METODI MATEMATICI PER L'INFORMATICA

ANNO ACCADEMICO 2011/2012

SOMMARIO. Sintassi e semantica della logica proposizionale. Tavole di verità. Soddisfacibilità, validità, conseguenza logica. Teoremi di sostituzione. Verità logiche notevoli. Completezza funzionale. Forme Normali CNF e DNF. Principio di Dualità AND/OR.

N.B. (Dicembre 2012) Sono stati corretti dei refusi presenti nella versione precedente.

1. Linguaggio e proposizioni formali

Definizione 1.1 (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.

Definizione 1.2 (Proposizioni)**.** Sia $\mathcal{L}$ un linguaggio proposizionale. L'insieme delle proposizioni 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 $\mathrm{PROP}_{\mathcal{L}}$ l'insieme delle proposizioni nel linguaggio $\mathcal{L}$. Se $\mathcal{L}$ è chiaro dal contesto, scriviamo PROP.

Osservazione 1.3. 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.

Chiamiamo *chiuso* un insieme X che soddisfa (1)(2)(3). Assumiamo che esiste un insieme chiuso (questo si può dimostrare usando i normali assiomi della teoria degli insiemi), e dimostriamo che esiste un minimo insieme chiuso. Osserviamo che se X e Y sono insiemi chiusi, allora anche $X \cap Y$ è un insieme chiuso, e più in generale che se S è un insieme non vuoto di insiemi chiusi, allora anche l'intersezione $\bigcap S = \{Z \text{ tali che } (\forall W \in S)(Z \subseteq W)\}$ è un insieme chiuso.

Sia X un insieme chiuso. Sia ora S l'insieme di tutti i sottinsiemi chiusi di X. Allora $\bigcap S$ è un insieme chiuso, ed è minimo nel senso di sopra. Sia infatti Y un insieme chiuso qualunque. Allora per ogni $W \in S$, anche $Y \cap W$ è un sottinsieme chiuso di X. Dunque se $x \in \bigcap S$ allora $x \in Y \cap W$ e dunque $x \in Y$, che dimostra $\bigcap S \subseteq Y$.

Definizione 1.4 (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 $\{\wedge, \vee, \rightarrow, \leftrightarrow\}$.

Note preparate da Lorenzo Carlucci, carlucci@di.uniroma1.it.

2. Induzione e Ricorsione sulle Proposizioni

Proposizione 2.1 (Principio di Induzione Strutturale)**.** *Sia $\mathcal{L}$ un linguaggio proposizionale. Sia $\mathcal{A}$ una proprietà di stringhe. Se valgono i tre punti seguenti allora $\mathcal{A}$ vale di tutte le proposizioni nel linguaggio $\mathcal{L}$.*

1. *$\mathcal{A}$ vale di tutte le variabili proposizionali,*
2. *Se $\mathcal{A}$ vale di una stringa A, allora vale di $(\neg A)$,*
3. *Se $\mathcal{A}$ vale delle stringhe A e B, allora vale della stringa $(A\Box B)$, dove usiamo il simbolo $\Box$ come un segnaposto per uno dei connettivi $\{\wedge, \vee, \to, \leftrightarrow\}$.*

Dimostrazione. Consideriamo l'insieme X di tutte le stringhe nel linguaggio $\mathcal{L}$ che soddisfano la proprietà $\mathcal{A}$. Tale insieme soddisfa le tre condizioni nella definizione dell'insieme $\mathrm{PROP}_{\mathcal{L}}$ (ossia è un insieme chiuso). Dunque $\mathrm{PROP}_{\mathcal{L}} \subseteq X$, perché $\mathrm{PROP}_{\mathcal{L}}$ è per definizione il minimo insieme che soddisfa le tre condizioni in questione. □

Possiamo condurre dimostrazioni per induzione sull'insieme delle proposizioni anche usando la comune induzione matematica completa. Vediamo come.

Definizione 2.2. Sia $\mathcal{L}$ un linguaggio proposizionale e siano $\{p_1, p_2, \dots\}$ le sue variabili proposizionali. Definiamo una famiglia di insiemi di stringhe, per ricorsione su n.

$$\mathbf{F}_0 = \{p_1, p_2, \dots\}$$

$$\mathbf{F}_{n+1} = \mathbf{F}_n \cup \{(\neg A) \ : \ A \in \mathbf{F}_n\} \cup \{(A \wedge B), (A \vee B), (A \to B), (A \leftrightarrow B) \ : \ A, B \in \mathbf{F}_n\}$$

$$\mathbf{F} = \bigcup_{n \in \mathbf{N}} \mathbf{F}_n$$

Si può dimostrare che $\mathbf{F}$ coincide con l'insieme delle proposizioni nel linguaggio $\mathcal{L}$ (Esercizio). Definiamo l'altezza $h(A)$ di una proposizione A nel linguaggio $\mathcal{L}$ come il minimo n tale che $A \in \mathbf{F}_n$.

Per dimostrare che una proprietà $\mathcal{A}$ vale di tutte le proposizioni possiamo allora usare la usuale induzione matematica completa, dimostrando che per ogni $n \in \mathbf{N}$, $\mathcal{A}$ vale di tutte le proposizioni di altezza n.

Per esempio possiamo dimostrare il Principio di Induzione Strutturale usando l'induzione completa sull'altezza. Dimostriamo la Proposizione seguente.

Proposizione 2.3. *Se X è un insieme che soddisfa le tre condizioni del Principio di Induzione Strutturale allora* $\mathrm{PROP} \subseteq X$.

Dimostrazione. Supponiamo il contrario, e sia $A \in \mathrm{PROP} - X$ di altezza minima. Allora non può essere $h(A) = 0$, perché tutte le variabili proposizionali sono in X. Dunque $h(A) = n + 1$ per qualche $n \in \mathbf{N}$. Abbiamo due casi.

(Caso 1) Esiste una proposizione B tale che $h(B) = n$ e $A = (\neg B)$. Dato che A è stata scelta come proposizione non contenuta in X di altezza minimale, abbiamo che $B \in X$. Ma allora per ipotesi su X vale anche $(\neg B) \in X$. Contraddizione.

(Caso 2) Esistono due proposizioni B e C tali che $h(B), h(C) \leq n$ tali che $A = (B\Box C)$. Ancora per la minimalità di $h(A)$, vale che $B, C \in X$ e per ipotesi su X vale $(A\Box C) \in X$. Contraddizione. □

Le definizioni per ricorsione sono definizioni in cui i valori di una funzione su un certo argomento sono espressi come funzione dei valori della stessa funzione su argomenti più piccoli. Esempi elementari sono i seguenti.

$$x^0 = 1, \quad x^{n+1} = x^n \cdot x.$$

$$(x + 0) = x, \quad (x + (n + 1)) = (x + n) + 1.$$

$$(x + 1)! = x!(x + 1).$$

Dimostriamo che si possono definire funzioni per ricorsione sull'insieme delle proposizioni. Sia X un insieme. Si possono definire per ricorsione funzioni di tipo $\mathrm{PROP} \to X$.

Proposizione 2.4 (Principio di Definizione per Ricorsione)**.** *Sia X un insieme. Siano*

$$f : X \times X \to X,$$
$$g : X \to X,$$
$$h : \mathrm{VAR} \to X.$$

Allora esiste ed è unica una funzione

$$F : \mathrm{PROP} \to X$$

tale che

(1) $F(A) = h(A)$ *se A è una variabile proposizionale,*
(2) $F(\neg A) = g(F(A))$,
(3) $F((A \square B)) = f(F(A), F(B))$.

Dimostrazione. Esercizio! □

Diamo alcuni esempi di definizioni per ricorsione.

Esempio 2.5. Definiamo per ricorsione il rango di una proposizione.

$$r(A) = \begin{cases} 0 & \text{se } A \in \mathrm{VAR} \\ r(B) + 1 & \text{se } A = (\neg B) \\ \max(r(B), r(C)) + 1 & \text{se } A = (B \square C) \end{cases}$$

Si può dimostrare che $r(A) = h(A)$, dove h è l'altezza definita sopra.

