Metodi Matematici per l'Informatica - Dispensa 17
(a.a. 22/23, I canale)

Docente: Lorenzo Carlucci (lorenzo.carlucci@uniroma1.it)

1 Introduzione

La Logica Proposizionale si occupa di studiare le proprietà di alcuni costrutti logici utilizzati nel linguaggio naturale e nella pratica scientifica e matematica, quali il *non* (negazione), l'*oppure* (disgiunzione), l'*e* (congiunzione), il *se ... allora* (implicazione) o il *se e solo se* (equivalenza, doppia implicazione).

Esempio 1.1. Consideriamo il seguente semplice argomento aritmetico.

1. Se $a = 0$ o $b = 0$ allora $a \cdot b = 0$.
2. $a \cdot b \neq 0$.
3. $a \neq 0$ e $b \neq 0$.

Intuitivamente la terza proposizione è la conclusione di un argomento che ha come premesse le prime due. Come si formalizza? Per prima cosa si individuano quelle parti che non possono essere ulteriormente analizzate in termini di costrutti logici e che possono essere vere o false (dette parti atomiche). Nel nostro caso, queste parti atomiche sono $a = 0$, $b = 0$, e $a \cdot b = 0$.

Associamo a ciascuna di queste parti atomiche una distinta lettera: a $a = 0$ associamo A, a $b = 0$ associamo B, a $a \cdot b = 0$ associamo C. Infine sostituiamo i costrutti logici del linguaggio naturale (Se ... allora, o, e, non) con dei simboli formali, detti connettivi Booleani: $\neg$ per la negazione, $\vee$ per la disgiunzione, $\wedge$ per la congiunzione, $\rightarrow$ per l'implicazione (se... allora), e $\leftrightarrow$ per la doppia implicazione (se e solo se).

Otteniamo la seguente formalizzazione,

(i) $(A \vee B) \rightarrow C$.

(ii) $(\neg C)$.

(iii) $(\neg A \wedge \neg B)$.

dove, intuitivamente, leggiamo $A \vee B$ come "A oppure B", $\neg C$ come "non C", etc.

Consideriamo ora il seguente argomento verbale.

(a) Se il padre è alto o la madre è alta allora il figlio è alto.

(b) Il figlio è basso.

(c) Il padre è basso e la madre è bassa.

Ovviamente la prima premessa (a) è empiricamente falsa, mentre la prima premessa (1) è matematicamente vera. Ciò nonostante, riconosciamo intuitivamente che il ragionamento è valido (o corretto).

Quando diciamo che l'argomento è valido (o corretto) intendiamo dire che *se* le premesse sono vere, *allora* è vera la conclusione; non che le premesse sono vere.

Se tentiamo una formalizzazione dell'argomento ci rendiamo conto facilmente che otteniamo la stessa formalizzazione che abbiamo ottenuto per l'argomento precedente, dove scriviamo A per "il padre è alto", B per "la madre è alta" e C per "il figlio è alto". I due argomenti risultano pertanto identici. La logica formale permette di individuare la *forma logica* comune ad argomenti che trattano di oggetti e strutture diverse, come è il caso negli esempi qui sopra.

La logica si occupa della validità di ragionamenti indipendentemente dal significato delle loro componenti. In questo è parente dell'Algebra moderna.

> Quanti sono a conoscenza dello stato attuale della teoria dell'algebra simbolica sono consapevoli del fatto che la validità dei processi di analisi non dipende dall'interpretazione dei simboli impiegati, ma soltanto dalle leggi della loro combinazione. Ogni sistema di interpretazione che non intacchi la verità delle relazioni presupposte è egualmente ammissibile. (George Boole, *L'analisi matematica della logica*, 1847)

2 Linguaggio e proposizioni formali

Definizione 2.1 (Linguaggio proposizionale)**.** Un linguaggio proposizionale è un insieme $\mathcal{L}$ di simboli contenente

1. I seguenti simboli, detti connettivi logici: $\neg$, $\vee$, $\wedge$, $\rightarrow$, $\leftrightarrow$,
2. Le parentesi tonde chiuse e aperte,
3. Una quantità finita o infinita numerabile di simboli (distinti dai connettivi e dalle parentesi) detti variabili proposizionali, il cui insieme viene indicato con $\mathsf{VAR}_{\mathcal{L}}$.

