

Logica Proposizionale - Parte 1

Corso di Logica

Pietro Galliani

Università dell'Insubria, Varese
`pietro.galliani@uninsubria.it`

(slides tratte dal corso di B. Gerla)

Logica proposizionale

La logica proposizionale si occupa di studiare il grado di verità delle *proposizioni* o *asserzioni*.

Una proposizione è una frase alla quale può essere assegnato un valore di verità , cioè della quale si può dire se è vera o falsa.

Sono esempi di asserzioni le frasi

‘questa mela è rossa’

oppure

‘il mare è giallo’

o anche frasi composte come

‘ogni numero intero o è pari o è dispari’

Esempi di frasi che non sono asserzioni sono tutte le domande, le esclamazioni (‘stai bene?’, ‘mangi quella mela?’, ‘vattene!’) e in generale le frasi per le quali non ha senso dire se sono vere o false. Questa chiaramente non è una definizione molto formale, ma può bastare per farsi un’idea del nostro contesto.

Una asserzione complessa è formata da più asserzioni semplici composte tra di loro tramite delle paroline speciali che chiameremo *connettivi*. A questo livello di studio siamo interessati solo ad alcuni connettivi, in particolare

- alla *negazione* ('non è vero che questa mela è rossa'),
- alla *coniunzione* ('questa mela è rossa e il mare è blu'),
- alla *disgiunzione* ('questa mela è rossa oppure è gialla') e
- all'*implicazione* ('se questa mela è rossa allora me la mangio').

Nella nostra formalizzazione useremo un simbolo per ogni asserzione che non è composta da altre asserzioni (cioè per ogni asserzione *atomica*), e poi utilizzeremo dei simboli per i connettivi. Le asserzioni atomiche saranno denotate con dei simboli che chiameremo *variabili proposizionali* perché il loro valore di verità potrà variare tra vero e falso.

Una proposizione può essere vera o falsa, a seconda del contesto.
Per ora ci occupiamo di logica con DUE valori di verità : VERO (o V o 1)
e FALSO (o F o 0).

Consideriamo le seguenti proposizioni:

La mela è rossa

n è un numero pari

Entrambe possono essere vere o false, la prima dipende da quale mela stiamo considerando, la seconda dipende dal valore di n .

Ma le seguenti proposizioni sono sempre vere:

Se la mela è rossa allora non è verde

n è un numero pari oppure è un numero dispari

Proposizioni di questo ultimo tipo, che sono sempre vere, si chiamano **tautologie**.

Definizione

Il linguaggio della logica proposizionale è formato dai seguenti insiemi

- *Var insieme delle variabili proposizionali: X, Y, \dots*
- *connettivi $\wedge, \vee, \rightarrow, \neg$*
- *parentesi $(,)$*

I connettivi \wedge, \vee e \rightarrow (rispettivamente chiamati congiunzione, disgiunzione e implicazione) sono connettivi *binari* che hanno cioè due argomenti. Invece la negazione \neg è un connettivo *unario*, con un solo argomento.

Definizione

L'insieme $Form$ delle formule è definito nel seguente modo:

- *Ogni variabile è una formula $Var \subseteq Form$;*
- *Se P è una formula allora $(\neg P)$ è una formula;*
- *Se P_1, P_2 sono formule allora $(P_1 \wedge P_2)$, $(P_1 \vee P_2)$, $(P_1 \rightarrow P_2)$ sono formule.*

Diremo che i connettivi \wedge , \vee , \rightarrow sono rispettivamente i connettivi *principali* delle formule $(P_1 \wedge P_2)$, $(P_1 \vee P_2)$, $(P_1 \rightarrow P_2)$ e che \neg è il connettivo principale della formula $(\neg P)$.

Gerarchia dei connettivi

Nella definizione delle formule, le parentesi sono utilizzate per evitare ambiguità .

La definizione data però ci obbliga ad usare tante parentesi: per esempio $X \wedge Y$ non è una formula perchè non ha le parentesi.

Cerchiamo quindi un compromesso tra la praticità di scrittura e la precisione sintattica.

La prima regola è quella di evitare di scrivere le parentesi che racchiudono tutta la formula. Poi diamo una gerarchia ai connettivi, in modo da risparmiare sulle parentesi.

Gerarchia dei connettivi

Stabiliamo che, in mancanza di parentesi che chiariscano la situazione, la negazione viene applicata prima degli altri connettivi: quindi per esempio la formula $\neg X \rightarrow Y$ va intesa come $(\neg X) \rightarrow Y$.

In secondo luogo stabiliamo che la congiunzione e la disgiunzione si applicano prima dell'implicazione (ma dopo la negazione): per esempio $\neg X \wedge Y \rightarrow \neg Z$ va letta come $((\neg X) \wedge Y) \rightarrow (\neg Z)$. In questo modo potremmo utilizzare una scrittura più veloce senza perdere in precisione.

Esempio

La formula

$$X \vee \neg Y \rightarrow X \wedge \neg Z$$

si legge come

$$(X \vee \neg Y) \rightarrow (X \wedge \neg Z)$$

Induzione strutturale

L'insieme delle formule è definito per induzione strutturale, cioè si parte con la definizione delle formule più piccole, quelle atomiche, e poi si dice come comporre formule più complesse. Questa definizione è molto comoda per esprimere concetti validi per tutte le formule. Di seguito ne vedremo alcuni.

Definizione

L'insieme $Sub(P)$ delle sottoformule di una formula P è definito nel seguente modo:

- *Se P è una variabile proposizionale allora $Sub(P) = \{P\}$;*
- *Se $P = P_1 \wedge P_2$, $P = P_1 \vee P_2$, o $P = P_1 \rightarrow P_2$ allora $Sub(P) = Sub(P_1) \cup Sub(P_2) \cup \{P\}$; in questo caso diremo che P_1 e P_2 sono le sottoformule principali di P .*
- *Se $P = \neg P_1$ allora $Sub(P) = Sub(P_1) \cup \{P\}$; in questo caso P_1 è la sottoformula principale di P .*

Esempio. Sia $P = (X \rightarrow Z) \wedge (Y \vee \neg X)$. Allora

$$\begin{aligned} \text{Sub}(P) &= \text{Sub}(X \rightarrow Z) \cup \text{Sub}(Y \vee \neg X) \cup \{P\} = \\ &= \text{Sub}(X) \cup \text{Sub}(Z) \cup \{X \rightarrow Z\} \cup \\ &\quad \text{Sub}(Y) \cup \text{Sub}(\neg X) \cup \{Y \vee \neg X\} \cup \{P\} = \\ &= \{X, Z, X \rightarrow Z\} \cup \{Y\} \cup \text{Sub}(X) \cup \{\neg X\} \cup \{Y \vee \neg X, P\} \\ &= \{X, Z, X \rightarrow Z, Y, \neg X, Y \vee \neg X, P\} \end{aligned}$$

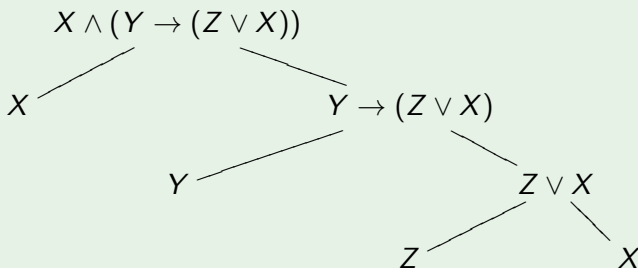
Albero di Parsing

La struttura di una formula P può essere resa esplicita disegnando il suo *albero di parsing*, che è un albero costruito nel seguente modo:

- la radice dell'albero è P .
- se in un nodo c'è una formula Q il cui connettivo principale è binario, allora questo nodo avrà due successori etichettati dalle sottoformule principali di Q .
- se in un nodo c'è una formula Q il cui connettivo principale è unario, allora questo nodo avrà un successore etichettato dalla sottoformula principale di Q .
- i nodi contenenti variabili proposizionali sono le foglie dell'albero.

Esempio

Questo è l'albero della formula $X \wedge (Y \rightarrow (Z \vee X))$:



$Sub(P)$ è l'insieme di tutti i nodi dell'albero di parsing.

Esercizio. Definire (usando l'induzione strutturale) l'altezza dell'albero di parsing di una formula P .

Una formula può quindi contenere più volte una variabile come sottoformula. Per indicare una variabile in una posizione particolare della formula, parliamo di *occorrenza* della variabile. Questo concetto può essere spiegato dalla prossima definizione.