Esempio 2.6. Definiamo per ricorsione il numero di parentesi di una proposizione.

$$b(A) = \begin{cases} 0 & \text{se } A \in \mathrm{VAR} \\ b(B) + 2 & \text{se } A = (\neg B) \\ b(B) + b(C) + 2 & \text{se } A = (B \square C) \end{cases}$$

Esempio 2.7. Definiamo per ricorsione una funzione che associa ad una proposizione un albero finito con radice i cui nodi sono etichettati da proposizioni.

- $T(A)$ è l'albero consistente di un solo nodo etichettato con A, se A è una variabile proposizionale.
- $T((\neg A))$ è l'albero consistente di un nodo etichettato con $(\neg A)$ il cui unico figlio è l'albero $T(A)$.
- $T((A \square B))$ è l'albero consistente di un nodo etichettato con $(A \square B)$ il cui figlio sinistro è l'albero $T(A)$ e il cui figlio destro è l'albero $T(B)$.

$T(A)$ è detto il *parsing tree* di A.

3. Espressività della Logica Proposizionale

Vogliamo usare la Logica Proposizionale per giudicare in modo rigoroso (e per quanto possibile automatizzabile) della validità di argomenti e della verità di proposizioni. Ma che tipo di argomenti e che tipo di proposizioni possiamo formalizzare nel linguaggio proposizionale?

Diamo tre esempi per farci un'idea.

Esempio 3.1. Semplici argomenti matematici che non riguardano i quantificatori.

(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 le parti atomiche, ossia quelle parti che non possono essere ulteriormente analizzate in termini di connettivi logici booleani e che possono essere vere o false. Nel nostro caso, queste parti atomiche sono $a = 0$, $b = 0$, e $a \cdot b = 0$. Associamo a ciascuna parte atomica una distinta variabile proposizionale: a $a = 0$ associamo p_1, a $b = 0$ associamo p_2, a $a \cdot b = 0$ associamo p_3. Infine sostituiamo i costrutti logici del linguaggio naturale (Se...allora, o, e, non) con i connettivi formali. Otteniamo la seguente formalizzazione.

(i) $(p_1 \vee p_2) \to p_3$.
(ii) $(\neg p_3)$.
(iii) $(\neg p_1 \wedge \neg p_2)$.

Quando avremo sviluppato rigorosamente la nozione di conseguenza logica avremo un criterio rigoroso per giudicare la validità dell'argomento che ha per premesse $(p_1 \vee p_2) \to p_3$ e $(\neg p_3)$ e per conclusione $(\neg p_1 \vee \neg p_2)$. In altre parole potremo rispondere alla domanda: la conclusione segue logicamente dalle premesse? Osserviamo che la validità dell'argomento non dipenderà più dal significato matematico delle parti atomiche ma solo dal loro essere vere o false (dal loro *valore di verità*). Se l'argomento formalizzato è valido, allora sono validi tutti gli argomenti ottenuti sostituendo proposizioni alle variabili proposizionali. Per esempio, se l'argomento di sopra è valido, allora è valido anche il seguente.

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

Esempio 3.2. Semplici argomenti verbali. La logica proposizionale si presta bene anche a a formalizzare argomenti verbali.

(1) Se studi e sei intelligente allora superi l'esame.
(2) Se sei intelligente allora studi.
(3) Non superi l'esame.
(4) Sei scemo.

Come si formalizza? Le parti atomiche in questo caso sono (studi), (sei intelligente), (superi l'esame). Possiamo infatti assumere che (sei scemo) equivalga a (non sei intelligente). Associamo p_1 a (studi), p_2 a (sei intelligente), p_3 a (superi l'esame). L'argomento si formalizza così.

(i) $(p_1 \wedge p_2) \to p_3$.
(ii) $p_2 \to p_1$.
(iii) $\neg p_3$.
(iv) $\neg p_2$.

Esempio 3.3. Principi combinatori su domini finiti. Questo esempio illustra come formalizzare in logica proposizionale principi matematici in cui appaiono quantificatori (per ogni, esiste) ma solo su un numero finito di oggetti. Consideriamo il famoso Principio dei Cassetti (o dei Piccioni, *Pigeonhole Principle*.

> **Principio dei Cassetti**. Per ogni $n \in \mathbf{N}$, $n \geq 1$, se ho messo $n+1$ oggetti in n cassetti allora un cassetto contiene più di un oggetto.

Indichiamo questo principio, per ogni $n \geq 1$ fissato, con $PHP(n+1, n)$. Ovviamente un analogo principio vale se usiamo un qualunque $m \geq n+1$ al posto di $n+1$. In termini più matematici, $PHP(n+1, n)$ si può esprimere come segue.

> **PHP**$(\mathbf{n+1}, \mathbf{n})$. Se f è una funzione suriettiva con dominio $\{1, \ldots, n+1\}$ e codominio $\{1, \ldots, n\}$, allora esiste un elemento del codominio che ha almeno due preimmagini secondo f.

In altre parole, non esiste una funzione iniettiva e suriettiva con dominio $\{1, \ldots, n+1\}$ e codominio $\{1, \ldots, n\}$. Per ogni scelta di n, facciamo vedere come formalizzare $PHP(n+1, n)$ nel linguaggio proposizionale.

Fissiamo per semplicità $n = 3$. Vogliamo formalizzare $PHP(4, 3)$, che dice che se f è una funzione suriettiva con dominio $\{1, 2, 3, 4\}$ e codominio $\{1, 2, 3\}$ allora un elemento del dominio ha almeno due preimmagini secondo f. Spezziamo questo enunciato in tre parti.

(1) f è una associazione suriettiva con dominio $\{1, 2, 3, 4\}$ e codominio $\{1, 2, 3\}$.
(2) f è una funzione con dominio $\{1, 2, 3, 4\}$ e codominio $\{1, 2, 3\}$.
(3) f non è iniettiva.

Dobbiamo formalizzare: **Se** f è una funzione suriettiva con dominio $\{1, 2, 3, 4\}$ e codominio $\{1, 2, 3\}$ **allora** f non è iniettiva. Ossia **Se** ((1) e (2)) allora (3).

Un linguaggio adeguato per formalizzare $PHP(4,3)$ è il linguaggio che ha come variabili proposizionali i simboli $p_{i,j}$, dove i varia in $\{1,2,3,4\}$ e j varia in $\{1,2,3\}$. Dunque le variabili del linguaggio sono 12 in tutto. (N.B.B. I simboli $p_{i,j}$ non fanno parte del linguaggio!! Sono solo un modo comodo per quantificare su $\{1,2,3,4\}$ e $\{1,2,3\}$. Le vere variabili sono simboli del tipo $p_{1,1}$, $p_{4,2}$, $p_{4,3}$ etc.). Il significato *intuitivo* delle variabili scelte è il seguente.

$$p_{i,j} \text{ sta per } f(i) = j.$$

Cominciamo a formalizzare (1). f è suriettiva se e solo se ogni elemento del codominio ha una preimmagine nel dominio, i.e., se e solo

$$\forall j \in \{1,2,3\} \exists i \in \{1,2,3,4\}(f(i) = j).$$

Anche se stiamo usando delle quantificazioni possiamo formalizzare l'enunciato in logica proposizionale perché stiamo quantificando su insiemi finiti. Possiamo quindi enumerare tutte le possibilità, e usare $\vee$ per tradurre $\exists$ e $\wedge$ per tradurre $\forall$.

Per $j = 1$, dobbiamo tradurre

$$\exists i \in \{1,2,3,4\}(f(i) = 1).$$

$f(i) = 1$ si traduce ovviamente con $p_{i,1}$. La quantificazione esistenziale sull'insieme $\{1,2,3,4\}$ si traduce con una disgiunzione a quattro termini:

$$p_{1,1} \vee p_{2,1} \vee p_{3,1} \vee p_{4,1}.$$

Per $j = 2$, dobbiamo tradurre

$$\exists i \in \{1,2,3,4\}(f(i) = 2).$$

Analogamente a quanto visto sopra otteniamo

$$p_{1,2} \vee p_{2,2} \vee p_{3,2} \vee p_{4,2}.$$

Per $j = 3$ otteniamo in modo analogo

$$p_{1,3} \vee p_{2,3} \vee p_{3,3} \vee p_{4,3}.$$

Dobbiamo ora mettere insieme le tre proposizioni ottenute in modo da esprimere la quantificazione universale $\forall j \in \{1,2,3\} \ldots$. Basta usare la congiunzione, perché la quantificazione universale in questione sta dicendo che

$$\text{Se } j = 1 \text{ allora } \exists i \in \{1,2,3,4\}(f(i) = 1),$$

e

$$\text{Se } j = 2 \text{ allora } \exists i \in \{1,2,3,4\}(f(i) = 2),$$

e

$$\text{Se } j = 3 \text{ allora } \exists i \in \{1,2,3,4\}(f(i) = 3).$$

Otteniamo quindi la proposizione

$$(p_{1,1} \vee p_{2,1} \vee p_{3,1} \vee p_{4,1}) \wedge (p_{1,2} \vee p_{2,2} \vee p_{3,2} \vee p_{4,2}) \wedge (p_{1,3} \vee p_{2,3} \vee p_{3,3} \vee p_{4,3}).$$

come formalizzazione di (f è una associazione suriettiva da $\{1,2,3,4\}$ su $\{1,2,3\}$).

