (3) | (1) |

- $(p \equiv q) \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$ (elim- $\equiv$ )
- $(p \Leftarrow q) \equiv (q \Rightarrow p)$ (elim-$\Leftarrow$)

# COMMENTI

- Si può mostrare che **tutte** le tautologie del Calcolo Proposizionale sono dimostrabili a partire dall'insieme delle leggi visto sinora

- Conviene comunque, per motivi di espressività e compattezza delle definizioni, introdurre altre leggi che corrispondono, per esempio, ad assodate tecniche di dimostrazione.