Definizione

Il numero di occorrenze di una variabile X in una formula P è il numero $\#(X, P)$ definito nel seguente modo:

- *Se P è una variabile proposizionale allora $\#(X, P) = 1$ se $P = X$ mentre $\#(X, P) = 0$ se $X \neq P$;*
- *Se $P = P_1 \wedge P_2$, $P = P_1 \vee P_2$, o $P = P_1 \rightarrow P_2$ allora $\#(X, P) = \#(X, P_1) + \#(X, P_2)$*
- *Se $P = \neg P_1$ allora $\#(X, P) = \#(X, P_1)$.*

Definizione

La lunghezza $|P|$ di una formula P è il numero di connettivi che compaiono in P ed è definita per induzione da:

- Se P è una variabile proposizionale allora $|P| = 0$;
- Se $P = P_1 \wedge P_2$, $P = P_1 \vee P_2$, o $P = P_1 \rightarrow P_2$ allora $|P| = |P_1| + |P_2| + 1$
- Se $P = \neg P_1$ allora $|P| = |P_1| + 1$.

A volte la lunghezza di una formula è definita come il numero totale di variabili. Quale rapporto c'è tra queste due lunghezze? (Provare a definirle entrambe per induzione strutturale).

Valutazioni

Come abbiamo detto, alle variabili proposizionali possiamo assegnare sia il valore vero che il valore falso. Non è un compito della logica proposizionale stabilire quale è il valore di verità di una variabile proposizionale (cioè di una formula atomica). Compito della logica proposizionale è invece quello di stabilire il valore di una formula per ogni possibile assegnamento dei valori di verità alle formule atomiche.

Definizione (Interpretazione delle formule)

Una valutazione delle variabili è una qualsiasi funzione $v : Var \rightarrow \{0, 1\}$. Ogni valutazione v si estende ad una valutazione $v^ : Form \rightarrow \{0, 1\}$ nel seguente modo:*

- se $P \in Var$ allora $v^*(P) = v(P)$;
- se $P = \neg Q$ allora $v^*(P) = 1 - v^*(Q)$;
- se $P = Q_1 \wedge Q_2$ allora $v^*(P) = \min(v^*(Q_1), v^*(Q_2))$;
- se $P = Q_1 \vee Q_2$ allora $v^*(P) = \max(v^*(Q_1), v^*(Q_2))$;
- se $P = Q_1 \rightarrow Q_2$ allora $v^*(P) = \max(1 - v^*(Q_1), v^*(Q_2))$;

(slides tratte dal corso di B. Gerla)

Tavole di verità

Le valutazioni dei connettivi possono essere riassunte con delle tabelle nelle quali si riportano le interpretazioni delle formule al variare delle valutazioni delle variabili:

X	Y	$X \wedge Y$
0	0	0
0	1	0
1	0	0
1	1	1

X	Y	$X \vee Y$
0	0	0
0	1	1
1	0	1
1	1	1

X	Y	$X \rightarrow Y$
0	0	1
0	1	1
1	0	0
1	1	1

X	$\neg X$
0	1
1	0

Quindi una valutazione permette di associare un valore di verità ad una formula a partire dal valore di verità delle variabili proposizionali che vi compaiono.

Nel seguito utilizzeremo i simboli di connettivi anche come simboli di operazioni tra 0 e 1 o tra V e F . Quindi scriveremo $0 \wedge 1$ oppure $F \rightarrow V$, considerando che l'interpretazione di tali espressioni sia chiara dal contesto.

Esempio

Sia $P = (X \vee \neg Y) \rightarrow (Y \wedge (Y \rightarrow X))$. Consideriamo la valutazione v tale che $v(X) = 1$ e $v(Y) = 0$. Allora sarà
$$v^*(P) = (1 \vee 1) \rightarrow (0 \wedge (0 \rightarrow 1)) = 1 \rightarrow 0 = 0.$$

Useremo v al posto di v^* .

Implicazione

Concentriamoci sulla tavola di verità dell'implicazione:

X	Y	$X \rightarrow Y$
0	0	1
0	1	1
1	0	0
1	1	1

In una implicazione $X \rightarrow Y$, la formula X che è scritta a sinistra del simbolo \rightarrow è chiamata *antecedente* mentre l'altra è il *conseguente*.

Il significato dell'implicazione deve essere ben chiaro: una implicazione è falsa solo quando l'antecedente è vero e il conseguente è falso.

Consideriamo per esempio la frase *Se piove allora apro l'ombrello* che posso anche scrivere come *piove implica apro l'ombrello*. Qual è l'unico modo per accorgersi che questa implicazione è falsa? Quando piove ma io non apro l'ombrello. In tutti gli altri casi non ci sono motivi per dire che la formula è falsa. In particolare, quando non piove la formula non è falsa. Questo esempio sarà ripreso più avanti.

(slides tratte dal corso di B. Gerla)

Per rappresentare tutte le possibili valutazioni della formula P al variare delle valutazioni delle variabili X e Y possiamo utilizzare una tabella, che chiameremo *tavola di verità* della formula.

Per comodità possiamo rappresentare nella tabella non solo le variabili e la formula da studiare, ma anche tutte (o alcune) le sue sottoformule.

Scriviamo la tabella della formula dell'esempio precedente

$P = (X \vee \neg Y) \rightarrow (Y \wedge (Y \rightarrow X))$:

X	Y	$\neg Y$	$X \vee \neg Y$	$Y \rightarrow X$	$Y \wedge (Y \rightarrow X)$	P
0	0	1	1	1	0	0
0	1	0	0	0	0	1
1	0	1	1	1	0	0
1	1	0	1	1	1	1

Ogni riga della tabella corrisponde ad una valutazione delle variabili.

Quindi per una formula con n variabili si dovrà scrivere una tabella con 2^n righe.

Esercizio: Scrivere la tavola di verità di $(X \rightarrow \neg Z) \vee (Y \wedge \neg X)$.

Definizione

Una formula P è **soddisfacibile** se esiste una valutazione delle variabili v tale che $v(P) = 1$, cioè se esiste una riga della sua tavola di verità nella quale la formula ha valore 1. In questo caso si dice che la valutazione v soddisfa la formula P e si scrive anche $v \models P$.

Una formula è una **tautologia** se per ogni valutazione delle variabili v si ha $v(P) = 1$, cioè se in ogni riga della tavola di verità di P la formula ha valore 1. In questo caso si scrive anche $\models P$.

Una formula è una **contraddizione** o insoddisfacibile se per ogni valutazione delle variabili v si ha $v(P) = 0$, cioè se in ogni riga della tavola di verità di P la formula ha valore 0.

Esempio

Sono tautologie:

- Tertium non datur: $A \vee \neg A$; ($A \wedge \neg A$ è invece una contraddizione);
- Ex falso quodlibet: $(A \wedge \neg A) \rightarrow A$
- Consequentia Mirabilis: $(\neg A \rightarrow A) \rightarrow A$;
- Modus ponens: $((A \rightarrow B) \wedge A) \rightarrow B$;
- Legge di Dummett: $(A \rightarrow B) \vee (B \rightarrow A)$
- Prefisso: $A \rightarrow (B \rightarrow A)$
- Contrapposizione: $(A \rightarrow B) \rightarrow (\neg B \rightarrow \neg A)$

Proposizione

P è una tautologia se e solo se $\neg P$ è una contraddizione. Se P è una tautologia allora P è soddisfacibile.

Proposizione

Se la formula A contiene le variabili X_1, \dots, X_n e se v e v' sono due valutazioni tali che

$$v(X_i) = v'(X_i)$$

per ogni $i = 1, \dots, n$, allora si ha che $v(A) = v'(A)$. (Quindi il valore $V(A)$ è determinato unicamente dal valore delle variabili).

La dimostrazione segue facilmente per induzione strutturale.

Consideriamo per esempio la formula $(X \wedge Y) \rightarrow Z$: le valutazioni della sottoformula $X \wedge Y$ saranno indipendenti dalla valutazione di Z , quindi nella tavola di verità si ripeteranno uguali sia per $Z = 0$ che per $Z = 1$:

X	Y	Z	$X \wedge Y$	$(X \wedge Y) \rightarrow Z$
0	0	0	0	1
0	1	0	0	1
1	0	0	0	1
1	1	0	1	0
0	0	1	0	1
0	1	1	0	1
1	0	1	0	1
1	1	1	1	1

Diamo un'altra definizione per induzione strutturale:

Definizione

Siano A e B delle formule e X una variabile. Allora la formula $A[B/X]$ è definita induttivamente (su A) nel seguente modo:

- se $A = X$ allora $A[B/X] = B$;
- se $A = Y$ (con Y variabile diversa da X) allora $A[B/X] = A$;
- se $A = \neg A_1$ allora $A[B/X] = \neg(A_1[B/X])$;
- se $A = A_1 * A_2$ (con $*$ $\in \{\wedge, \vee, \rightarrow\}$) allora $A[B/X] = A_1[B/X] * A_2[B/X]$.

Questa definizione coincide con l'idea che $A[B/X]$ si ottiene scrivendo B al posto di ogni occorrenza di X nella formula A .

