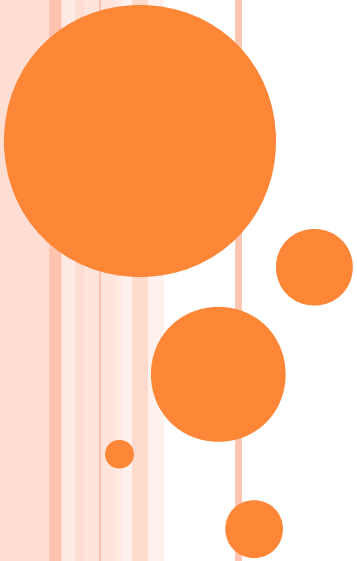

DIMOSTRAZIONI DI TAUTOLOGIE

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
  - 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

- Ma come è strutturata una dimostrazione?

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 $r = r_p^q$

- 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)

- Esempio di dimostrazione:

(Unità)

p	T	p ≡ T	(p ≡ T) ≡ p
T	T	T	T
F	T	F	T

LEGGI PER L'EQUIVALENZA (≡)

- $((p \equiv q) \wedge (q \equiv r)) \Rightarrow (p \equiv r)$ (Transitività)
- Dimostrazione:

p	q	r	$p \equiv q$	$q \equiv r$	$(p \equiv q) \wedge (q \equiv r)$	$p \equiv r$	$((p \equiv q) \wedge (q \equiv r)) \Rightarrow (p \equiv r)$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	T
T	F	T	F	F	F	T	T
T	F	F	F	T	F	F	T
F	T	T	F	T	F	F	T
F	T	F	F	F	F	T	T
F	F	T	T	F	F	F	T
F	F	F	T	T	T	T	T

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)
$p \vee \mathbf{T} \equiv \mathbf{T}$	
$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	(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	$p \Rightarrow q$	$\sim p$	$\sim p \vee q$
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

- $(p \equiv q) \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$ (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.

TORNIAMO ALL'ESEMPIO DAL TEST

- **Premesse:**
  - Se Corrado va al cinema, allora ci va anche Antonio; **(C ⇒ A)**
  - Condizione necessaria perché Antonio vada al cinema è che ci vada Bruno. **(A ⇒ B)**
- **Il giorno successivo possiamo affermare con certezza che:**
  - Se Corrado è andato al cinema, allora ci è andato anche Bruno
    - **(C ⇒ B)**
  - Nessuno dei tre amici è andato al cinema
    - **(~A ∧ ~B ∧ ~C)**
  - Se Bruno è andato al cinema, allora ci è andato anche Corrado
    - **(B ⇒ C)**
  - Se Corrado non è andato al cinema, allora non ci è andato nemmeno Bruno
    - **(~C ⇒ ~B)**

COME POSSIAMO ESSERE CERTI DELLA RISPOSTA?

- Basta determinare quale delle seguenti formule è una tautologia:

1) $((C \Rightarrow A) \wedge (A \Rightarrow B)) \Rightarrow (C \Rightarrow B)$
2) $((C \Rightarrow A) \wedge (A \Rightarrow B)) \Rightarrow (\sim A \wedge \sim B \wedge \sim C)$
3) $((C \Rightarrow A) \wedge (A \Rightarrow B)) \Rightarrow (B \Rightarrow C)$
4) $((C \Rightarrow A) \wedge (A \Rightarrow B)) \Rightarrow (\sim C \Rightarrow \sim B)$

- Si possono verificare con tabelle di verità o dimostrazioni, usando le leggi viste.
- Mostreremo che (1) è una tautologia
- Esercizio: mostrare che (2), (3) e (4) **non sono tautologie**

DIMOSTRIAMO CHE (1) E' UNA TAUTOLOGIA (omettiamo le giustificazioni)

$$((C \Rightarrow A) \wedge (A \Rightarrow B)) \Rightarrow (C \Rightarrow B)$$

$$\equiv \sim ((C \Rightarrow A) \wedge (A \Rightarrow B)) \vee (C \Rightarrow B)$$

$$\equiv \sim ((C \Rightarrow A) \wedge (A \Rightarrow B)) \vee (\sim C \vee B)$$

$$\equiv (\sim (C \Rightarrow A) \vee \sim (A \Rightarrow B)) \vee (\sim C \vee B)$$

