

Fondamenti di Informatica
per la Sicurezza
a.a. 2006/07

Logica proposizionale

Stefano Ferrari



UNIVERSITÀ DEGLI STUDI DI MILANO
DIPARTIMENTO DI TECNOLOGIE DELL'INFORMAZIONE

Logica formale

La **logica formale** è una branca della matematica che studia i principi su cui si basa la formalizzazione di asserzioni e delle regole di inferenza.

Semplificando, si può dire che la logica formale permette una formalizzazione del "ragionamento".

Formalizzazione

Formalizzare significa tradurre dal linguaggio naturale in un linguaggio semplificato con una sintassi rigida e precisa.

Un linguaggio con regole rigide serve:

- per comunicare con le macchine;
- per comunicare con altre persone;
- per progettare algoritmi.

Questo procedimento è necessario in molte discipline.

Logiche

Ambiti diversi hanno esigenze diverse.

A seconda della necessità ci si può appoggiare, fra le altre, alla logica:

- **classica**: studia i processi per trarre conclusioni a partire da assunzioni;
- **intuizionista**: basata su un approccio costruttivo, utile per esigenze pratiche di realizzazione;
- **temporale**: arricchita da operatori per indicare intervalli temporali;
- **fuzzy**: infinite gradazioni di verità.

Logica proposizionale

La logica proposizionale studia gli schemi di composizione di frasi dichiarative.

Queste frasi saranno chiamate **proposizioni**.

La logica non indaga sul significato delle singole proposizioni, ma solo sugli schemi in cui le proposizioni possono essere composte mediante operatori detti **connettivi logici**.

Si occupa di stabilire la verità o la falsità di asserzioni (espressioni linguistiche) ottenute componendo proposizioni semplici.

Linguaggio formale

Bisogna stabilire:

- cosa si vuole formalizzare;
- **alfabeto**:
elementi simbolici usati per la rappresentazione;
- **sintassi**:
come si rappresentano gli oggetti del discorso;
- **semantica**:
quale significato si dà a tali rappresentazioni.

Alfabeto

Le proposizioni sono costruite usando:

- **costanti** (valori di verità): $\{F, V\}$
(indicati anche come: $\{F, T\}$, $\{0, 1\}$, $\{\perp, \top\}$)
- **simboli enunciativi**: $\{a, b, \dots, z\}$
- **connettivi**: $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$
- **simboli ausiliari**: $\text{"(", "}"$

Proposizioni semplici

Una **proposizione semplice** (o **atomica**) è un'affermazione che:

- non dipende da variabili;
- può essere **vera** o **falsa**;
- viene formalizzata da un simbolo enunciativo.

Esempi:

- ogni triangolo si può inscrivere in un cerchio *vera*
- Roma è in Francia *falsa*

NB: non interessa il significato delle proposizioni, solo se sono vere o false.

Connettivi (1)

Le proposizioni semplici sono composte per mezzo dei **connettivi logici**:

- **coniunzione**: \wedge , **et**, AND, e
 $a \wedge b$ è vera se lo è sia a che b ;
- **disgiunzione**: \vee , **vel**, OR, o
 $a \vee b$ è vera quando lo è almeno uno fra a e b ;
- **negazione**: \neg , \sim , **non**, NOT, non
 $\neg a$ è vera quando a è falsa;

Connettivi (2)

- **implicazione** (condizionale): \rightarrow , se ... allora
 $a \rightarrow b \equiv \neg a \vee b$;
 a viene detta **premessa** e b **conseguenza**;
- **biimplicazione** (bicondizionale): \leftrightarrow , se e solo se
 $a \leftrightarrow b \equiv (a \rightarrow b) \wedge (b \rightarrow a) \equiv (a \wedge b) \vee (\neg a \wedge \neg b)$.

Proposizioni composte

Una **proposizione composta** può essere:

- sempre vera;
- sempre falsa;
- vera o falsa in funzione dei componenti.

Esempi:

- $a \vee \neg a$ *vera*
- $a \wedge \neg a$ *falsa*
- $a \wedge b$ *da valutare*

Sintassi (1)

Le proposizioni (o **formule**) sono definite induttivamente dalle regole:

- **caso base**: ogni simbolo enunciativo o costante è una formula;
- **passo**: ogni composizione di formule è una formula;
- nient'altro è una formula.