Per esempio, se $A = X \rightarrow (\neg X \vee (Y \wedge X))$ e $B = Z \vee \neg Y$ allora

$$A[B/X] = (Z \vee \neg Y) \rightarrow (\neg(Z \vee \neg Y) \vee (Y \wedge (Z \vee \neg Y))).$$

Proposizione

Sia A una tautologia contenente la variabile proposizionale X e sia B un'altra formula. Allora anche $A[B/X]$ è una tautologia.

Esempio

Legge di Dummett: sia $A = (X \rightarrow Y) \vee (Y \rightarrow X)$. A è una tautologia.
Allora anche $A[(X \wedge Y)/Y] =$

$$(X \rightarrow (X \wedge Y)) \vee ((X \wedge Y) \rightarrow X)$$

è una tautologia (provare).

Definizione

Un insieme di formule Δ è **soddisfacibile** se esiste una valutazione v che soddisfa tutte le formule di Δ . In questo caso si scrive $v \models \Delta$ oppure $v(\Delta) = 1$.

Esempio

Sia $\Delta = \{X \wedge Y, Y\}$. Δ è soddisfacibile?

Sì, perché esiste una valutazione v , per esempio $v(X) = 1$ e $v(Y) = 1$ che soddisfa entrambe le formule di Δ .

E l'insieme $\Delta' = \{X \wedge Y, \neg Y, \neg X\}$?

Tale insieme non è soddisfacibile perché se $v(X \wedge Y) = 1$ allora deve essere necessariamente $v(X) = 1$ e quindi $v(\neg X) = 0$, quindi non può esistere una valutazione che soddisfa tutte le formule di Δ' .

Nota che è molto diverso dire che un insieme è soddisfacibile e che tutte le sue formule sono soddisfacibili. Per esempio Δ' non è soddisfacibile ma tutte le sue formule lo sono.

Esempio

Consideriamo i seguenti fatti:

Ci sono tre amiche, Anna, Beatrice e Carla che devono decidere se uscire per andare al cinema. Se Anna esce allora anche Beatrice e Carla escono. Se Beatrice esce anche Carla esce, ma Beatrice decide di non uscire. C'è una soluzione per questa situazione?

Possiamo rappresentare con delle variabili proposizionali i seguenti fatti:

A per "Anna esce"

B per "Beatrice esce"

C per "Carla esce".

Allora la situazione totale è descritta dall'insieme di formule

$$\{A \rightarrow B \wedge C, B \rightarrow C, \neg B\}$$

che è soddisfacibile: le valutazioni $A = B = C = 0$ (cioè le tre ragazze restano a casa) e $A = B = 0, C = 1$ (cioè esce solo Carla) soddisfano entrambe le condizioni iniziali.

Definizione

Sia Δ un insieme di formula e A una formula. Allora diciamo che Δ implica logicamente A (o che A è una conseguenza logica di Δ) e si scrive $\Delta \models A$, se per ogni valutazione v tale che $v \models \Delta$, si ha $v(A) = 1$. Se $\Delta = \{P\}$ è formato solo da un elemento (cioè è un singleton) allora scriviamo $P \models A$ invece di $\{P\} \models A$.

Esempio

Sia $\Delta = \{X \rightarrow Y, X\}$. Allora $\Delta \models Y$. Infatti andando a scrivere la tavola di verità si ha:

X	Y	$X \rightarrow Y$
0	0	1
0	1	1
1	0	0
1	1	1

e l'unica valutazione che soddisfa l'insieme Δ (cioè l'ultima) soddisfa anche Y .

$$\Delta_1 = \{A \vee B, C \vee \neg A\} \models B \vee C.$$

$$\Delta_2 = \{A \vee B, B \rightarrow C\} \not\models C \text{ ma } \Delta_2 \models A \vee C.$$

(slides tratte dal corso di B. Gerla)

Esempio

Consideriamo vera la frase "Se piove apro l'ombrello". Posso dedurre che se apro l'ombrello allora sta piovendo? E che se non apro l'ombrello vuol dire che non sta piovendo?

Proviamo a formalizzare nella logica proposizionale considerando una variabile proposizionale P per dire "piove" e una variabile proposizionale " O " per dire che apro l'ombrello.

I due problemi quindi corrispondono a chiedersi se:

- (i) $P \rightarrow O \models O \rightarrow P$;
- (ii) $P \rightarrow O \models \neg O \rightarrow \neg P$.

Si verifica che (i) è falsa mentre (ii) è vera.

Teorema

$\Delta \models A$ se e solo se $\Delta \cup \{\neg A\}$ è insoddisfacibile.

Dimostrazione.

Cominciamo con l'assumere che $\Delta \models A$, vogliamo dimostrare che per ogni valutazione v c'è una formula di $\Delta \cup \{\neg A\}$ che non è soddisfatta da v . Se v è una valutazione tale che $v \not\models \Delta$ allora ci sarà una formula di Δ non soddisfatta da v e quindi v non soddisfa neanche $\Delta \cup \{\neg A\}$. Se invece $v \models \Delta$ allora dato che A è una conseguenza logica di Δ si avrà $v(A) = 1$ e quindi $v(\neg A) = 0$. Anche in questo caso allora v non soddisfa l'insieme $\Delta \cup \{\neg A\}$ che risulta quindi insoddisfacibile.

Viceversa, supponiamo che $\Delta \cup \{\neg A\}$ sia insoddisfacibile. Sia v una valutazione che soddisfa Δ . Se fosse $v(A) = 0$ allora sarebbe $v(\neg A) = 1$ e quindi v soddisferebbe l'insieme $\Delta \cup \{\neg A\}$ che abbiamo detto essere insoddisfacibile. Deve quindi necessariamente essere $v(A) = 1$ e quindi A è una conseguenza logica di Δ . □

Teorema (di Deduzione)

$A \models B$ se e solo se $\models A \rightarrow B$.

Dimostrazione.

Se $A \models B$ allora per ogni interpretazione v , se $v(A) = 1$ si ha per ipotesi che anche $v(B) = 1$ e quindi $v(A \rightarrow B) = 1$ mentre se $v(A) = 0$ allora ancora $v(A \rightarrow B) = 1$ e quindi $A \rightarrow B$ è una tautologia.

Viceversa, se per ogni valutazione v si ha che $v(A \rightarrow B) = 1$, allora se $v(A) = 1$ deve essere necessariamente (per come è definita l'implicazione) $v(B) = 1$. □

In generale, se Γ è un insieme finito di formule, si ha che

$$\Gamma \models B \text{ se e solo se } \models \bigwedge_{A \in \Gamma} A \rightarrow B$$

Equivalenza logica

Definizione

Due formule A e B sono *logicamente equivalenti* (e scriviamo $A \equiv B$) se per ogni valutazione v si ha $v(A) = v(B)$.

Due formule logicamente equivalenti hanno la stessa tavola di verità (considerando lo stesso ordine di valutazione delle variabili, cioè lo stesso ordine delle righe).

Esempio

Primi esempi di equivalenze logiche molto semplici da verificare sono la legge commutativa e associativa di \wedge e \vee :

$$\begin{array}{ll} A \wedge B \equiv B \wedge A & A \vee B \equiv B \vee A \\ A \vee (B \vee C) \equiv (A \vee B) \vee C & A \wedge (B \wedge C) \equiv (A \wedge B) \wedge C. \end{array}$$

Nota che la legge associativa ci permette di scrivere congiunzioni e disgiunzioni di più di due formule, senza usare le parentesi (si scriverà quindi $A \vee B \vee C$ per indicare $(A \vee B) \vee C$ o equivalentemente $A \vee (B \vee C)$).

(slides tratte dal corso di B. Gerla)

Esempio

L'implicazione invece non è commutativa $A \rightarrow B \not\equiv B \rightarrow A$ e neanche associativa $A \rightarrow (B \rightarrow C) \not\equiv (A \rightarrow B) \rightarrow C$.

Contronominale: $A \rightarrow B \equiv \neg B \rightarrow \neg A$. Questa equivalenza si usa spesso nelle dimostrazioni: se voglio dimostrare che da A segue B posso provare a ipotizzare la negazione di B e concludere che da tale ipotesi segue la negazione di A . Se poi aggiungo che $A \wedge \neg A \equiv \perp$ ottengo le dimostrazioni per assurdo.

Implicazione materiale: le formule $A \rightarrow B$ e $\neg A \vee B$ sono logicamente equivalenti:

A	B	$A \rightarrow B$	$\neg A \vee B$
0	0	1	1
0	1	1	1
1	0	0	0
1	1	1	1

Esempio

Doppia negazione: $\neg\neg A \equiv A$.

Leggi di De Morgan: Le formule $\neg(A \vee B)$ e $\neg A \wedge \neg B$ sono logicamente equivalenti.