Ora formalizziamo (2). f è una funzione (e non una semplice relazione) se e solo se non esiste un elemento del dominio che ha due immagini distinte. In altre parole, per ogni elemento i del dominio, per ogni scelta di due immagini distinte j, j' nel codominio, dobbiamo dire che non è possibile che $f(i) = j$ e $f(i) = j'$. In altre parole dobbiamo formalizzare la seguente proposizione.

$$\forall i \in \{1,2,3,4\} \forall j \neq j' \in \{1,2,3\}(f(i) \neq j \vee f(i) \neq j').$$

Come sopra, consideriamo i possibili valori di i uno per uno.

Per $i = 1$ dobbiamo formalizzare

$$\forall j \neq j' \in \{1,2,3\}(f(1) \neq j \vee f(1) \neq j').$$

Per ogni scelta di $j, j' \in \{1,2,3\}$ con $j \neq j'$ dobbiamo formalizzare

$$(f(1) \neq j \vee f(1) \neq j').$$

Per questo basta scrivere $\neg(p_{1,j} \wedge p_{1,j'})$. Dato che la quantificazione è universale, dobbiamo congiungere tutte le proposizioni così ottenute. Otteniamo

$$\neg(p_{1,1} \wedge p_{1,2}) \wedge \neg(p_{1,1} \wedge p_{1,3}) \wedge \neg(p_{1,2} \wedge p_{1,3}).$$

Per $i = 2$ dobbiamo formalizzare

$$\forall j \neq j' \in \{1,2,3\}(f(2) \neq j \vee f(2) \neq j').$$

Analogamente a sopra ottenitamo

$$\neg(p_{2,1} \wedge p_{2,2}) \wedge \neg(p_{2,1} \wedge p_{2,3}) \wedge \neg(p_{2,2} \wedge p_{2,3}).$$

Per $i = 3$ con lo stesso ragionamento otteniamo

$$\neg(p_{3,1} \wedge p_{3,2}) \wedge \neg(p_{3,1} \wedge p_{3,3}) \wedge \neg(p_{3,2} \wedge p_{3,3}).$$

Per $i = 4$ con lo stesso ragionamento otteniamo

$$\neg(p_{4,1} \wedge p_{4,2}) \wedge \neg(p_{4,1} \wedge p_{4,3}) \wedge \neg(p_{4,2} \wedge p_{4,3}).$$

Ora possiamo esprimere la quantificazione su i, $\forall i \in \{1,2,3,4\} \dots$ congiungendo le quattro proposizioni ottenute per i singoli valori di i.

$$\neg(p_{1,1} \wedge p_{1,2}) \wedge \neg(p_{1,1} \wedge p_{1,3}) \wedge \neg(p_{1,2} \wedge p_{1,3}) \wedge \neg(p_{2,1} \wedge p_{2,2}) \wedge \neg(p_{2,1} \wedge p_{2,3}) \wedge \neg(p_{2,2} \wedge p_{2,3}) \wedge$$
$$\neg(p_{3,1} \wedge p_{3,2}) \wedge \neg(p_{3,1} \wedge p_{3,3}) \wedge \neg(p_{3,2} \wedge p_{3,3}) \wedge \neg(p_{4,1} \wedge p_{4,2}) \wedge \neg(p_{4,1} \wedge p_{4,3}) \wedge \neg(p_{4,2} \wedge p_{4,3}).$$

Ora formalizziamo (3). f non è iniettiva se e solo se non esiste un elemento del codominio con due preimmagini distinte secondo f. In altre parole, f non è iniettiva se e solo se per ogni elemento j del codominio, per ogni scelta di due preimmagini distinte i, i' nel dominio, non è vero che $f(i) = j$ e $f(i') = j$. Dobbiamo quindi formalizzare l'enunciato seguente.

$$(\forall j \in \{1,2,3\} \forall i \neq i' \in \{1,2,3,4\}(f(i) \neq j \vee f(i') \neq j).$$

Procediamo come sopra. Consideriamo uno per uno i valori di j.

Per $j = 1$, dobbiamo formalizzare

$$\forall i \neq i' \in \{1,2,3,4\}(f(i) \neq 1 \vee f(i') \neq 1).$$

Per ognuna delle $\binom{4}{2}$ scelte di due elementi distinti $i, i' \in \{1,2,3,4\}$ dobbiamo formalizzare $(f(i) \neq 1 \vee f(i') \neq 1)$. Quest'ultimo enunciato si formalizza ovviamente con $\neg(p_{i,1} \wedge p_{i',1})$ (o equivalentemente con $(\neg p_{i,1} \vee \neg p_{i',1})$). Dato che la quantificazione su i, i' è universale, otteniamo la seguente congiunzione.

$$\neg(p_{1,1} \wedge p_{2,1}) \wedge \neg(p_{1,1} \wedge p_{3,1}) \wedge \neg(p_{1,1} \wedge p_{4,1}) \wedge \neg(p_{2,1} \wedge p_{3,1}) \wedge \neg(p_{2,1} \wedge p_{4,1}) \wedge \neg(p_{3,1} \wedge p_{4,1}).$$

Analogamente, per $j = 2$ otteniamo

$$\neg(p_{1,2} \wedge p_{2,2}) \wedge \neg(p_{1,2} \wedge p_{3,2}) \wedge \neg(p_{1,2} \wedge p_{4,2}) \wedge \neg(p_{2,2} \wedge p_{3,2}) \wedge \neg(p_{2,2} \wedge p_{4,2}) \wedge \neg(p_{3,2} \wedge p_{4,2}).$$

Analogamente, er $j = 3$ otteniamo

$$\neg(p_{1,3} \wedge p_{2,3}) \wedge \neg(p_{1,3} \wedge p_{3,3}) \wedge \neg(p_{1,3} \wedge p_{4,3}) \wedge \neg(p_{2,3} \wedge p_{3,3}) \wedge \neg(p_{2,3} \wedge p_{4,3}) \wedge \neg(p_{3,3} \wedge p_{4,3}).$$

Infine, per esprimere la quantificazione universale $\forall j \in \{1,2,3\} \dots$ basta prendere la congiunzione delle tre proposizioni ottenute per i singoli valori di j.

$$\neg(p_{1,1} \wedge p_{2,1}) \wedge \neg(p_{1,1} \wedge p_{3,1}) \wedge \neg(p_{1,1} \wedge p_{4,1}) \wedge \neg(p_{2,1} \wedge p_{3,1}) \wedge \neg(p_{2,1} \wedge p_{4,1}) \wedge \neg(p_{3,1} \wedge p_{4,1}) \wedge$$
$$\neg(p_{1,2} \wedge p_{2,2}) \wedge \neg(p_{1,2} \wedge p_{3,2}) \wedge \neg(p_{1,2} \wedge p_{4,2}) \wedge \neg(p_{2,2} \wedge p_{3,2}) \wedge \neg(p_{2,2} \wedge p_{4,2}) \wedge \neg(p_{3,2} \wedge p_{4,2}) \wedge$$
$$\neg(p_{1,3} \wedge p_{2,3}) \wedge \neg(p_{1,3} \wedge p_{3,3}) \wedge \neg(p_{1,3} \wedge p_{4,3}) \wedge \neg(p_{2,3} \wedge p_{3,3}) \wedge \neg(p_{2,3} \wedge p_{4,3}) \wedge \neg(p_{3,3} \wedge p_{4,3}).$$