Definizione 2.2 (Proposizioni)**.** Sia $\mathcal{L}$ un linguaggio proposizionale. L'insieme delle proposizioni (o formule ben formate) in $\mathcal{L}$ è il minimo insieme X di stringhe finite di simboli in $\mathcal{L}$ tale che

1. Tutte le variabili proposizionali di $\mathcal{L}$ sono in X, e
2. Se A è in X allora $(\neg A)$ è in X, e
3. Se A e B sono in X allora $(A \wedge B)$, $(A \vee B)$, $(A \rightarrow B)$ e $(A \leftrightarrow B)$ sono in X.

Denotiamo con $\mathrm{PROP}_{\mathcal{L}}$ (o $\mathsf{FML}_{\mathcal{L}}$) l'insieme delle proposizioni (o formule) nel linguaggio $\mathcal{L}$. Se $\mathcal{L}$ è chiaro dal contesto, scriviamo PROP.

Osservazione 2.3. Cosa significa nella Definizione precedente che PROP è *il minimo insieme tale che...*? Quello che si intende è che, se Y è un qualunque insieme che soddisfa (1)(2)(3), allora $\mathrm{PROP} \subseteq Y$. Come sappiamo che un tale Y esiste? Possiamo argomentare come segue.

Definizione 2.4 (Sottoformula)**.** Una proposizione B è una sottoformula di una proposizione A se è verificato uno dei seguenti casi.

1. A è identica a B.
2. A è $(\neg C)$ e B è sottoformula di C.
3. A è $(C \square D)$ e B è sottoformula di C oppure è sottoformula di D.

Se A è $(\neg C)$, C è detta sottoformula immediata di A. Se A è $(C \square D)$, C e D sono dette sottoformule immediate di A, dove usiamo il simbolo $\square$ come un segnaposto per uno dei connettivi $\{\wedge, \vee, \rightarrow, \leftrightarrow\}$.

3 Semantica della Logica Proposizionale

Definizione 3.1 (Assegnamento)**.** Un assegnamento è una funzione di tipo

$$v : \mathrm{VAR} \to \{1, 0\}.$$

I numeri $1, 0$ vengono detti *valori di verità*, e sono intuitivamente da identificarsi come *Vero* e *Falso*.

Vogliamo estendere un qualunque assegnamento $v : \mathrm{VAR} \to \{1, 0\}$ a una funzione

$$v' : \mathrm{PROP} \to \{0, 1\}.$$

Lo facciamo dando delle regole per calcolare ricorsivamente il valore di v' su una proposizione A come funzione dei valori di v' sulle sottoformule immediate di A. Per alleggerire la notazione, a rischio di ambiguità, usiamo v per indicare la funzione di tipo $\mathrm{PROP} \to \{0, 1\}$ ottenuta estendendo v secondo le regole seguenti.

$$v((\neg A)) = \begin{cases} 1 & \text{se } v(A) = 0 \\ 0 & \text{se } v(A) = 1 \end{cases}$$

$$v((A \vee B)) = \begin{cases} 0 & \text{se } v(A) = v(B) = 0 \\ 1 & \text{altrimenti.} \end{cases}$$

$$v((A \wedge B)) = \begin{cases} 1 & \text{se } v(A) = v(B) = 1 \\ 1 & \text{altrimenti.} \end{cases}$$

$$v((A \to B)) = \begin{cases} 0 & \text{se } v(A) = 1 \text{ e } v(B) = 0 \\ 1 & \text{altrimenti.} \end{cases}$$

$$v((A \leftrightarrow B)) = \begin{cases} 1 & \text{se } v(A) = v(B) \\ 0 & \text{altrimenti.} \end{cases}$$

Osserviamo che è possibile presentare i casi della definizione di v qui sopra in modo compatto usando le cosidette Tavole di verità. Per esempio, possiamo riscrivere la definizione di $v((\neg A))$ in forma tabulare come segue.

A	$\neg A$
1	0
0	1

Analogamente possiamo riscrivere la definizione di $v((A \vee B))$ in forma tabulare come segue.

A	B	$(A \vee B)$
1	1	1
1	0	1
0	1	1
0	0	0

Lo stesso possiamo fare per tutti gli altri casi.

Con la definizione data sopra di $v : \mathrm{PROP} \to \{0, 1\}$ abbiamo identificato una proposizione con una funzione booleana. Una proposizione A contenente n variabili proposizionali si può identificare con una funzione booleana di n argomenti, $A : \{0, 1\}^n \to \{0, 1\}$. Chiamiamo funzioni di questo tipo *funzioni di verità*.

Osservazione 3.2. La definizione del valore di verità di una implicazione $A \to B$ data sopra definisce la cosidetta *implicazione materiale*. Secondo questa definizione una implicazione $A \to B$ è vera nei tre casi seguenti.