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

Analogamente si ha che $\neg(A \wedge B) \equiv \neg A \vee \neg B$. Inoltre vale

$$A \wedge B \equiv \neg(\neg A \vee \neg B)$$

$$A \vee B \equiv \neg(\neg A \wedge \neg B).$$

Esempio

Assorbimento:

$$X \vee (X \wedge Y) \equiv X$$

$$X \wedge (X \vee Y) \equiv X$$

Legge distributiva: Vale la distributività di \wedge rispetto a \vee e anche il viceversa.

$$X \vee (Y \wedge Z) \equiv (X \vee Y) \wedge (X \vee Z)$$

$$X \wedge (Y \vee Z) \equiv (X \wedge Y) \vee (X \wedge Z)$$

Generalizzando si ha che vale:

$$(X_1 \vee X_2) \wedge (Y_1 \vee Y_2) \equiv (X_1 \wedge Y_1) \vee (X_1 \wedge Y_2) \vee (X_2 \wedge Y_1) \vee (X_2 \wedge Y_2)$$

$$(X_1 \wedge X_2) \vee (Y_1 \wedge Y_2) \equiv (X_1 \vee Y_1) \wedge (X_1 \vee Y_2) \wedge (X_2 \vee Y_1) \wedge (X_2 \vee Y_2)$$

Posso usare l'equivalenza logica anche per definire nuovi connettivi:
Per esempio

$$\perp \equiv \neg X \wedge X$$

$$\top \equiv X \vee \neg X$$

denotano rispettivamente la formula sempre falsa e la formula vera.

Proposizione

Se P è una tautologia allora $P \equiv \top$.

Se P è una contraddizione allora $P \equiv \perp$.

Teorema (di sostituzione)

Sia v una valutazione tale che $v(P) = v(Q)$: allora per ogni formula R e variabile proposizionale X si ha

$$v(R[P/X]) = v(R[Q/X]).$$

In particolare, se $P \equiv Q$ allora $R[P/X] \equiv R[Q/X]$.

Dimostrazione.

Procediamo per induzione strutturale su R .

- Se $R = X$ variabile proposizionale, allora $R[P/X] = P$ e $R[Q/X] = Q$, quindi banalmente $v(R[P/X]) = v(P) = v(Q) = v(R[Q/X])$;
- se $R = Y$ variabile proposizionale diversa da X , allora $R[P/X] = R$ e $R[Q/X] = R$, quindi banalmente $v(R[P/X]) = v(R) = v(R[Q/X])$;
- se $R = R_1 * R_2$ con $*$ $\in \{\wedge, \vee, \rightarrow\}$ allora $R[P/X] = R_1[P/X] * R_2[P/X]$ e $R[Q/X] = R_1[Q/X] * R_2[Q/X]$, quindi, per ipotesi di induzione, $v(R_1[P/X]) = v(R_1[Q/X])$ e $v(R_2[P/X]) = v(R_2[Q/X])$ e quindi $v(R[P/X]) = v(R[Q/X])$;
- se $R = \neg R_1$ è analogo.

Esempio

Sia $P = X \rightarrow Y$ e $Q = X \vee Y$. Se $v(X) = 0$ e $v(Y) = 1$ allora $v(X \rightarrow Y) = 1$ e $v(X \vee Y) = 1$. Sia $R = \neg(X \rightarrow Y)$. Allora

$$R[P/Y] = \neg(X \rightarrow (X \rightarrow Y))$$

$$R[Q/Y] = \neg(X \rightarrow (X \vee Y))$$

e $v(R[P/Y]) = 0$ e $v(R[Q/Y]) = 0$. Nota che per una valutazione v' tale che $v'(X) = 1$ e $v'(Y) = 0$ si ha $v(R[P/Y]) = 1$ e $v(R[Q/Y]) = 0$, e infatti $v'(X \rightarrow Y) = 0$ e $v'(X \vee Y) = 1$.

Il teorema di sostituzione ci permette di sostituire una parte di una formula con una ad essa equivalente, e ottenere una formula equivalente a quella di partenza.

Consideriamo un nuovo connettivo \leftrightarrow definito da

$$A \leftrightarrow B \equiv (A \rightarrow B) \wedge (B \rightarrow A).$$

La tavola di verità di questo connettivo sarà :

A	B	$A \leftrightarrow B$
0	0	1
0	1	0
1	0	0
1	1	1

Nota che $\models A \leftrightarrow B$ se e solo se $A \equiv B$. Che differenza c'è tra \leftrightarrow e \equiv ?

\leftrightarrow è un connettivo, cioè un simbolo del linguaggio. Invece \equiv è un simbolo che usiamo per parlare delle formule, è quindi un simbolo del *metalinguaggio*.

Forma normale disgiuntiva

Definizione

Un **letterale** è una variabile o la negazione di una variabile. Lo indicheremo in generale con ℓ .

Una formula è in **forma normale disgiuntiva (DNF)** se è della forma

$$\bigvee_{i=1}^n \left(\bigwedge_{j=1}^{m_i} \ell_{ij} \right)$$

dove per ogni $i = 1, \dots, n$ e $j = 1, \dots, m_i$ (con $n \geq 1$ e $m_i \geq 1$) gli ℓ_{ij} sono letterali.

Esempio

$(X \wedge \neg Y) \vee (\neg Z \wedge X \wedge Y)$ è una formula in DNF (dove $n = 2$, $m_1 = 2$ e $m_2 = 3$).

DNF

Se $n = 1$ allora la disgiunzione ha un solo disgiunto che deve essere una congiunzione di letterali. Quindi per esempio la formula $\neg Z \wedge X \wedge Y$ è un caso particolare di DNF.

Analogamente, se $m_i = 1$ allora l' i -esimo disgiunto è costituito solo da un congiunto. Quindi per esempio la formula $X \vee (Y \wedge \neg X) \vee (\neg Y \wedge X \wedge Z)$ è in DNF ($m_1 = 1$).

Se $m_i = 1$ per ogni i , allora si hanno formule che sono disgiunzioni di letterali, che sono quindi ancora in DNF (per esempio $\neg X \vee Y \vee \neg X$).

Se $n = 1$ e $m_1 = 1$ allora si ha un solo letterale, che è un caso speciale di DNF.

Definizione

Analogamente diciamo che una formula è in **forma normale congiuntiva** se è una congiunzione di disgiunzioni di letterali.

Esempio

La formula $(X \vee \neg Y) \wedge (\neg Y \vee Z)$ è in CNF.

La formula $\neg Y \wedge (X \vee Z)$ è in CNF.

Le formule $\neg Y \wedge X \wedge Z$ e $\neg Y \vee Z \vee \neg Z$ sono in CNF (e anche in DNF).

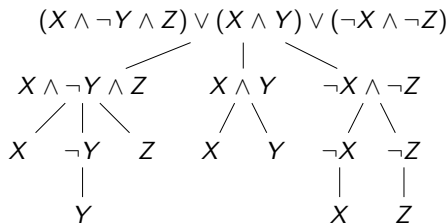
Albero di parsing di una DNF

Che forma ha l'albero di parsing di una DNF?

Abbiamo detto che per la proprietà associativa i connettivi \wedge and \vee possono essere considerati di arità variabile, quindi modifichiamo anche la definizione di albero di parsing per permettere ad un nodo di avere più di due successori. Procediamo con un esempio: la formula in DNF

$$(X \wedge \neg Y \wedge Z) \vee (X \wedge Y) \vee (\neg X \wedge \neg Z)$$

ha il seguente albero di parsing:



Trasformazione tramite equivalenze logiche

C'è un metodo algebrico per trasformare una formula in forma normale congiuntiva o disgiuntiva:

Trasformiamo una formula P in formule ad essa equivalenti nel seguente modo (le leggi commutative e associative e della doppia negazione sono applicate quando necessario):

- Togliere tutte le occorrenze di \rightarrow usando l'equivalenza logica $X \rightarrow Y \equiv \neg X \vee Y$;
- Usando le leggi di De Morgan, portare la negazione vicino alle variabili;
- usando la distributività, trasformare in CNF o DNF.

Esempio

- Sia

$$P = \neg Y \wedge (Z \rightarrow \neg X)$$

Allora $P \equiv \neg Y \wedge (\neg Z \vee \neg X) \equiv (\neg Y \wedge \neg Z) \vee (\neg Y \wedge \neg X)$ che è in DNF.

- Sia

$$\begin{aligned} P &= (\neg Y \wedge (Z \rightarrow \neg X)) \rightarrow (X \vee (Z \rightarrow Y)) \equiv \\ &(\neg Y \wedge (\neg Z \vee \neg X)) \rightarrow (X \vee (\neg Z \vee Y)) \equiv \\ &\neg(\neg Y \wedge (\neg Z \vee \neg X)) \vee (X \vee (\neg Z \vee Y)) \equiv \\ &(Y \vee \neg(\neg Z \vee \neg X)) \vee (X \vee \neg Z \vee Y) \equiv \\ &Y \vee (Z \wedge X) \vee X \vee \neg Z \vee Y \end{aligned}$$

$Form/ \equiv$

La relazione \equiv è una relazione d'equivalenza sull'insieme $Form$ di tutte le formule proposizionali. Infatti:

- è riflessiva, ogni formula è equivalente a se stessa;
- è simmetrica, se P è equivalente a Q allora Q è equivalente a P ;
- è transitiva, se P è equivalente a Q e Q è equivalente a R allora P è equivalente a R .

