Logica per la programmazione

Franco Turini

turini@di.unipi.it

IPSE DIXIT

- Occorre dire, anzitutto, quale oggetto riguardi ed a quale disciplina spetti la presente indagine, che essa cioè riguarda la dimostrazione e spetta alla scienza dimostrativa; in seguito, bisogna precisare che cosa sia la premessa, cosa sia il termine, cosa sia il sillogismo ...

  Aristotele

- La logica è la disciplina che studia le condizioni di correttezza del ragionamento

Si consideri la frase: *in un dato campione di pazienti, chi ha fatto uso di droghe pesanti ha utilizzato anche droghe leggere*. Quali delle seguenti osservazioni relative ai pazienti del campione si può dedurre da essa?

1. Chi ha fatto uso di droghe leggere ha utilizzato anche droghe pesanti
2. Chi non ha fatto uso di droghe leggere non ha utilizzato droghe pesanti
3. Chi non ha fatto uso di droghe pesanti non ha utilizzato droghe leggere
4. Chi non ha fatto uso di droghe leggere ha utilizzato droghe pesanti

Tre amici, Antonio, Bruno e Corrado, sono incerti se andare al cinema. Si sa che:

•Se Corrado va al cinema, allora ci va anche Antonio;

•Condizione necessaria perché Antonio vada al cinema è che ci vada Bruno.

Il giorno successivo possiasmo affermare con certezza che:

1. Se Corrado è andato al cinema, allora ci è andato anche Bruno
2. Nessuno dei tre amici è andato al cinema
3. Se Bruno è andato al cinema, allora ci è andato anche Corrado
4. Se Corrado non è andato al cinema, allora non ci è andato nememno Bruno

Formalizzazione di dimostrazioni

- Caso semplice: dimostrazioni di equivalenza (=)

E1

= {giustificazione_1}

E2

= {giustificazione_2}

....

= {giustificazione_n-1}

En

Principio di sostituzione

- Se p=q allora una espressione r in cui a p è sostituito q (o viceversa) mantiene il suo valore

- In formule

$$r = r[q/p]$$

$$r = r_p^q$$

DIMOSTRAZIONI: COMINCIAMO DALLA ARITMETICA

(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

Il calcolo delle proposizioni

- Le proposizioni (enunciati dichiarativi) sono asserzioni a cui sia assegnabile in modo univoco un valore di verità in accordo ad una interpretazione del mondo a cui si riferiscono.

- “dichiarativi sono non già tutti i discorsi, ma quelli in cui sussiste una enunciazione vera oppure falsa” *Aristotele*

ESEMPI DI PROPOSIZIONI (IN ACCORDO ALLA INTERPRETAZIONE OVVIA)

1. Roma è la capitale d'Italia
2. La Francia è uno stato del continente asiatico
3. $1+1 = 2$
4. $2+2 = 3$

Esempi di non proposizioni

1. Che ora è?

2. Leggete queste note con attenzione

3. X+1 = 2

CONNETTIVI LOGICI

Connettivo	*Forma simbolica*	*Operazione corrispondente*
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

Sintassi (struttura) delle proposizioni

$$
\begin{aligned}
\mathrm{Prop} ::= {} & \mathrm{Prop} \equiv \mathrm{Prop} \mid \mathrm{Prop} \wedge \mathrm{Prop} \mid \mathrm{Prop} \vee \mathrm{Prop} \mid \\
& \mathrm{Prop} \Rightarrow \mathrm{Prop} \mid \mathrm{Prop} \Leftarrow \mathrm{Prop} \mid \\
& \mathrm{Atom} \mid \sim\mathrm{Atom} \\
\mathrm{Atom} ::= {} & \mathbf{T} \mid \mathbf{F} \mid \mathrm{Ide} \mid (\mathrm{Prop}) \\
\mathrm{Ide} ::= {} & \mathrm{p} \mid \mathrm{q} \mid \ldots\ldots
\end{aligned}
$$

Semantica (significato) delle proposizioni

p	q	~p	p∧q	p∨q	p⇒q	p≡q	p⇐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

Tautologie

- Una proposizione è una tautologia se e soltanto se il suo valore di verità rimane T indipendentemente dal valore di verità delle sue componenti elementari.
- Esempio: $p \vee \sim p$ (vedi tabella di verità)

- La proprietà di essere una tautologia e il principio di sostituzione ci permettono di dimostrare
  - equivalenze $p \equiv q$
  - Implicazioni tautologiche $p \Rightarrow q$

Leggi

- Le leggi sono tautologie (dimostrabili p.e. con le tabelle di verità) utili per effettuare le dimostrazioni
- Leggi per $\equiv$

$p \equiv p$	(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)

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)

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

ESEMPIO

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

Prova:

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

$\equiv$ {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 (tautologie utili per trasformare proposizioni in proposizioni equivalenti) garantisce la correttezza della dimostrazione
- 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.

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

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 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)

$\sim p \vee \sim q \equiv \sim(p \wedge q)$ (De Morgan)

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

$\sim\mathbf{T} \equiv \mathbf{F}$ **(T:F)**

$\sim\mathbf{F} \equiv \mathbf{T}$

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)
F	F	T	F	F	F
F	T	T	T	T	T
T	F	F	T	F	T
T	T	F	T	F	T

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}

$(p \vee q)$

Leggi dell'implicazione (1)

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

p	q	$(p \Rightarrow q)$	$\sim p$	$(\sim p \vee q)$
F	F	T	T	T
F	T	T	T	T
T	F	F	F	F
T	T	T	F	T

Leggi dell'implicazione (2)

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

- Tutte le tautologie del calcolo proposizionale sono derivabili dall'insieme delle leggi visto

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

Leggi derivate

- $(p \wedge (p \Rightarrow q)) \Rightarrow q$ (modus ponens)
- $(p \Rightarrow q) \equiv (\sim q \Rightarrow \sim p)$ (controposizione)
- $(p \Rightarrow \sim p) \equiv \sim p$ (reductio ad absurdum)
- $((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$ (transitività)

Correttezza del modus ponens

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

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

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

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

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

$\equiv$ {DeMorgan}

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

$\equiv$ {DeMorgan}

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

$\equiv$ {Complemento}

$\sim p \vee \sim q \vee q$

$\equiv$ {TerzoEscluso}

$\sim p \vee \mathbf{T}$

$\equiv$ {Zero}

$\mathbf{T}$

Il sillogismo

uomo(x) = x è un uomo

mortale(x)= x è mortale

uomo(x) $\Rightarrow$ mortale(x)

Istanziando x con Socrate abbiamo:

uomo(Socrate) $\wedge$ (uomo(Socrate) $\Rightarrow$ mortale(Socrate))

$\Rightarrow$ {modus ponens}

Mortale (Socrate)

Esercizi del test (1)

- dp= fare uso di droghe pesanti
- dl = fare uso di droghe leggere

$dp \Rightarrow dl$

$\equiv$ {contropositiva}

$\sim dl \Rightarrow \sim dp$

Esercizi del test (2)

- Se Corrado va al cinema, allora ci va anche Antonio
  - Corrado $\Rightarrow$ Antonio
- Condizione necessaria perché Antonio vada al cinema è che ci vada Bruno
  - Antonio $\Rightarrow$ Bruno

(Corrado $\Rightarrow$ Antonio) $\wedge$ (Antonio $\Rightarrow$ Bruno)

$\Rightarrow$ {transitività}

Corrado $\Rightarrow$ Bruno