Per concludere, possiamo formalizzare $PHP(4,3)$ formalizzando: Se ((1) e (2)) allora (3). Otteniamo la proposizione seguente.

$$((p_{1,1} \vee p_{2,1} \vee p_{3,1} \vee p_{4,1}) \wedge (p_{1,2} \vee p_{2,2} \vee p_{3,2} \vee p_{4,2}) \wedge (p_{1,3} \vee p_{2,3} \vee p_{3,3} \vee p_{4,3}) \wedge$$
$$\neg(p_{1,1} \wedge p_{1,2}) \wedge \neg(p_{1,1} \wedge p_{1,3}) \wedge \neg(p_{1,2} \wedge p_{1,3}) \wedge \neg(p_{2,1} \wedge p_{2,2}) \wedge \neg(p_{2,1} \wedge p_{2,3}) \wedge \neg(p_{2,2} \wedge p_{2,3}) \wedge$$
$$\neg(p_{3,1} \wedge p_{3,2}) \wedge \neg(p_{3,1} \wedge p_{3,3}) \wedge \neg(p_{3,2} \wedge p_{3,3}) \wedge \neg(p_{4,1} \wedge p_{4,2}) \wedge \neg(p_{4,1} \wedge p_{4,3}) \wedge \neg(p_{4,2} \wedge p_{4,3})) \rightarrow$$
$$(\neg(p_{1,1} \wedge p_{2,1}) \wedge \neg(p_{1,1} \wedge p_{3,1}) \wedge (p_{1,1} \wedge p_{4,1}) \wedge \neg(p_{2,1} \wedge p_{3,1}) \wedge \neg(p_{2,1} \wedge p_{4,1}) \wedge \neg(p_{3,1} \wedge p_{4,1}) \wedge$$
$$\neg(p_{1,2} \wedge p_{2,2}) \wedge \neg(p_{1,2} \wedge p_{3,2}) \wedge \neg(p_{1,2} \wedge p_{4,2}) \wedge \neg(p_{2,2} \wedge p_{3,2}) \wedge \neg(p_{2,2} \wedge p_{4,2}) \wedge \neg(p_{3,2} \wedge p_{4,2}) \wedge$$
$$\neg(p_{1,3} \wedge p_{2,3}) \wedge \neg(p_{1,3} \wedge p_{3,3}) \wedge \neg(p_{1,3} \wedge p_{4,3}) \wedge \neg(p_{2,3} \wedge p_{3,3}) \wedge \neg(p_{2,3} \wedge p_{4,3}) \wedge \neg(p_{3,3} \wedge p_{4,3})).$$

Tanta fatica per formalizzare un singolo caso del Principio dei Cassetti? Osserviamo che la formalizzazione svolta sopra è *uniforme* nel senso che se volessimo formalizzare $PHP(101, 100)$ o $PHP(2^9, 2^9 - 1)$ potremmo usare lo stesso procedimento. Avremmo proposizioni più lunghe ma di stessa struttura.

4. Semantica della Logica Proposizionale

Definizione 4.1 (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 4.2. 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 $0 \to 0$.

5. 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 $A = ((\neg P) \wedge Q) \to R)$.

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.

6. Soddisfacibilità, conseguenza logica, validità logica

Definizione 6.1 (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 6.2 (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 6.3 (Equivalenza Logica)**.** Diciamo che A e B sono logicamente equivalenti se per ogni assegnamento v, $v(A) = v(B)$. In questo caso scriviamo $A \equiv B$.

Definizione 6.4 (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.

Si osserva che A è una tautologia se e solo se $\models A$. Anche, $A \equiv B$ se e solo se $\models (A \leftrightarrow B)$.

Si osserva che $A \in$ Sat è un concetto *esistenziale*:

$$A \in \textsc{Sat} \Leftrightarrow \exists v(v(A) = 1),$$

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

$$A \in \textsc{Taut} \Leftrightarrow \forall v(v(A) = 1),$$

Esiste la seguente dualità tra Taut e UnSat:

$$A \in \textsc{Taut} \Leftrightarrow \neg A \in \textsc{UnSat}.$$

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

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

Lemma 6.5. *Siano $A_1, \ldots, A_n, A$ proposizioni. Allora i seguenti punti sono equivalenti.*

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

Dimostrazione. Esercizio! □

Osservazione 6.6. 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.

7. Teoremi di Sostituzione

Vogliamo dimostrare che valgono le seguenti proprietà (intuitivamente corrette).

(1) Se A è una tautologia, se sostituisco in A una variabile proposizionale con una formula qualunque, ottengo ancora una tautologia.
(2) Se A e B sono equivalenti, e sostituisco sia in A che in B una stessa variabile proposizionale con una stessa formula qualunque, ottengo due formule equivalenti.
(3) Se sostituisco in una stessa formula A una variabile proposizionale con due formule equivalenti, ottengo due formule equivalenti.

Siano $A, B_1, \ldots, B_n$ proposizioni, siano $p_1, \ldots, p_n$ variabili proposizionali distinte. Denotiamo con $A[p_1/B_1 \ldots p_n/B_n]$ il risultato di sostituire simultaneamente nella proposizione A la variabile proposizionale p_i con la formula B_i, per ogni $i \in \{1, \ldots, n\}$. Nota bene: la sostituzione è un'operazione puramente sintattica che trasforma proposizioni in proposizioni, e la sostituzione deve essere simultanea, non sequenziale! La proposizione $A[p_1/B_1 \ldots p_n/B_n]$ può essere definita rigorosamente per ricorsione (Esercizio!).

Otteniamo (1) e (2) come conseguenze del seguente teorema.

Teorema 7.1. *Siano $A, B_1, \ldots, B_n$ proposizioni, siano $p_1, \ldots, p_n$ variabili proposizionali distinte. Abbreviamo $A[p_1/B_1 \ldots p_n/B_n]$ con A^*. Sia v un assegnamento. Definiamo un nuovo assegnamento $v^* : \mathrm{VAR} \to \{0, 1\}$ (in funzione di v, p_i, B_i) come segue.*

$$v^*(Q) = \begin{cases} v(Q) & \text{se } Q \neq P_i \text{ per ogni } i \in \{1, \ldots, n\} \\ v(B_i) & \text{se } Q = P_i \text{ per qualche } i \in \{1, \ldots, n\}. \end{cases}$$

Allora

$$v(A^*) = v^*(A).$$

Dimostrazione. Per induzione strutturale su A.

(Caso Base) A è una variabile proposizionale Q. Distinguiamo due casi.

Se Q è p_i per un $i \in \{1, \ldots, n\}$, allora

$$A^* = Q[p_1/B_1 \ldots p_n/B_n] = p_i[p_1/B_1 \ldots p_n/B_n] = B_i.$$

Dunque

$$v(A^*) = v(B_i) = v^*(p_i) = v^*(A).$$

Se Q è diversa da p_i per ogni $i \in \{1, \ldots, n\}$, allora

$$A^* = Q[p_1/B_1 \ldots p_n/B_n] = Q.$$

Dunque

$$v(A^*) = v(Q) = v^*(Q) = v^*(A).$$

(Caso induttivo 1) Sia A la formula $(\neg C)$.

$$A^* = (\neg C)^* = (\neg C)[p_1/B_1 \ldots p_n/B_n] = (\neg C[p_1/B_1 \ldots p_n/B_n]) = (\neg C^*).$$

Allora

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

D'altra parte,

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

Per ipotesi induttiva $v^*(C) = v(C^*)$. Dunque $v(A^*) = v^*(A)$.

(Caso induttivo 2) Sia A la formula $(C \wedge D)$.

$$A^* = (C \wedge D)^* = (C[p_1/B_1 \ldots p_n/B_n] \wedge D[p_1/B_1 \ldots p_n/B_n]) = (C^* \wedge D^*).$$

$$v(A^*) = v(C^* \wedge D^*) = \begin{cases} 1 & \text{se } v(C^*) = v(D^*) = 1 \\ 0 & \text{altrimenti} \end{cases}$$

D'altra parte

$$v^*(A) = v^*(C \wedge D) = \begin{cases} 1 & \text{se } v^*(C) = v^*(D) = 1 \\ 0 & \text{altrimenti} \end{cases}$$

Per ipotesi induttiva $v(C^*) = v^*(C)$ e $v(D^*) = v^*(D)$.