La classe d'equivalenza $[P]$ di una formula P è l'insieme di tutte le formule che hanno la stessa tavola di verità di P . Quanti elementi avrà allora l'insieme quoziente $Form/ \equiv$, cioè l'insieme di tutte le classi d'equivalenza?

Questo equivale a contare quante diverse tavole di verità ci sono.

Consideriamo le tavole di verità delle formule che si possono scrivere con una sola variabile X . Tali tavole di verità avranno due righe, quindi le possibili tavole di verità diverse tra di loro sono 4:

X			
0	1	0	1
1	0	0	1

che sono le tavole di verità delle formule X , $\neg X$, $X \wedge \neg X$, $X \vee \neg X$ (ma anche di altre). Non si possono scrivere altre tavole di verità .

Una tavola di verità si può considerare come una funzione

$$f : \{0, 1\}^n \rightarrow \{0, 1\};$$

le n -uple $(x_1, \dots, x_n) \in \{0, 1\}^n$ sono le valutazioni delle variabili proposizionali X_1, \dots, X_n e $f(x_1, \dots, x_n)$ è il valore assegnato alla formula. Tutte le formule di una classe d'equivalenza hanno la stessa tavola di verità . Ci chiediamo adesso se per ogni funzione $f : \{0, 1\}^n \rightarrow \{0, 1\}$ c'è una formula che ha f come tavola di verità .

Teorema (Completezza funzionale)

Per ogni funzione $f : \{0, 1\}^n \rightarrow \{0, 1\}$ esiste una formula A con n variabili tale che f è la tavola di verità di A .

Teorema (Completezza funzionale)

Per ogni funzione $f : \{0, 1\}^n \rightarrow \{0, 1\}$ esiste una formula A con n variabili in forma normale disgiuntiva tale che f è la tavola di verità di A .

Dimostrazione.

Sia $f : \{0, 1\}^n \rightarrow \{0, 1\}$. Consideriamo la formula

$$A_f = \bigvee_{(x_1, \dots, x_n) \in f^{-1}(1)} \left(\bigwedge_{i=1}^n X_i^* \right)$$

dove

$$X_i^* = \begin{cases} X_i & \text{se } x_i = 1 \\ \neg X_i & \text{se } x_i = 0 \end{cases}.$$

In altre parole, consideriamo tutte le n -uple (x_1, \dots, x_n) di elementi di $\{0, 1\}$ tali che $f(x_1, \dots, x_n) = 1$ e in corrispondenza di ogni x_i prendiamo una variabile con lo stesso indice che è negata oppure no a seconda se $x_i = 0$ oppure $x_i = 1$. Facciamo quindi la congiunzione di queste variabili e poi la disgiunzione per tutte le n -uple.

(slides tratte dal corso di B. Gerla)

Dimostrazione.

[Continua]

$$A_f = \bigvee_{(x_1, \dots, x_n) \in f^{-1}(1)} \left(\bigwedge_{i=1}^n x_i^* \right)$$

Perché questa è la formula che cerchiamo?

Perché essendo una disgiunzione, questa formula sarà vera quando almeno uno dei disgiunti è vero, cioè per quelle valutazioni v tali che per un $(x_1, \dots, x_n) \in f^{-1}(1)$ si ha che $v(\bigwedge X_i^*) = 1$.

Ma questa cosa vale quando tutti i congiunti sono veri, cioè quando $v(X_i^*) = 1$ per ogni i_1, \dots, n , che è equivalente a dire che $v(X_i) = x_i$.

Ricapitolando, la formula A è vera per quelle valutazioni

$(x_1, \dots, x_n) \in \{0, 1\}^n$ delle variabili tali che $v(X_i) = x_i$, che è proprio la definizione di tavola di verità .

Esempio

Consideriamo la seguente funzione, rappresentata in forma di tabella:

x_1	x_2	f	
0	0	1	\leftarrow
0	1	0	
1	0	1	\leftarrow
1	1	0	

Consideriamo la prima e la terza riga che corrispondono ad un valore 1 della funzione: in corrispondenza della prima riga consideriamo i letterali $\neg X_1$ e $\neg X_2$, mentre in corrispondenza della terza consideriamo X_1 e $\neg X_2$. La formula finale è quindi:

$$A_f = (\neg X_1 \wedge \neg X_2) \vee (X_1 \wedge \neg X_2)$$

A partire da una funzione $f : \{0, 1\}^n \rightarrow \{0, 1\}$ posso anche scrivere una formula in CNF:

$$\bigwedge_{(x_1, \dots, x_n) \in f^{-1}(0)} \left(\bigvee_{i=1}^n X_i^{**} \right)$$

dove

$$X_i^{**} = \begin{cases} \neg X_i & \text{se } x_i = 1 \\ X_i & \text{se } x_i = 0 \end{cases}.$$

Esempio

x_1	x_2	f	
0	0	1	
0	1	0	\leftarrow
1	0	1	
1	1	0	\leftarrow

La formula che si ottiene è

$$(X_1 \vee \neg X_2) \wedge (\neg X_1 \vee \neg X_2)$$

(slides tratte dal corso di B. Gerla)

Teorema

Ogni formula è equivalente ad una formula in DNF e ad una formula in CNF.

Dimostrazione.

Data una formula P , si può scrivere la sua tavola di verità che sarà una funzione $f : \{0, 1\}^n \rightarrow \{0, 1\}$ e quindi ricavare la CNF e la DNF come spiegato in precedenza.

Esempio

Trasformare la formula

$$P = X \rightarrow (Y \wedge \neg X)$$

in forma normale congiuntiva.

Bisogna scrivere prima la tavola di verità di P :

X	Y	$(Y \wedge \neg X)$	$X \rightarrow (Y \wedge \neg X)$
0	0	0	1
0	1	1	1
1	0	0	0
1	1	0	0

Quindi calcolare la DNF:

$$(\neg X \wedge \neg Y) \vee (\neg X \wedge Y)$$

e la CNF:

$$(\neg X \vee Y) \wedge (\neg X \vee \neg Y).$$

Definizione

Un insieme di connettivi C è **funzionalmente completo** se ogni formula è equivalente ad una formula scritta utilizzando unicamente i connettivi di C .

Per i teoremi precedenti, possiamo dire che l'insieme dei connettivi $\{\vee, \wedge, \neg\}$ è funzionalmente completo.

(Abbiamo anche visto che le formule $A \rightarrow B$ e $\neg A \vee B$ sono logicamente equivalenti: questo ci permette di dire che il connettivo di implicazione può essere definito a partire dalla negazione e dalla disgiunzione.)

Ci sono insiemi funzionalmente completi più piccoli?

Considerando che

$$\begin{aligned} X \wedge Y &\equiv \neg(\neg X \vee \neg Y) \\ X \rightarrow Y &\equiv \neg X \vee Y, \end{aligned}$$

abbiamo che $\{\neg, \vee\}$ è **funzionalmente completo**, così come $\{\neg, \wedge\}$.

E' possibile trovare un insieme di connettivi funzionalmente completo che consiste di un solo connettivo?

NOR

Consideriamo il connettivo NOR avente la seguente tavola di verità:

X	Y	$X \text{ NOR } Y$
0	0	1
0	1	0
1	0	0
1	1	0

(è cioè la negazione dell'OR). Questo connettivo può essere utilizzato per definire tutti gli altri. Infatti (provare scrivendo le tavole di verità):

$$\neg X \equiv X \text{ NOR } X$$

$$X \vee Y \equiv (X \text{ NOR } Y) \text{ NOR } (X \text{ NOR } Y) \equiv \neg(X \text{ NOR } Y)$$

$$X \wedge Y \equiv (X \text{ NOR } X) \text{ NOR } (Y \text{ NOR } Y)$$

In maniera analoga anche il NAND è funzionalmente completo.

Contare le tavole di verità

Ci eravamo posti il problema di contare gli elementi di $Form/ \equiv$.

Consideriamo l'insieme $Form_n$ delle formule che contengono n variabili X_1, \dots, X_n . Ricordiamo che data una funzione $f : \{0, 1\}^n \rightarrow \{0, 1\}$ denotiamo con A_f la formula in DNF che ha f come tavola di verità. L'insieme di tutte le funzioni da $\{0, 1\}^n$ in $\{0, 1\}$ si denota con $\{0, 1\}^{\{0, 1\}^n}$. Notiamo che la funzione

$$F : f \in \{0, 1\}^{\{0, 1\}^n} \mapsto A_f \in Form_n$$

è una funzione iniettiva perchè a tavole di verità diverse corrispondono formule diverse, ma non è suriettiva perchè non tutte le formule sono in DNF. Possiamo considerare allora la funzione

$$F : f \in \{0, 1\}^{\{0, 1\}^n} \mapsto [A_f] \in Form_n/ \equiv$$

che invece è sia iniettiva che suriettiva.