Sintassi (2)

Più formalmente, detto \mathcal{L} l'insieme dei simboli enunciativi e delle costanti, l'insieme \mathcal{P} delle proposizioni è così definito:

- $\forall a \in \mathcal{L}, (a) \in \mathcal{P}$
- $\forall p \in \mathcal{P}, \neg(p) \in \mathcal{P}$
- $\forall p, q \in \mathcal{P}, (p \vee q), (p \wedge q), (p \rightarrow q), (p \leftrightarrow q) \in \mathcal{P}$

Precedenze

Le **precedenze** permettono di ridurre il numero di parentesi necessarie per interpretare correttamente una proposizione.

\neg precede \wedge precede \vee precede \rightarrow precede \leftrightarrow

Esempi:

- $((\neg a) \vee a)$ si può scrivere $\neg a \vee a$
- $(a \vee (b \wedge c))$ si può scrivere $a \vee b \wedge c$
- $(a \wedge (b \vee c))$ si può scrivere $a \wedge (b \vee c)$

Semantica

La **semantica** è l'insieme delle regole che permettono di associare un valore di verità ad una proposizione, a partire dai valori dei simboli enunciativi che vi compaiono.

La semantica dei connettivi è illustrata dalle seguenti tabelle, dette **tabelle di verità**:

a	b	$a \vee b$	$a \wedge b$	$\neg a$	$a \rightarrow b$	$a \leftrightarrow b$
F	F	F	F	V	V	V
F	V	V	F	V	V	F
V	F	V	F	F	F	F
V	V	V	V	F	V	V

Interpretazione (1)

Diremo **interpretazione** di una proposizione una funzione che assegna uno dei due valori di verità, V o F , a ciascuna proposizione atomica componente e che quindi assegna un valore di verità alla proposizione composta sulla base delle tavole di verità.

Formalmente, quindi, una **interpretazione** è una funzione $v : \mathcal{P} \rightarrow \{F, V\}$.

L'interpretazione di una proposizione p può essere calcolata mediante la costruzione della tabella di verità di p .

Interpretazione (2)

Esempio: $\neg p \wedge (q \rightarrow p)$

p	q	$\neg p$	$q \rightarrow p$	$\neg p \wedge (q \rightarrow p)$
F	F	V	V	V
F	V	V	F	F
V	F	F	V	F
V	V	F	V	F

Ogni riga di una tabella di verità è una interpretazione.
Se una proposizione ha n componenti atomici, esistono 2^n interpretazioni per essa.

Soddisfacibilità

Se una interpretazione, $v(\cdot)$, rende una proposizione, p , vera ($v(p) = V$), si dice che v **soddisfa** p .

Una proposizione, p , si dice **soddisfacibile** se esiste almeno una interpretazione, $v(\cdot)$, che la soddisfa.

Una proposizione, p , si dice **tautologia** (o anche che è **valida**) se tutte le sue interpretazioni possibili la rendono vera: $\forall v, v(p) = V$.

Una proposizione non soddisfacibile (cioè resa falsa da tutte le interpretazioni possibili) viene detta **contraddizione**.

Relazioni tra proposizioni

Implicazione logica :

a **implica logicamente** b se e solo se $a \rightarrow b$ è una tautologia: $a \Rightarrow b$

Equivalenza logica :

a è **logicamente equivalente** a b se e solo se $a \leftrightarrow b$ è una tautologia: $a \Leftrightarrow b$

NB: $a \Rightarrow b$ e $a \Leftrightarrow b$ sono relazioni tra la proposizione a e la proposizione b .

Ad esse sono associabili rispettivamente le proposizioni $a \rightarrow b$ e $a \leftrightarrow b$.

Leggi logiche (1)

Le tautologie sono chiamate anche **leggi logiche**.