I casi degli altri connettivi si trattano analogamente. □

Corollario 7.2 (Sostituzione in tautologie)**.** *Siano $A, B_1, \ldots, B_n$ proposizioni, siano $p_1, \ldots, p_n$ variabili proposizionali distinte. Se A è una tautologia allora $A[p_1/B_1 \ldots p_n/B_n]$ è una tautologia.*

Dimostrazione. Segue facilmente dal teorema precedente. Esercizio! □

Corollario 7.3 (Sostituzione in formule equivalenti)**.** *Siano $C, D, B_1, \ldots, B_n$ proposizioni, siano $p_1, \ldots, p_n$ variabili proposizionali distinte. Se $\models (C \leftrightarrow D)$ allora*

$$\models (C[p_1/B_1 \ldots p_n/B_n]) \leftrightarrow (D[p_1/B_1 \ldots p_n/B_n]).$$

Dimostrazione. Segue facilmente dal teorema precedente. Esercizio! □

Dimostriamo ora un risultato duale del precedente: l'equivalenza logica è preservata sostituendo all'interno di una formula variabili proposizionali con formule logicamente equivalenti.

Lemma 7.4. *$\models (A \to B)$ se e solo se $v(A) \leq v(B)$, per ogni assegnamento v.*

Dimostrazione. Esercizio! □

Teorema 7.5. *Siano A, B_1, B_2 proposizioni e sia p una variabile proposizionale. Allora*

$$v(B_1 \leftrightarrow B_2) \leq v(A[p/B_1] \leftrightarrow A[p/B_2]).$$

Osserviamo che dal Teorema, usando il Lemma precedente, segue il risultato desiderato, ossia

$$\models (B_1 \leftrightarrow B_2) \to (A[p/B_1] \leftrightarrow A[p/B_2]).$$

Dimostriamo ora il Teorema.

Dimostrazione. Il caso $v(B_1 \leftrightarrow B_2) = 0$ è facile: ovviamente $0 \leq v(A[p/B_1] \leftrightarrow A[p/B_2])$. Consideriamo il caso $v(B_1 \leftrightarrow B_2) = 1$. Procediamo per induzione su A.

(Caso Base) A è una variabile proposizionale. Distinguiamo due sottocasi.

Se A è p, allora

$$A[p/B_1] = p[p/B_1] = B_1$$

e

$$A[p/B_2] = p[p/B_2] = B_2.$$

La tesi è allora che $v(B_1 \leftrightarrow B_2) = 1$, che è vera per ipotesi.

Se A non è p, allora

$$A[p/B_1] = A$$

e

$$A[p/B_1] = A$$

La tesi è allora che $v(A \leftrightarrow A) = 1$, che è ovviamente vero.

(Caso Induttivo 1) Sia A la proposizione $(\neg C)$. Allora

$$A[p/B_1] = (\neg C[p/B_1]),$$

e

$$A[p/B_2] = (\neg C[p/B_2]).$$

Per ipotesi induttiva su C vale che $v(C[p/B_1] \leftrightarrow C[p/B_2]) = 1$. Questo vale se e solo se

$$v(C[p/B_1]) = v(C[p/B_2]).$$

Allora

$$v(A[p/B_1]) = v((\neg C[p/B_1]) = v(\neg C[p/B_2]) = v(A[p/B_2]),$$

perché il valore $v(\neg X)$ dipende soltanto dal valore di verità $v(X)$.

(Caso Induttivo 2) Trattiamo uniformemente il caso dei connettivi binari. Sia A la proposizione $(C \Box D)$. Allora

$$A[p/B_1] = (C[p/B_1] \Box D[p/B_1]),$$

e

$$A[p/B_2] = (C[p/B_2] \Box D[p/B_2]).$$

Per ipotesi induttiva su C vale che $v(C[p/B_1] \leftrightarrow C[p/B_2]) = 1$. Questo vale se e solo se

$$v(C[p/B_1]) = v(C[p/B_2]).$$

Per ipotesi induttiva su D vale che $v(D[p/B_1] \leftrightarrow D[p/B_2]) = 1$. Questo vale se e solo se

$$v(D[p/B_1]) = v(D[p/B_2]).$$

Ma allora

$$v(A[p/B_1]) = v((C[p/B_1] \Box D[p/B_1]) = v(C[p/B_2] \Box D[p/B_2]) = v(A[p/B_2]),$$

perché $(x, y) \mapsto v(x \Box y)$ è una funzione dei valori di verità $v(x)$ e $v(y)$. □

8. Principi generali e verità notevoli

Enunciamo alcune proprietà fondamentali della conseguenza logica e alcune leggi logiche notevoli. Tutte le dimostrazioni sono lasciate per Esercizio.

8.1. **Proprietà della conseguenza logica.** La relazione $\models$ di conseguenza logica gode delle seguenti proprietà

(1) $A \models A$
(2) Se $A \models B$ e $B \models C$ allora $A \models C$
(3) $A \models B$ se e solo se $\models (A \to B)$.

La relazione di equivalenza logica (definita come $A \equiv B$ se e solo se $\models (A \leftrightarrow B)$) è invece una relazione di equivalenza sull'insieme delle proposizioni.

(1) $A \equiv A$
(2) Se $A \equiv B$ e $B \equiv C$ allora $A \equiv C$
(3) Se $A \equiv B$ allora $B \equiv A$.

8.2. **Leggi Algebriche.**

(1) Associatività
  (a) $(A \vee (B \vee C)) \equiv A \vee (B \vee C)$
  (b) $(A \wedge (B \wedge C)) \equiv A \wedge (B \wedge C)$
(2) Commutatività
  (a) $(A \vee B) \equiv (B \vee A)$
  (b) $(A \wedge B) \equiv (B \wedge A)$
(3) Distributività
  (a) $(A \vee (B \wedge C)) \equiv (A \vee B) \wedge (A \vee C)$
  (b) $(A \wedge (B \vee C)) \equiv (A \wedge B) \vee (A \wedge C)$
(4) Leggi di De Morgan
  (a) $\neg(A \vee B) \equiv (\neg A \wedge \neg B)$
  (b) $\neg(A \wedge B) \equiv (\neg A \vee \neg B)$
(5) Doppia Negazione $\neg\neg A \equiv A$
(6) Idempotenza
  (a) $(A \vee A) \equiv A$
  (b) $(A \wedge A) \equiv A$

8.3. **Interdefinibilità dei connettivi.** Questo gruppo di leggi logiche notevoli illustra la possibilità di definire alcuni connettivi in funzione di altri.

(1) $(A \leftrightarrow B) \equiv ((A \to B) \wedge (B \to A))$
(2) $(A \to B) \equiv (\neg A \vee B)$
(3) $(A \vee B) \equiv (\neg A \to B)$
(4) $(A \vee B) \equiv \neg(\neg A \wedge \neg B)$
(5) $(A \wedge B) \equiv \neg(\neg A \vee \neg B)$

Possiamo dimostrare l'equivalenza logica di due formule usando le verità notevoli qui sopra *e i teoremi di sostituzione*, scrivendo una serie di equazioni logiche.

Esempio Dimostriamo che $\models (A \to (B \to C) \leftrightarrow ((A \wedge B) \to C)$.

$$\begin{aligned} A \to (B \to C) &\equiv \neg A \vee (B \to C) \\ &\equiv \neg A \vee (\neg B \vee C) \\ &\equiv (\neg A \vee \neg B) \vee C \\ &\equiv \neg(A \wedge B) \vee C \\ &\equiv (A \wedge B) \to C \end{aligned}$$

Esempio Dimostriamo che $\models (A \to B) \leftrightarrow (\neg B \to \neg A)$.

$$\begin{aligned} \neg B \to \neg A &\equiv \neg\neg B \vee \neg A \\ &\equiv B \vee \neg A \\ &\equiv \neg A \vee B \\ &\equiv A \to B \end{aligned}$$

8.4. **Altre leggi algebriche.** Se conveniamo di usare — all'interno di proposizioni — la costante 1 al posto di una qualunque tautologia e la costante 0 al posto di una qualunque formula insoddisfacibile, allora possiamo formulare le seguenti leggi algebriche aggiuntive.