Contare le tavole di verità

Quindi gli elementi di $Form_n/ \equiv$ sono in corrispondenza biunivoca con le tavole di verità delle formule con n variabili $f : \{0, 1\}^n \rightarrow \{0, 1\}$ e quindi

$$|Form_n/ \equiv| = |\{0, 1\}^{|\{0, 1\}^n|}| = 2^{2^n}.$$

Ci sono quindi 2^{2^n} tavole di verità con n variabili e quindi questo è anche il numero di elementi di $Form_n/ \equiv$.

L'insieme $Form/ \equiv$ (dove non mettiamo un limite al numero di variabili) è invece ancora infinito (numerabile).

Algebra di Boole

Un'algebra di Boole è una struttura $(B, \wedge, \vee, ', 0, 1)$ dove:

- \wedge e \vee sono operazioni binarie associative e commutative e $'$ è un'operazione unaria;
- per ogni $x \in B$, si ha $x \wedge x = x$ e $x \vee x = x$;
- per ogni $x \in B$ si ha $x \vee 1 = 1$, $x \wedge 0 = 0$, $x \vee 0 = x$ e $x \wedge 1 = x$;
- valgono le proprietà distributive di \wedge rispetto a \vee e di \vee rispetto a \wedge ;
- per ogni $x, y \in B$ si ha $x \wedge (x \vee y) = x$ e $x \vee (x \wedge y) = x$;
- per ogni $x \in B$, $(x')' = x$;
- valgono le leggi di De Morgan: $(x' \wedge y') = (x \vee y)'$ e $(x' \vee y') = (x \wedge y)'$;
- $x \wedge x' = 0$ e $x \vee x' = 1$.

Esempio

Un esempio tipico di algebra di Boole è l'algebra formata dall'insieme delle parti $\mathcal{P}(A)$ di un insieme A con le operazioni di unione e intersezione, e dove il complemento è da intendersi come complemento rispetto all'insieme A . In questo caso $0 = \emptyset$ e $1 = A$.

Un altro esempio fondamentale è l'insieme $\{0, 1\}$ con le operazioni determinate dai connettivi.

Anche il prodotto cartesiano $\{0, 1\}^n = \{0, 1\} \times \dots \times \{0, 1\}$ n -volte è un'algebra di Boole, dove le operazioni sono definite componente per componente, cioè per esempio

$$(x_1, \dots, x_n) \vee (y_1, \dots, y_n) = (x_1 \vee y_1, \dots, x_n \vee y_n).$$

In ogni algebra di Boole è possibile definire una relazione d'ordine ponendo

$$x \leq y \quad \text{se e solo se} \quad x \wedge y = x.$$

Con questa relazione d'ordine, l'elemento 0 viene ad essere il minimo dell'algebra, mentre 1 è il massimo.

Dati $x, y \in B$ si ha che $x \wedge y$ è l'estremo inferiore di $\{x, y\}$ rispetto alla relazione d'ordine, mentre $x \vee y$ è l'estremo superiore.

Nell'algebra $\mathcal{P}(A)$ l'ordine coincide con l'inclusione tra insiemi.

Nell'algebra $\{0, 1\}$ l'ordine è quello che si può immaginare: $0 \leq 1$.

Sia $Form_n$ l'insieme delle formule che contengono solo le variabili X_1, \dots, X_n .

Per il teorema di completezza funzionale abbiamo che l'insieme $Form_n / \equiv$ delle classi d'equivalenza delle formule che usano n variabili coincide con l'insieme di tutte le funzioni $\{0, 1\}^n \rightarrow \{0, 1\}$ quindi ha 2^{2^n} elementi.

Elenchiamo per $n = 2$ tutti gli elementi di $Form_2 / \equiv$ (ne sono $2^{2^2} = 16$).

Per poterli rappresentare, possiamo considerare le tavole di verità $\{0, 1\}^2 \rightarrow \{0, 1\}$ considerando solo i quattro valori

$$(f(0, 0), f(0, 1), f(1, 0), f(1, 1)).$$

Quindi per esempio la classe della formula \perp , quando considerata come tavola di verità con quattro righe, sarà rappresentata con $(0, 0, 0, 0)$.

\perp	$(0, 0, 0, 0)$	\top	$(1, 1, 1, 1)$
$X \wedge Y$	$(0, 0, 0, 1)$	$\neg X \wedge \neg Y$	$(1, 0, 0, 0)$
$\neg X \wedge Y$	$(0, 1, 0, 0)$	$X \wedge \neg Y$	$(0, 0, 1, 0)$
X	$(0, 0, 1, 1)$	Y	$(0, 1, 0, 1)$
$\neg X$	$(1, 1, 0, 0)$	$\neg Y$	$(1, 0, 1, 0)$
$X \leftrightarrow Y$	$(1, 0, 0, 1)$	$X \leftrightarrow \neg Y$	$(0, 1, 1, 0)$
$X \vee Y$	$(0, 1, 1, 1)$	$\neg X \vee \neg Y$	$(1, 1, 1, 0)$
$Y \rightarrow X$	$(1, 0, 1, 1)$	$X \rightarrow Y$	$(1, 1, 0, 1)$

La relazione \equiv non solo è una relazione d'equivalenza, ma è anche una **congruenza** rispetto alle operazioni determinate dai connettivi, nel seguente senso:

Se $P \equiv R$ e $Q \equiv S$ allora $P \wedge Q \equiv R \wedge S$.

Possiamo quindi definire l'operazione \wedge in $Form/\equiv$ come

$$[P] \wedge [Q] = [P \wedge Q].$$

Analogamente per gli altri connettivi.

La struttura $(Form/\equiv, \wedge, \vee, \neg, [\perp], [\top])$ è un'algebra di Boole. Questo vuol dire che questa algebra verifica molte delle proprietà soddisfatte per esempio da $\mathcal{P}(A)$ e da $\{0, 1\}$.

Consideriamo per esempio la relazione definita in precedenza in ogni algebra di Boole:

$$x \leq y \text{ se e solo se } x \wedge y = x.$$

Nell'algebra $Form/\equiv$ si ha che

$$[P] \leq [Q] \text{ se e solo se } [P \wedge Q] = [P],$$

cioè se $P \wedge Q \equiv P$. Vediamo la tavola di verità :

P	Q	$P \wedge Q$	$P \rightarrow Q$
0	0	0	1
0	1	0	1
1	0	0	0
1	1	1	1

Quindi $[P] \leq [Q]$ se e solo se $P \rightarrow Q$ è una tautologia se e solo se $P \models Q$ se e solo se per ogni valutazione v si ha che $v(P) \leq v(Q)$.

Questa relazione d'ordine non è totale, cioè ci sono coppie di formule che non sono confrontabili.

Per esempio se X e Y sono variabili proposizionali non vale né $X \models Y$ né $Y \models X$.

Consideriamo l'algebra $Form_2 / \equiv$, che abbiamo visto si può rappresentare come le quadruple di elementi di $\{0, 1\}$.

La relazione d'ordine che abbiamo definito nelle algebre di Boole funziona in questo modo:

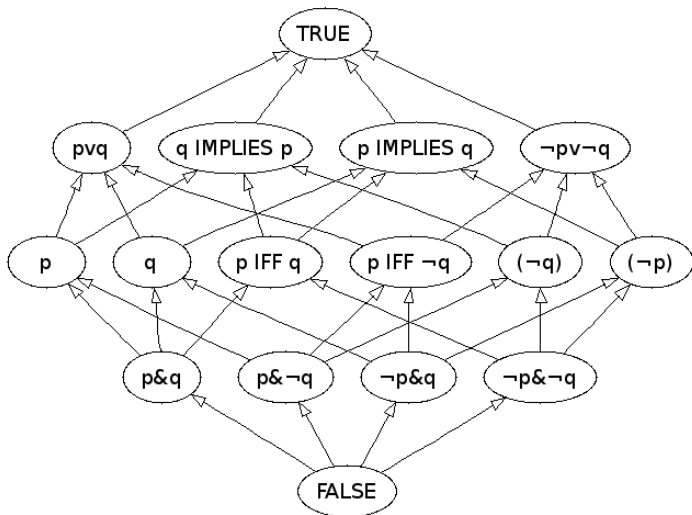
$$\perp < X \wedge Y < X < X \vee Y < \top$$

ma anche

$$\perp < X \wedge Y < Y < X \vee Y < \top.$$

Invece X e Y non sono confrontabili, così come non lo sono $\neg X \vee \neg Y$ e $X \vee Y$.