1. A e B sono vere,
2. A è falsa e B è vera,
3. A è falsa e B è falsa.

La scelta della definizione di $v(A \to B)$ in funzione di $v(A)$ e $v(B)$, e in particolare i punti (2) e (3), possono giustificarsi come segue.

Nel nostro sistema vogliamo che la proposizione $(A \wedge B) \to B$ sia sempre vera, qualunque siano A e B. Vediamo come questa richiesta impone un vincolo alla definizione di $v(A \to B)$.

A	B	$A \wedge B$	$(A \wedge B) \to B$
1	1	1	1
1	0	0	1
0	1	0	1
0	0	0	1

Se vogliamo riempire la tavola di verità di $X \to Y$, siamo vincolati dalla tavola precedente alla scelta seguente, leggendo X come $(A \wedge B)$ e Y come B.

X	Y	$X \to Y$
1	1	1
1	0	0
0	1	1
0	0	1

Un'altra giustificazione (parziale) della scelta della definizione della tavola di verità di $\to$ è che vogliamo che valga l'implicazione seguente, che formalizza il ragionamento per contrapposizione:

$$(A \to B) \to (\neg B \to \neg A).$$

Se A e B sono vere la premessa è vera e il conseguente è di tipo $0 \to 0$.

4 Tavole di verità

La possibilità di organizzare in una tabella i valori di verità di una proposizione composta come funzione dei valori di verità delle sue componenti sopra accennato può essere generalizzato a proposizioni qualunque.

Data una proposizione A che contiene le variabili proposizionali $p_1, \ldots, p_n$ distinte e le sottoformule $B_1, \ldots, B_k$, possiamo organizzare la Tavola di verità di A come segue. Nelle prime n colonne scriviamo tutti i possibili valori assunti dalle variabili proposizionali $p_1, \ldots, p_n$. Nelle restanti colonne scriviamo i valori assunti dalle sottoformule di A in ordine crescente di complessità (misurata in termini di rango).

Esempio Sia $A = ((P \vee Q) \to (R \vee (R \to Q)))$.

P	Q	R	$(R \to Q)$	$(R \vee (R \to Q))$	$(P \vee Q)$	A
1	1	1	1	1	1	1
1	1	0	1	1	1	1
1	0	1	0	1	1	1
1	0	0	1	1	1	1
0	1	1	1	1	1	1
0	1	0	1	1	1	1
0	0	1	0	1	0	1
0	0	0	1	1	0	1

Esempio Sia $A = ((\neg P) \wedge Q) \rightarrow R)$.

P	Q	R	$(\neg P)$	$((\neg P) \wedge Q)$	A
1	1	1	0	0	1
1	1	0	0	0	1
1	0	1	0	0	1
1	0	0	0	0	1
0	1	1	1	1	1
0	1	0	1	1	0
0	0	1	1	0	1
0	0	0	1	0	1

Possiamo costruire (meccanicamente) la tavola di verità di una qualunque proposizione A. Se la proposizione contiene n variabili proposizionali, la sua tavola di verità ha 2^n righe. Ogni assegnamento di valori di verità alle variabili proposizionali di A corrisponde ad una riga della tavola di verità di A, e viceversa.

5 Soddisfacibilità, conseguenza logica, validità logica

Definizione 5.1 (Proposizione Soddisfacibile)**.** Un assegnamento v soddisfa una proposizione A se $v(A) = 1$. Si dice anche che v è un modello di A. A è soddisfacibile se esiste un assegnamento che la soddisfa. Altrimenti A è insoddisfacibile. Indichiamo con SAT l'insieme delle proposizioni soddisfacibili (*satisfiable*) e con UNSAT l'insieme delle proposizioni insoddisfacibili.

Definizione 5.2 (Conseguenza Logica)**.** Siano $\mathcal{F} = \{A_1, \ldots, A_n\}$ un insieme di proposizioni e sia A una proposizione. Diciamo che A è conseguenza logica di $\mathcal{F}$ se ogni assegnamento che soddisfa tutti gli elementi di $\mathcal{F}$ soddisfa anche A. Scriviamo in tal caso $A_1, \ldots, A_n \models A$ e diciamo che le premesse $A_1, \ldots, A_n$ implicano logicamente la conclusione A.

Se $\mathcal{F}$ è l'insieme vuoto scriviamo $\models A$ per $\varnothing \models A$. In questo caso la definizione, letta correttamente, dice che A è soddisfatta da tutti gli assegnamenti, i.e., che per ogni assegnamento v, $v(A) = 1$. Infatti per qualunque v è vero a vuoto che v soddisfa tutti gli elementi dell'insieme $\varnothing$.