- Eliminazione di congiunzione

$$a \wedge b \Rightarrow a$$

- Introduzione di disgiunzione

$$a \Rightarrow a \vee b$$

- Negazione della biimplicazione

$$\neg(a \leftrightarrow b) \Leftrightarrow \neg a \leftrightarrow b$$

Leggi logiche (2)

- Sillogismo disgiuntivo

$$(a \vee b) \wedge \neg b \Rightarrow a$$

- *Ex falso sequitur quodlibet*

$$\neg a \Rightarrow a \rightarrow b$$

- *Verum sequitur a quodlibet*

$$a \Rightarrow b \rightarrow a$$

- Terzo escluso

$$a \vee \neg a$$

Leggi logiche (3)

- Non contraddizione

$$\neg(a \wedge \neg a)$$

- Dimostrazione per casi

$$(a \rightarrow b) \wedge (\neg a \rightarrow b) \Rightarrow b$$

- Dimostrazione per assurdo

$$(\neg b \rightarrow a \wedge \neg a) \Rightarrow b$$

- Contrapposizione

$$a \rightarrow b \Leftrightarrow \neg b \rightarrow \neg a$$

Leggi logiche (4)

- Leggi di De Morgan

$$\neg(a \wedge b) \Leftrightarrow \neg a \vee \neg b$$

$$\neg(a \vee b) \Leftrightarrow \neg a \wedge \neg b$$

- Sillogismo ipotetico

$$(a \rightarrow b) \wedge (b \rightarrow c) \Rightarrow a \rightarrow c$$

- Transitività dell'implicazione

$$a \rightarrow b \Rightarrow (b \rightarrow c) \rightarrow (a \rightarrow c)$$

Leggi logiche (5)

- Distributività delle conseguenze

$$a \rightarrow (b \wedge c) \Leftrightarrow (a \rightarrow b) \wedge (a \rightarrow c)$$

- Esportazione/importazione delle premesse

$$(a \wedge b) \rightarrow c \Leftrightarrow a \rightarrow (b \rightarrow c)$$

- Doppia negazione

$$\neg\neg a \Leftrightarrow a$$

Teoremi

Un **teorema** della logica proposizionale è composto da:

- una o più proposizioni , a_k ($1 \leq k \leq n$), dette **assunzioni** o **ipotesi**;
- da una proposizione, t , detta **tesi**.

Un teorema è esprimibile come:

$$a_1 \wedge \dots \wedge a_n \Rightarrow t$$

Regole di inferenza

Le **regole di inferenza** permettono di dedurre una proposizione valida:

- dato che p è vera e $p \Leftrightarrow q$, anche q è vera (**equivalenza logica**);
- se p è una tautologia e a è una sua proposizione componente, sostituendo a tutte le occorrenze di a in p la proposizione q , si ottiene ancora una tautologia (**sostituzione**);
- dato che sia $a \rightarrow b$ che a sono vere, si deduce che anche b è vera (**modus ponens**);
- dato che sia $a \rightarrow b$ che $\neg b$ sono vere, si deduce che anche $\neg a$ è vera (**modus tollens**).

Dimostrazione di teoremi

Una **dimostrazione** può essere formulata come una sequenza di proposizioni vere p_1, \dots, p_m , dove $p_j, 1 \leq j \leq m$:

- è un'assunzione;
- è una tautologia;
- è ottenuta per applicazione delle regole di inferenza;
- p_m è la tesi.

Esempio – teorema

Assumiamo che le seguenti proposizioni siano vere:

- se è vacanza sto a casa o vado in montagna;
- oggi sono al lavoro.

Date le precedenti assunzioni, dimostrare che:

- oggi è un giorno lavorativo.

Esempio – formalizzazione

Le proposizioni coinvolte possono essere formalizzate come segue:

- v = "oggi è vacanza"
- c = "stare a casa"
- m = "andare in montagna"

e il teorema diventa:

$$a_1: v \rightarrow (c \vee m)$$

$$a_2: \neg c \wedge \neg m$$

$$t: \neg v$$

Esempio – dimostrazione

$$p_1: v \rightarrow (c \vee m)$$

a_1

$$p_2: \neg(c \vee m) \rightarrow \neg v$$

contrapposizione di p_1

$$p_3: \neg c \wedge \neg m$$

a_2

$$p_4: \neg(c \vee m)$$

Legge di De Morgan da p_3

$$p_5: \neg v$$

modus ponens da p_2 e p_4