(1) Assorbimento
   (a) $(A \vee 0) \equiv A$
   (b) $(A \wedge 1) \equiv A$
(2) Contraddizione, Terzo Escluso
   (a) $(A \vee \neg A) \equiv 1$
   (b) $(A \wedge \neg A) \equiv 0$

9. Completezza Funzionale

Siamo sicuri che con connettivi che abbiamo scelto siamo capaci di rappresentare il comportamento di qualunque funzione di verità

$$f : \{0,1\}^n \to \{0,1\}$$

a n argomenti, per $n \in \mathbf{N}$?

Teorema 9.1. *Sia $f : \{0,1\}^n \to \{0,1\}$ una funzione di verità. Esiste una proposizione A contenente n variabili proposizionali $\{p_1, \ldots, p_n\}$ e i connettivi logici $\{\neg, \vee, \wedge\}$ e tale che per ogni assegnamento v,*

$$v(A) = f(v(p_1), \ldots, v(p_n)).$$

Dimostrazione. Per induzione su n.

Se $n = 1$ abbiamo solo quattro possibili f.

$$\begin{aligned} f_1(0) = 0, f_1(1) = 0 \\ f_2(0) = 1, f_2(1) = 1 \\ f_3(0) = 0, f_3(1) = 1 \end{aligned}$$

$$f_4(0) = 1, f_4(1) = 0$$

Alla funzione f_1 corrisponde la formula $(p \wedge \neg p)$, alla funzione f_2 la formula $(p \vee \neg p)$, allora funzione f_3 la formula p, e alla funzione f_4 la formula $(\neg p)$.

Se $n > 1$, scriviamo il grafico di $f : \{0,1\}^n \to \{0,1\}$ in forma di tavola di verità, come segue.

p_1	p_2	$\dots$	p_n	$f(p_1, \dots, p_n)$
0	$\dots$	$\dots$	$\dots$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
0	$\dots$	$\dots$	$\dots$	$\dots$
1	$\dots$	$\dots$	$\dots$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
1	$\dots$	$\dots$	$\dots$	$\dots$

La parte superiore della tabella, senza considerare la prima colonna, definisce una funzione f_0 di $n-1$ argomenti, il cui comportamento è definito dalle prime 2^{n-1} righe. La parte inferiore della tabella, senza considerare la prima colonna, definisce una funzione f_1 di $n-1$ argomenti, il cui comportamento è definito dalle ultime 2^{n-1} righe.

Per ipotesi induttiva sulle funzioni f_0 e f_1, esistono formule B_0 e B_1 con $n-1$ variabili proposizionali (siano senza pregiudizio di generalità $p_2, \dots, p_n$) e contenenti soltanto i connettivi $\wedge, \vee, \neg$ tali che, per ogni assegnamento v,

$$v(B_0) = f_0(v(p_2), \dots, v(p_n)),$$

e

$$v(B_1) = f_1(v(p_2), \dots, v(p_n)).$$

Sia A la formula seguente

$$((p_1 \vee B_0) \wedge ((\neg p_1) \vee B_1)).$$

Dimostriamo che A soddisfa la tesi del teorema rispetto alla funzione f. Sia v un assegnamento qualunque. Dimostriamo che

$$v(A) = f(v(p_1), v(p_2), \dots, v(p_n)).$$

Distinguamo due casi.

Se $v(p_1) = 1$, allora $v(p_1 \vee B_0) = 1$ e vale

$$v(((p_1 \vee B_0) \wedge ((\neg p_1) \vee B_1))) = 1 \text{ se e solo se } v(((\neg p_1) \vee B_1)) = 1.$$

Inoltre, $v((\neg p_1)) = 0$, e dunque

$$v((\neg p_1 \vee B_1)) = 1 \text{ se e solo se } v(B_1) = 1.$$

Ma per quanto visto circa B_1, vale

$$v(B_1) = f_1(v(p_2, \dots, v(p_n))),$$

e in questo caso – dato che $v(p_1) = 1$ – vale

$$f(v(p_1), v(p_2), \dots, v(p_n)) = f(1, v(p_2), \dots, v(p_n)) = f_1(v(p_2), \dots, v(p_n)).$$

Dunque in questo caso

$$v(A) = f(v(p_1), v(p_2), \dots, v(p_n)).$$

Se $v(p_1) = 0$, allora $v((\neg p_1)) = 1$ e dunque $v(((\neg p_1) \vee B_1))) = 1$. Allora

$$v(((p_1 \vee B_0) \wedge ((\neg p_1) \vee B_1))) = 1 \text{ se e solo se } v((p_1 \vee B_0)) = 1.$$

Inoltre, dato che $v(p_1) = 0$,

$$v((p_1 \vee B_0)) = 1 \text{ se e solo se } v(B_0) = 1.$$

Ma per quanto visto circa B_0, vale

$$v(B_0) = f_0(v(p_2, \dots, v(p_n))),$$

e in questo caso – dato che $v(p_1) = 0$ – vale

$$f(v(p_1), v(p_2), \dots, v(p_n)) = f(0, v(p_2), \dots, v(p_n)) = f_0(v(p_2), \dots, v(p_n)).$$

Dunque in questo caso

$$v(A) = f(v(p_1), v(p_2), \ldots, v(p_n)).$$

□

10. Forme Normali

Chiamiamo "letterale" una variabile proposizionale o una negazione di una variabile proposizionale. Diciamo che A è in Forma Normale Congiuntiva (CNF) se A è di forma è una congiunzione di disgiunzioni di letterali, ossia è della forma seguente, dove gli $A_{i,j}$ sono letterali.

$$(A_{1,1} \vee A_{1,2} \vee \cdots \vee A_{1,m_1}) \wedge (A_{2,1} \vee A_{2,2} \vee \cdots \vee A_{2,m_2}) \cdots \wedge (A_{n,1} \vee A_{n,2} \vee \cdots \vee A_{n,m_n})$$

Diciamo che A è in Forma Normale Disgiuntiva (DNF) se A è una disgiunzione di congiunzioni di letterali, ossia è della forma seguente, dove gli $A_{i,j}$ sono letterali.

$$(A_{1,1} \wedge A_{1,2} \wedge \cdots \wedge A_{1,m_1}) \vee (A_{2,1} \wedge A_{2,2} \wedge \cdots \wedge A_{2,m_2}) \cdots \vee (A_{n,1} \wedge A_{n,2} \wedge \cdots \wedge A_{n,m_n}).$$

Usiamo $\bigwedge_{i \leq n} A_i$ come abbreviazione di

$$A_1 \wedge A_2 \wedge \cdots \wedge A_n.$$

e analogamente $\bigvee_{i \leq n} A_i$ come abbreviazione di

$$A_1 \vee A_2 \vee \cdots \vee A_n.$$

Conquesta notazione, A è una CNF se è della forma

$$\bigwedge_{i \leq n} \bigvee_{j \leq m_i} A_{i,j},$$

ed è in DNF se è della forma

$$\bigvee_{i \leq n} \bigwedge_{j \leq m_i} A_{i,j},$$

dove gli $A_{i,j}$ sono letterali.

Diamo due dimostrazioni (una induttiva l'altra più intuitiva) del seguente Teorema di Forma Normale.

Teorema 10.1 (Forme Normali Congiuntive e Disgiuntive)**.** *Per ogni A esiste A^{CNF} e A^{DNF} tali che A^{CNF} è una CNF, A^{DNF} è una DNF, e*

$$\models A \leftrightarrow A^{\mathrm{CNF}},$$

$$\models A \leftrightarrow A^{\mathrm{DNF}},$$

Dimostrazione n.1. Assumiamo che A sia scritta nel linguaggio ristretto ai connettivi $\{\vee, \wedge, \neg\}$. Dimostriamo il Teorema per induzione su A.

Se A è atomica, è ovvio.

Se A è $(B \wedge C)$, allora scegliamo $(B^{\mathrm{CNF}} \wedge C^{\mathrm{CNF}})$ come A^{CNF}. Sia $B^{\mathrm{DNF}} = \bigvee B_i$, e $C^{\mathrm{DNF}} = \bigvee C_j$. Allora

$$A = B \wedge C \equiv \bigvee B_i \wedge \bigvee C_j \equiv \bigvee_{i,j} (B_i \wedge C_j).$$

Poniamo A^{DNF} uguale a $\bigvee_{i,j} (B_i \wedge C_j)$.