Se vogliamo rappresentare tutte le relazioni possiamo considerare questo diagramma di Hasse (nota che coincide con il diagramma dell'insieme delle parti di 4 elementi, ordinato con la relazione di inclusione).



(slides tratte dal corso di B. Gerla)

Un **isomorfismo** tra strutture algebriche è un omomorfismo biiettivo.

Se $(A, \wedge_A, \vee_A, \neg_A, 0_A, 1_A)$ e $(B, \wedge_B, \vee_B, \neg_B, 0_B, 1_B)$ sono due algebre di Boole, un isomorfismo tra A e B è una funzione biettiva $f : A \rightarrow B$ tale che per ogni $a_1, a_2 \in A$ si ha:

- $f(a_1 \vee_A a_2) = f(a_1) \vee_B f(a_2)$
- $f(a_1 \wedge_A a_2) = f(a_1) \wedge_B f(a_2)$
- $f(\neg_A a_1) = \neg_B f(a_1)$.
- $f(0_A) = 0_B$
- $f(1_A) = 1_B$.

Se esiste un isomorfismo tra due algebre di Boole A e B si dice che le algebre sono **isomorfe**.

Per fare un primo esempio di isomorfismo di algebre di Boole consideriamo $n = 2$ e le algebre $Form_2 / \equiv$ e $\{0, 1\}^4$. Iniziamo a notare che entrambe hanno 16 elementi.

Per ogni $[A] \in Form_2 / \equiv$ consideriamo la sua tavola di verità $f_A : \{0, 1\}^2 \rightarrow \{0, 1\}$ e consideriamo la funzione

$$G : [A] \in Form_2 / \equiv \rightarrow (f_A(0, 0), f_A(0, 1), f_A(1, 0), f_A(1, 1)) \in \{0, 1\}^4.$$

In altre parole stiamo associando ad ogni classe d'equivalenza di una formula, la quadrupla di valori della sua tavola di verità.

La funzione G è biettiva, per mostrare che è un isomorfismo dobbiamo verificare che conservi le operazioni. Ma questo è ovvio per come sono definite le tavole di verità. Infatti se considero due formule A e B , la quadrupla corrispondente a $[A \wedge B]$ si ottiene andando a considerare per ogni valutazione delle variabili l'operazione \wedge tra il valore di A e il valore di B . Questo vale per tutte le operazioni.

Esempio

Sia $A = X \vee Y$ e $B = X \rightarrow Y$. Allora $G([A]) = (0, 1, 1, 1)$ mentre $G([B]) = (1, 1, 0, 1)$ e

$$G([A \wedge B]) = G([(X \vee Y) \wedge (X \rightarrow Y)]) = (0, 1, 0, 1) = (0, 1, 1, 1) \wedge (1, 1, 0, 1).$$

Consideriamo ora l'insieme $\mathcal{P}(\{a, b, c, d\})$ dei sottoinsiemi di un insieme di 4 elementi.

Si ha:

$$\begin{aligned}\mathcal{P}(\{a, b, c, d\}) = & \{\emptyset, \{a\}, \{b\}, \{c\}, \{d\}, \\ & \{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}, \\ & \{a, b, c\}, \{a, b, d\}, \{a, c, d\}, \{b, c, d\}, \{a, b, c, d\}\}\end{aligned}$$

Chiaramente si ha che $S \subseteq T$ se e solo se $S \cap T = S$.

$(\mathcal{P}(\{a, b, c, d\}), \cup, \cap, ', \emptyset, \{a, b, c, d\})$ è un'algebra di Boole.

Teorema

Le algebre di Boole $\mathcal{P}(\{a, b, c, d\})$ e Form_2/\equiv sono isomorfe.

Per dimostrare il teorema precedente, dobbiamo rappresentare gli elementi di $\mathcal{P}(\{a, b, c, d\})$ con le funzioni caratteristiche:
per ogni insieme $S \in \mathcal{P}(\{a, b, c, d\})$ poniamo

$$\chi_S : x \in \{a, b, c, d\} \rightarrow \begin{cases} 1 & \text{se } x \in S \\ 0 & \text{se } x \notin S \end{cases}$$

Ogni funzione caratteristica si può vedere come una quadrupla di valori:

$$\chi_S = (\chi_S(a), \chi_S(b), \chi_S(c), \chi_S(d)).$$

Per esempio se $S = \{a, c\}$ allora $\chi_S = (1, 0, 1, 0)$.

Ma ricordiamo che una quadrupla di valori può essere anche considerata come la tavola di verità di una formula...

La funzione

$$F : S \in \mathcal{P}(\{a, b, c, d\}) \rightarrow [\phi_S] \in \text{Form}_2 / \equiv$$

dove ϕ_S è una delle formule che ha $(\chi_S(a), \chi_S(b), \chi_S(c), \chi_S(d))$ come tavola di verità, è un **isomorfismo** tra algebre di Boole.

Per esempio se $S = \{a, c\}$ e $T = \{c, d\}$, allora $\chi_S = (1, 0, 1, 0)$, $\chi_T = (0, 0, 1, 1)$ e quindi $\phi_S = \neg Y$ e $\phi_T = X$. La funzione F è un isomorfismo, infatti per esempio

$$S \cup T = \{a, c, d\} \text{ con } \chi_{S \cup T} = (1, 0, 1, 1)$$

$$\phi_{S \cup T} = Y \rightarrow X \equiv \neg Y \vee X = \phi_S \vee \phi_T$$

In genere, per ogni n si ha un isomorfismo tra Form_n / \equiv e $\{0, 1\}^{2^n}$ e tra $\{0, 1\}^{2^n}$ e $P(X)$ dove X è un qualsiasi insieme con 2^n elementi.

Teorema di compattezza

Teorema

Un insieme è soddisfacibile se e solo se ogni suo sottoinsieme finito è soddisfacibile.

Chiaramente l'importanza del teorema si evidenzia quando l'insieme di partenza è infinito, altrimenti l'asserto è banale.

Dal teorema di compattezza possiamo anche dedurre che

Teorema

Un insieme non è soddisfacibile se e solo se esiste un suo sottoinsieme finito che non è soddisfacibile.

Per dimostrare il teorema di compattezza utilizziamo una definizione e due lemmi preparatori.

Definizione

Un albero ha rami di lunghezza arbitraria (cioè *qualsiasi*) se per ogni $n \in \mathbb{N}$ esiste un ramo di lunghezza n .

Nota che dire che un albero non ha rami di lunghezza arbitraria significa che esiste un numero n tale che l'albero non ha rami più lunghi di n , cioè n è la lunghezza massima dei rami dell'albero.

Lemma di König

Lemma

Un albero binario con rami di lunghezza arbitraria ha almeno un ramo di lunghezza infinita.

Dimostrazione del Lemma di König

Sia a la radice dell'albero. Poichè l'albero è binario ed ha rami di lunghezza arbitraria, allora a o ha un figlio o ne ha due. Infatti se non avesse figli allora l'albero avrebbe solo un ramo di lunghezza 1.

Se a ha un solo figlio a_1 , allora anche a_1 è la radice di un (sotto)albero con rami di lunghezza arbitraria: infatti se così non fosse, allora detta n la lunghezza massima dei rami che partono da a_1 si avrebbe che $n + 1$ è la lunghezza massima dei rami che partono da a , il che è contrario alla nostra ipotesi.

Continua la dimostrazione del Lemma di König

Se invece a ha due figli a_1 e a_2 , allora se ci fosse un massimo n_1 per la lunghezza dei rami che partono da a_1 e un massimo n_2 per la lunghezza dei rami che partono da a_2 si avrebbe che $\max(n_1, n_2) + 1$ è la lunghezza massima dei rami dell'albero con radice in a , che è contrario alla nostra ipotesi. Quindi almeno da uno dei due nodi a_1 e a_2 partono rami di lunghezza arbitraria, supponiamo che sia a_1 .

Possiamo allora ripetere questo ragionamento a partire dall'albero con radice in a_1 e così via, trovando che per ogni livello dell'albero c'è un nodo dal quale partono rami di lunghezza arbitraria. Ripetendo questo procedimento otteniamo il ramo infinito cercato.

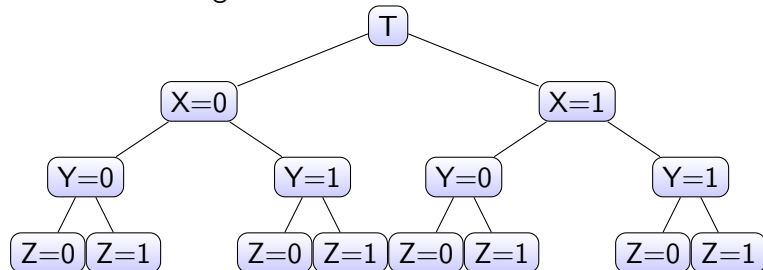
Ancora sul lemma di König

Nota che l'ipotesi che l'albero sia binario può essere sostituita con ternario o quaternario, etc.