$$\equiv (\sim (\sim C \vee A) \vee \sim (\sim A \vee B)) \vee (\sim C \vee B)$$

$$\equiv ((C \wedge \sim A) \vee (A \wedge \sim B)) \vee (\sim C \vee B)$$

$$\equiv ((C \wedge \sim A) \vee \sim C) \vee ((A \wedge \sim B) \vee B)$$

$$\equiv ((C \vee \sim C) \wedge (\sim A \vee \sim C)) \vee ((A \vee B) \wedge (\sim B \vee B))$$

$$\equiv (T \wedge (\sim A \vee \sim C)) \vee ((A \vee B) \wedge T)$$

$$\equiv (\sim A \vee \sim C) \vee (A \vee B)$$

$$\equiv (T \vee \sim C \vee B)$$

$$\equiv T$$

TRANSITIVITA' DELL'IMPLICAZIONE: DIMOSTRAZIONE CON TABELLE DI VERITA'

p	q	r	$p \Rightarrow q$	$q \Rightarrow r$	$(p \Rightarrow q) \wedge (q \Rightarrow r)$	$p \Rightarrow r$	$((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	F	T
T	F	T	F	T	F	T	T
T	F	F	F	T	F	F	T
F	T	T	T	T	T	T	T
F	T	F	T	F	F	T	T
F	F	T	T	T	T	T	T
F	F	F	T	T	T	T	T

LEGGI DI ASSORBIMENTO (1)

- $p \wedge (p \vee q) \equiv p$ (Assorbimento)
- $p \vee (p \wedge q) \equiv p$

Prova (semantica) di $p \wedge (p \vee q) \equiv p$

p	q	$p \vee q$	$p \wedge (p \vee q)$
T	T	T	T
T	F	T	T
F	T	T	F
F	F	F	F

LEGGI DI ASSORBIMENTO (2)

- $p \wedge (p \vee q) \equiv p$ (Assorbimento)
- $p \vee (p \wedge q) \equiv p$

Prova (calcolo) di $p \wedge (p \vee q) \equiv p$

$p \wedge (p \vee q)$

$\equiv$ {Unità}

$(p \vee \mathbf{F}) \wedge (p \vee q)$

$\equiv$ {Distributività}

$p \vee (\mathbf{F} \wedge q)$

$\equiv$ {Zero}

$p \vee \mathbf{F}$

$\equiv$ {Unità}

p

LEGGI DEL COMPLEMENTO (1)

- $p \vee (\sim p \wedge q) \equiv p \vee q$ (Complemento)
- $p \wedge (\sim p \vee q) \equiv p \wedge q$

Prova (semantica) di $p \vee (\sim p \wedge q) \equiv p \vee q$

p	q	~p	p ∨ q	~p ∧ q	p ∨ (~p ∧ q)
T	T	F	T	F	T
T	F	F	T	F	T
F	T	T	T	T	T
F	F	T	F	F	F

LEGGI DEL COMPLEMENTO (2)

- $p \vee (\sim p \wedge q) \equiv p \vee q$ (Complemento)
- $p \wedge (\sim p \vee q) \equiv p \wedge q$

Prova (calcolo) di $p \vee (\sim p \wedge q) \equiv p \vee q$

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

$\equiv$ {Distributività}

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

$\equiv$ {Terzo escluso}

$\mathbf{T} \wedge (p \vee q)$

$\equiv$ {Unità}

$(p \vee q)$

INSIEMI FUNZIONALMENTE COMPLETI DI CONNETTIVI LOGICI

- Abbiamo introdotto 6 connettivi logici:

not	$\sim p$	negazione
and	$p \wedge q$	congiunzione
or	$p \vee q$	disgiunzione
se p allora q	$p \Rightarrow q$	implicazione
p se e solo se q	$p \equiv q$	equivalenza
p se q	$p \Leftarrow q$	conseguenza

- Alcuni possono essere definiti in termini di altri.
- Molti sottoinsiemi sono "funzionalmente completi", cioè permettono di derivare tutti gli altri.
- **Esercizio**: Mostrare che $\{\wedge, \sim\}$, $\{\vee, \sim\}$ e $\{\Rightarrow, \sim\}$ sono funzionalmente completi

IL CONNETTIVO "NAND"

- Si consideri il connettivo proposizionale binario **nand** la cui semantica è definita dalla seguente tabella di verità:

p	q	p nand q
T	T	F
T	F	T
F	T	T
F	F	T

- Si provi che l'insieme **{ nand }** è funzionalmente completo.