Se A è $(B \vee C)$, il ragionamento è duale.

Se A è $(\neg B)$. Sia $B^{\mathrm{DNF}} = \bigvee \bigwedge B_{i,j}$. Allora

$$\neg B \equiv \neg B^{\mathrm{DNF}} \equiv \neg \bigvee \bigwedge B_{i,j} \equiv \bigwedge \bigvee \neg B_{i,j}.$$

Poniamo A^{CNF} uguale a $\bigwedge \bigvee \neg B'_{i,j}$, dove $B'_{i,j}$ è $B_{i,j}$ se $B_{i,j}$ è una variabile negata ed è $\neg B_{i,j}$ altrimenti.

A^{DNF} si definisce in maniera duale partendo da B^{CNF}. □

Dimostrazione n.2. Scriviamo la tavola di verità di A

p_1	p_2	$\dots$	p_n	A
0	$\dots$	$\dots$	$\dots$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
0	$\dots$	$\dots$	$\dots$	$\dots$
1	$\dots$	$\dots$	$\dots$	$\dots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
1	$\dots$	$\dots$	$\dots$	$\dots$

La tavola ha 2^n righe. Per ogni $1 \leq i \leq n$, la riga i determina un assegnamento di valori di verità a $p_1, \dots, p_n, A$, che chiamiamo v_i. La riga i-esima dice che se p_1 ha valore $v_i(p_1)$, e p_2 ha valore $v_i(p_2)$, ..., e p_n ha valore $v_i(p_n)$ allora A ha il valore $v_i(A)$. I casi in cui A è vera sono completamente descritti dalle righe i in cui $v_i(A) = 1$. In altre parole, A è vera se e solo se le variabili proposizionali $p_1, \dots, p_n$ assumono i valori $v_i(p_1), \dots, v_i(p_n)$ per una qualche riga i tale che $v_i(A)$. Dunque, per ogni assegnamento v, $v(A) = 1$ se e solo se v coincide con v_i su $p_1, \dots, p_n$ dove i è una riga in cui A è vera.

Usiamo i letterali per rappresentare all'interno del linguaggio i due casi $v_i(p_{i,j}) = 1$ e $v_i(p_{i,j}) = 0$, per $i \in \{1, \dots, 2^n\}$ e $j \in \{1, \dots, n\}$. Definiamo $p'_{i,j} = p_{i,j}$ se $v_i(p_{i,j}) = 1$ e $p'_{i,j} = \neg p_{i,j}$ se $v_i(p_{i,j}) = 0$. Consideriamo ora l'insieme $I_1 \subseteq \{1, \dots, 2^n\}$ delle righe in cui A ha valore 1. Per $i \in I_1$, alla riga i-esima associamo la congiunzione

$$p'_{i,1} \wedge \dots \wedge p'_{i,n}.$$

Questa congiunzione rappresenta l'assegnamento v_i, nel senso che, per ogni assegnamento v,

$$v(p'_{i,1} \wedge \dots \wedge p'_{i,n}) = 1 \Rightarrow v(A) = 1.$$

Infatti vale che

$$v(p'_{i,1} \wedge \dots \wedge p'_{i,n}) = 1 \Rightarrow v(p'_{i,1}) = v_i(p_{i,1}), \dots, v(p'_{i,n}) = v_i(p_{i,n}).$$

Dato che per ogni v vale $v(A) = 1$ se e solo se per qualche $i \in I_1$, v coincide con v_i sulle variabili $p_1, \dots, p_n$ di A, abbiamo che l'intera tavola di verità di A è rappresentata dalla DNF

$$\bigvee_{i \in I_1} \bigwedge_{j \in \{1,\dots,n\}} p'_{i,j}.$$

Per Esercizio, sviluppare i dettagli di un argomento analogo per ottenere una CNF equivalente a A. □

Proposizione 10.2. *Una CNF è una tautologia se e soltanto se tutti i suoi congiunti sono tautologie.*

Proposizione 10.3. *Una DNF è insoddisfacibile se e soltanto se tutti i suoi disgiunti sono insoddisfacibili.*

Potremmo allora pensare di affrontare il problema di decidere se $A \in$ Taut (o equivalentemente $\neg A \in$ UnSat) scrivendola in CNF e decidendo se i congiunti sono in Taut o scrivendola in DNF e decidendo se i disgiunti sono in UnSat. Purtroppo questo metodo non dà luogo a un algoritmo efficiente (vedi *infra* per un esempio).

11. Altre manipolazioni algebriche

Illustriamo un altro metodo per manipolare le verità logiche basato sulle leggi di distributività. Si procede come segue, data una proposizione A.

(1) Si eliminano i connettivi $\to$ e $\leftrightarrow$, utilizzando le equivalenze $A \to B \equiv \neg A \vee B$ e $A \leftrightarrow B \equiv (A \to B) \wedge (B \to A)$.
(2) Si spingono le negazioni all'interno, utilizzando le equivalenze $\neg(A \wedge B) \equiv (\neg A \vee \neg B)$ e $\neg(A \vee B) \equiv (\neg A \wedge \neg B)$.
(3) Si sostituisce $\wedge$ con $+$ e $\vee$ con $\cdot$ (o viceversa!)
(4) Si sviluppa usando la legge di distributività.
(5) Se abbiamo sostituito $\wedge$ con $+$ e $\vee$ con $\cdot$ allora sostituiamo le occorrenze di tipo $p + (\neg p)$ con 0 e quelle di tipo $p \cdot (\neg p)$ con 1 (se abbiamo sostituito $\wedge$ con $\cdot$ e $\vee$ con $+$, facciamo il viceversa).
(6) Si sostituisce $+$ con $\wedge$ e $\cdot$ con $\vee$ (o viceversa, a seconda della scelta fatta sopra!).

Questo metodo permette di trasformare una proposizione preservando l'equivalenza logica. In particolare permette di ottenere verità logiche (formule valide) da altre verità logiche. Inoltre, permette di ottenere forme normali CNF o DNF.

Esempio 11.1.

$$(A \to B) \to (\neg B \to \neg A)$$
$$\neg(A \to B) \vee (\neg B \to \neg A)$$
$$\neg(\neg A \vee B) \vee (\neg\neg B \vee \neg A)$$
$$(A \wedge \neg B) \vee (B \vee \neg A)$$
$$(A + \bar{B}) \cdot (B \cdot \bar{A})$$
$$(AB\bar{A}) + (\bar{B}B\bar{A})$$
$$(A \vee B \vee \neg A) \wedge (\neg B \vee B \vee \neg A)$$

In questo modo abbiamo ottenuto una CNF equivalente alla proposizione iniziale. Alternativamente, possiamo continuare la valutazione dalla penultima riga come segue.

$$(AB\bar{A}) + (\bar{B}B\bar{A})$$
$$B1 + \bar{A}1$$
$$(B \vee 1) \wedge (\bar{A} \vee 1)$$
$$1$$

Così abbiamo dimostrato che la proposizione iniziale è una verità logica.

Esempio 11.2. Vogliamo verificare la seguente relazione di conseguenza logica

$$(A \to B), (C \vee \neg B), \neg(A \wedge C) \models \neg A$$

Abbiamo due strade.

(1) Verifichiamo che
$$(((A \to B), (C \vee \neg B), \neg(A \wedge C)) \to \neg A) \in \textsc{Taut}$$
(2) Verifichiamo che
$$(((A \to B), (C \vee \neg B), \neg(A \wedge C)) \wedge A) \in \textsc{UnSat}$$

Nel primo caso, trasformiamo in CNF e verifichiamo che ogni congiunto è una tautologia. Nel secondo caso, trasformiamo in DNF e verifichiamo che ogni disgiunto è insoddisfacibile. Sviluppiamo entrambi gli esempi e osserviamo che danno luogo a procedimenti di stessa lunghezza.