Definizione 5.3 (Tautologia, verità Logica)**.** Una proposizione A è una verità logica se per ogni assegnamento v, $v(A) = 1$. Si dice anche che A è valida, o è una tautologia. Indichiamo con TAUT l'insieme delle tautologie.

Osservazione 5.4. Si osserva che A è una tautologia se e solo se $\models A$.

Osservazione 5.5. Si osserva che $A \in$ SAT è un concetto *esistenziale*:

$$A \in \text{SAT} \Leftrightarrow \exists v(v(A) = 1),$$

mentre $A \in$ TAUT è un concetto *universale*:

$$A \in \text{TAUT} \Leftrightarrow \forall v(v(A) = 1),$$

Esiste la seguente dualità tra TAUT e UNSAT:

$$A \in \text{TAUT} \Leftrightarrow \neg A \in \text{UNSAT}.$$

D'altra parte è ovvio che esistono proposizioni tali che sia $A \in$ SAT che $\neg A \in$ SAT.

Vale inoltre il seguente Teorema, che riduce il problema della conseguenza logica (valitdità di un argomento) a quello della verità logica e della soddisfacibilità.

Teorema 5.6. *Siano $A_1, \ldots, A_n, A$ proposizioni. Allora i seguenti punti sono equivalenti.*

1. $A_1, \ldots, A_n \models A$.
2. $((A_1 \wedge \cdots \wedge A_n) \to A) \in$ Taut.
3. $(A_1 \wedge \cdots \wedge A_n \wedge \neg A) \in$ UnSat.

Dimostrazione. Assumiamo il punto (1) e dimostriamo il (2). Supponiamo per assurdo che esista una valutazione v tale che $v((A_1 \wedge \cdots \wedge A_n) \to A) = 0$. Dunque $v(A_1 \wedge \cdots \wedge A_n)) = 1$ e $v(A) = 0$. Ma questo contraddice (1). Assumiamo il punto (2) e dimostriamo il (3). Per assurdo esista una valutazione v tale che $v(A_1 \wedge \cdots \wedge A_n \wedge \neg A) = 1$. Allora $v(A_1) = v(A_2) = \cdots = v(A_n) = v(\neg A) = 1$ e $v(A) = 0$, e dunque $v((A_1 \wedge \cdots \wedge A_n) \to A) = 0$, contro l'ipotesi che si tratti di una tautologia. Assumiamo il punto (3) e dimostriamo il punto (1). Per assurdo supponiamo che $A_1, \ldots, A_n \not\models A$. Allora esiste un assegnamento v tale che $v(A_1) = \cdots = v(A_n) = 1$ e $v(A) = 0$, e dunque $v(\neg A) = 1$ e così $v(A_1 \wedge \cdots \wedge A_n \wedge \neg A) = 1$, contro l'ipotesi. □

Osservazione 5.7. Il metodo delle tavole di verità permette di calcolare i valori di verità di una funzione arbitrariamente complessa. Data una proposizione A qualunque, possiamo rispondere algoritmicamente alla domanda: $A \in$ Taut? Basta costruire la tavola di verità di A e controllare se l'ultima colonna contiene solo il valore 1. La tavola di verità di una proposizione in cui appaiono n variabili proposizionali contiene 2^n righe. Per questo motivo il metodo delle tavole di verità è *computazionalmente inefficiente*. Lo stesso vale per la domanda: $A \in$ Sat? Anche in questo caso le tavole di verità danno una risposta, ma in modo inefficiente.

Non si conoscono però algoritmi efficienti (polinomiali) per rispondere a questa domanda. Trovare un tale algoritmo o dimostrare che un tale algoritmo non esiste equivale a risolvere il Problema del Millennio ($\mathbf{P} = \mathbf{NP}$)? (i.e., la classe dei problemi risolvibili in tempo polinomiale da un algoritmo deterministico coincide con la classe dei problemi risolvibili in tempo polinomiale da un algoritmo non-deterministico?). Per questo problema il *Clay Mathematical Institute* offre un premio di un milione di dollari.

In molti casi è possibile decidere se una certa proposizione è in Taut o no, oppure se una certa conclusione è conseguenza logica di certe altre proposizioni senza costruire la tavola di verità, ma ragionando in modo rigoroso a un più alto livello. Nel seguito vediamo alcuni risultati che permettono di manipolare proposizioni in modo algebrico, preservando la relazione di equivalenza logica.