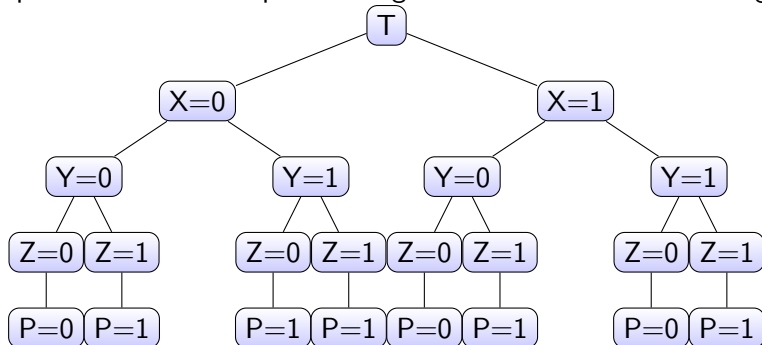
E' però fondamentale imporre che ogni nodo abbia al più un numero fissato di figli. Infatti se non ci fosse questa condizione potremmo considerare un albero costituito da una radice il cui primo figlio ha lunghezza 1, il secondo ha lunghezza 2, il terzo ha lunghezza 3, e così via: avremmo un albero con rami di lunghezza arbitraria senza avere però un ramo di lunghezza infinita.

Perché gli alberi

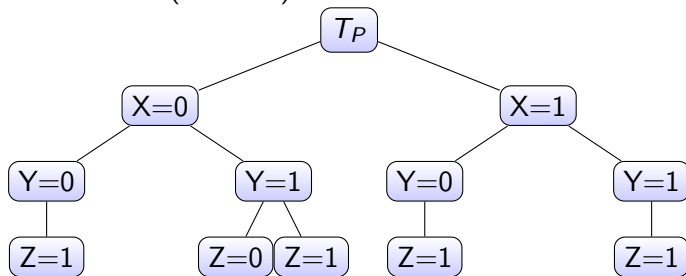
Possiamo rappresentare le valutazioni di una formula usando un albero. Le 8 valutazioni delle tre variabili X , Y e Z si possono rappresentare come gli 8 cammini sul seguente albero:



Consideriamo la formula $P = (X \vee \neg Y) \rightarrow Z$. Le 8 valutazioni possibili di questa formula corrispondenti agli 8 rami sono scritte nelle foglie:



Posso considerare l'albero costituito solo dai rami che soddisfano la formula $P = (X \vee \neg Y) \rightarrow Z$:



Lemma

Sia Γ un insieme di formule. Allora esiste un sottoinsieme $\Gamma' \subseteq \Gamma$ tale che Γ' non contiene formule logicamente equivalenti e Γ è soddisfacibile se e solo se Γ' è soddisfacibile.

Dimostrazione.

Basta scegliere una formula in ogni classe d'equivalenza di Γ / \equiv .

Dimostrazione del teorema di compattezza

Se Γ è soddisfacibile allora banalmente ogni suo sottoinsieme è soddisfacibile.

Viceversa, supponiamo che ogni sottoinsieme finito di Γ sia soddisfacibile, e supponiamo anche che in Γ non ci siano formule logicamente equivalenti. Abbiamo due casi: se le formule di Γ utilizzano solo un numero finito di variabili X_1, \dots, X_n , allora dato che Γ non contiene formule logicamente equivalenti, vuol dire che Γ avrà al massimo 2^{2^n} formule, quindi è un insieme finito. Quindi è soddisfacibile per ipotesi.

Se invece ci sono infinite variabili allora l'insieme Γ è infinito. Dobbiamo mostrare che esiste una valutazione che soddisfa tutte le formule di Γ . Per ogni n sia Γ_n l'insieme delle formule di Γ che utilizzano solo le variabili X_1, \dots, X_n . Per quanto abbiamo detto prima, Γ_n è finito e quindi soddisfacibile.

Consideriamo un albero binario T che abbia su ogni ramo una valutazione delle variabili: al primo livello ci saranno le due possibili valutazioni della variabile X_1 , al secondo le due possibili valutazioni di X_2 per ognuno dei due valori di X_1 , quindi quattro valutazioni in tutto, e così via.

Sia T_Γ il sottoalbero di T formato da tutti i cammini $ra_1 \cdots a_n$ che sono valutazioni delle variabili X_1, \dots, X_n che soddisfano Γ_n . L'albero T_Γ ha quindi rami di lunghezza arbitraria, perchè per ogni n ci sono valutazioni che soddisfano Γ_n . Quindi per il lemma di König, T_Γ ha un ramo infinito $ra_1a_2 \cdots$.

Consideriamo allora l'interpretazione $e(X_i) = a_i$. Dato che per ogni i si ha $\Gamma_i \subseteq \Gamma_{i+1}$, allora le valutazioni che soddisfano Γ_{i+1} soddisfano anche Γ_i . Quindi la valutazione e soddisfa tutte le formule dell'insieme Γ .

Esempio 1

Consideriamo l'insieme

$$\Gamma = \{X_1, X_3, X_5, \dots, X_{2i-1}, \dots, \\ X_1 \rightarrow \neg X_4, X_3 \rightarrow \neg X_8, X_5 \rightarrow \neg X_{12}, \dots, X_{2i-1} \rightarrow \neg X_{4i}, \dots\}.$$

Per controllare se l'insieme Γ è soddisfacibile dovremmo trovare una valutazione che soddisfi tutte le infinite formule di Γ .

Nota che ogni variabile e ogni formula del tipo $X \rightarrow Y$ è soddisfacibile.

Per il teorema di compattezza possiamo considerare i sottoinsiemi finiti:

- Tutti i sottoinsiemi finiti di Γ che contengono solo variabili o solo implicazioni sono soddisfacibili (non ci sono formule con le stesse variabili);
- I sottoinsiemi finiti di Γ che contengono alcune variabili e implicazioni che non contengono tali variabili, anche sono soddisfacibili (anche in questo caso non ci sono formule con le stesse variabili);
- Se un sottoinsieme finito contiene qualche variabile X_{2j-1} per $j \in J$ e qualche implicazione che contiene queste variabili quindi del tipo $X_{2j-1} \rightarrow X_{4j}$, allora è soddisfatto dalla valutazione v tale che $v(X_{2j-1}) = 1$ e $v(X_{4j}) = 0$.

Quindi, tutti i sottoinsiemi finiti sono soddisfacibili e quindi l'insieme Γ è soddisfacibile.

Vediamo il teorema applicato all'esempio

$$\Gamma = \{X_1, X_3, X_5, \dots, X_{2i-1}, \dots, \\ X_1 \rightarrow \neg X_4, X_3 \rightarrow \neg X_8, X_5 \rightarrow \neg X_{12}, \dots, X_{2i-1} \rightarrow \neg X_{4i}, \dots\}.$$

Consideriamo i seguenti insiemi finiti:

$$\Gamma_1 = \{X_1\}$$

$$\Gamma_2 = \{X_1\}$$

$$\Gamma_3 = \{X_1, X_3\}$$

$$\Gamma_4 = \{X_1, X_3, X_1 \rightarrow \neg X_4\}$$

...

Tutti questi insiemi sono soddisfacibili. Inoltre una valutazione che soddisfa Γ_i soddisfa anche Γ_{i-1} . Possiamo quindi costruire l'albero di tutte le valutazioni dei Γ_i che avrà un ramo infinito. Tale ramo infinito sarà la valutazione che soddisfa Γ .

Esempio 2

Consideriamo l'insieme

$$\Gamma = \{X_1, X_2, X_3, \dots, X_i, \dots, X_1 \rightarrow \neg X_2, X_2 \rightarrow \neg X_3, \dots, X_i \rightarrow \neg X_{i+1}, \dots\}.$$

Per controllare se l'insieme Γ è soddisfacibile dovremmo trovare una valutazione che soddisfi tutte le infinite formule di Γ .

Ma per il teorema di compattezza possiamo considerare i sottoinsiemi finiti:

- $\{X_1\}$ è soddisfacibile;
- $\{X_1, X_1 \rightarrow \neg X_2\}$ è soddisfacibile (per esempio con $v(X_1) = 1$ e $v(X_2) = 0$);
- $\{X_1, X_2, X_1 \rightarrow \neg X_2\}$ non è soddisfacibile.

Quindi, avendo trovato un sottoinsieme finito non soddisfacibile, l'insieme Γ non è soddisfacibile.

Corollary

Γ è insoddisfacibile se e solo se esiste un sottoinsieme finito di Γ che è insoddisfacibile.

Corollary

$\Gamma \models P$ se e solo se esiste un sottoinsieme finito Δ di Γ tale che $\Delta \models P$.