Cominciamo con (1), verificando che

$$(((A \to B), (C \vee \neg B), \neg(A \wedge C)) \to \neg A) \in \textsc{Taut}$$

Per farlo, trasformiamo in CNF e verifichiamo che ogni congiunto è una tautologia.

$$\neg((A \to B) \wedge (C \vee \neg B) \wedge \neg(A \wedge C)) \vee \neg A$$
$$\neg((A \to B) \vee \neg(C \vee \neg B) \vee \neg\neg(A \wedge C)) \vee \neg A$$
$$(\neg(\neg A \vee B) \vee (\neg C \wedge \neg\neg B) \vee (A \wedge C)) \vee \neg A$$
$$((A \wedge \neg B) \vee (\neg C \wedge B) \vee (A \wedge C)) \vee \neg A$$

Osserviamo che la formula appena scritta è in DNF, ma non è questa la forma normale che ci serve! Sostituiamo $\wedge$ con $+$ e $\vee$ con $\cdot$

$$((A + \bar{B}) \cdot (\bar{C} + B) \cdot (A + C)) \cdot \bar{A}$$
$$(((A + \bar{B}) \cdot (\bar{C} + B)) \cdot (A + C)) \cdot \bar{A}$$
$$(((A + \bar{B}) \cdot \bar{C} + (A + \bar{B}) \cdot B) \cdot (A + C)) \cdot \bar{A}$$
$$(((A\bar{C} + \bar{B}\bar{C}) + (AB + \bar{B}B)) \cdot (A + C)) \cdot \bar{A}$$
$$((A\bar{C} + \bar{B}\bar{C}) \cdot (A + C) + (AB + \bar{B}B) \cdot (A + C)) \cdot \bar{A}$$
$$(((A\bar{C} \cdot (A + C) + \bar{B}\bar{C} \cdot (A + C)) + (AB \cdot (A + C) + \bar{B}B \cdot (A + C))) \cdot \bar{A}$$
$$(A\bar{C}A + A\bar{C}C + \bar{B}\bar{C}A + \bar{B}\bar{C}C + ABA + ABC + \bar{B}BA + \bar{B}BC) \cdot \bar{A}$$
$$A\bar{C}A\bar{A} + A\bar{C}C\bar{A} + \bar{B}\bar{C}A\bar{A} + \bar{B}\bar{C}C\bar{A} + ABA\bar{A} + ABC\bar{A} + \bar{B}BA\bar{A} + \bar{B}BC\bar{A}$$

Sostituendo $+$ con $\wedge$ e $\cdot$ con $\vee$ otteniamo la seguente proposizione

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

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

La proposizione è in CNF e tutti i congiunti sono tautologie. Dunque la relazione di conseguenza logica iniziale è verificata.

Procediamo ora con (2), verificando che

$$(((A \to B), (C \vee \neg B), \neg(A \wedge C)) \wedge A) \in \textsc{UnSat}$$

Per farlo, trasformiamo in DNF e verifichiamo che ogni disgiunto è insoddisfacibile.

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

Osserviamo che la formula appena scritta è in CNF, ma non è questa la forma normale che ci serve! Sostituiamo $\wedge$ con $\cdot$ e $\vee$ con $+$ e otteniamo

$$(\bar{A} + B) \cdot (C + \bar{B}) \cdot (\bar{A} + \bar{C}) \cdot A$$

Osserviamo che l'espressione appena ottenuta è duale a quella ottenuta nell'approccio precedente dopo la sostituzione, se invertiamo $\cdot$ e $+$ e sostituiamo ogni lettera X con la sua negata $\bar{X}$. Procedendo nello sviluppo usando la legge di distributività, otterremo una forma DNF con lo stesso numero di clausole della CNF ottenuta sopra.

12. Principio di Dualità tra $\wedge$ e $\vee$

Se osserviamo le leggi logiche notevoli osserviamo una dualità tra $\vee$ e $\wedge$. In questo paragrafo dimostriamo rigorosamente che vale il seguente.

> **Principio di Dualità** Ogni enunciato corretto che riguarda i connettivi $\wedge$, $\vee$, e le costanti 0 e 1 si traduce in un enunciato duale corretto invertendo $\wedge$ con $\vee$, 0 con 1.

Naturalmente l'applicazione corretta del Principio prevede che le nozioni che riguardano la verità siano sostituite con le loro duali, per esempio "tautologia" con "insoddisfacibile", etc. Così, per esempio, il duale di "$A \vee \neg A \in \textsc{Taut}$" è "$A \wedge \neg A \in \textsc{UnSat}$", e il duale di "Se $A \vee B \notin \textsc{Taut}$ allora $A \notin \textsc{Taut}$" è "Se $A \wedge B \notin \textsc{UnSat}$ allora $A \notin \textsc{UnSat}$". Per dirla con Martin Davis,

> Un essere di un altro pianeta che ci osservasse fare logica proposizionale sarebbe in grado di capire che stiamo facendo logica proposizionale. Ma questo essere non avrebbe modo di capire quale valore di verità stiamo rappresentando con 0 e quale con 1, e di conseguenza non sarebbe in grado di dire quale dei due connettivi rappresenti "e" e quale "o".

Dimostriamo il Principio di Dualità definendo una mappa d da proposizioni in proposizioni che scambia $\wedge$ con $\vee$ e dimostrando che la mappa preserva l'equivalenza logica. Facciamo un passo intermedio definendo una mappa $*$ da proposizioni in proposizioni che scambia $\wedge$ con $\vee$ e ogni variabile proposizionale con la sua negazione.

Definizione 12.1. Definiamo una mappa * da proposizioni in proposizioni.

$$A^* = \neg A \text{ se } A \text{ è una variabile.}$$

$$(B \wedge C)^* = (B^* \vee C^*)$$

$$(B \vee C)^* = (B^* \wedge C^*)$$

$$(\neg B)^* = \neg B^*$$

Lemma 12.2. *Per ogni assegnamento v,*

$$v(A^*) = v(\neg A).$$

Dimostrazione. Esercizio (induzione). □

Definizione 12.3. Definiamo una mappa ^{d} da proposizioni in proposizioni.

$$A^d = A \text{ se } A \text{ è una variabile.}$$
$$(B \wedge C)^d = (B^d \vee C^d)$$
$$(B \vee C)^d = (B^d \wedge C^d)$$
$$(\neg B)^d = \neg B^d$$

Teorema 12.4. *$A \equiv B$ se e solo se $A^d \equiv B^d$.*

Dimostrazione. Supponiamo $A \equiv B$ e dimostriamo $A^d \equiv B^d$. Osserviamo che

$$A^* = A^d[p_1/\neg p_1, \ldots, p_n/\neg p_n].$$

Allora

$$A^*[p_1/\neg p_1, \ldots, p_n/\neg p_n] = A^d[p_1/\neg\neg p_1, \ldots, p_n/\neg\neg p_n].$$

Dato che $\neg\neg p_i \equiv p_i$, abbiamo che

$$A^*[p_1/\neg p_1, \ldots, p_n/\neg p_n] \equiv A^d,$$

per il Teorema di Sostituzione di equivalenti. Con lo stesso ragionamento, per B, abbiamo che

$$B^*[p_1/\neg p_1, \ldots, p_n/\neg p_n] \equiv B^d,$$

Dal Lemma precedente abbiamo che

$$\neg A \equiv A^*$$

e

$$\neg B \equiv B^*$$

Da $A \equiv B$ (ipotesi) segue $\neg A \equiv \neg B$ e dunque $A^* \equiv B^*$, e dunque anche

$$A^*[p_1/\neg p_1, \ldots, p_n/\neg p_n] \equiv B^*[p_1/\neg p_1, \ldots, p_n/\neg p_n] \equiv B^d,$$

per il Teorema di Sostituzione in equivalenti. Per quanto visto sopra, segue

$$A^d \equiv B^d.$$

L'altra direzione dell'implicazione (se $A^d \equiv B^d$ allora $A \equiv B$) è lasciata per Esercizio. □

13. Altri esercizi assegnati in classe

Esercizio 13.1. Dimostrare il Principio di Definizione per Ricorsione. *Suggerimento*: insiemisticamente la funzione $F : \text{PROP} \to X$ definita per ricorsione da f, g, h è un insieme di coppie ordinate (A, x) con $A \in \text{PROP}$ e $x \in X$. Definire questo insieme di coppie induttivamente. Dimostrare che costituisce una funzione con dominio PROP e dimostrare che è l'unica funzione su PROP che soddisfa le equazioni ricorsive date. Usare una forma adeguata di induzione sulla funzione F definita insiemisticamente.

Esercizio 13.2. Indichiamo con $T(A)$ il parsing-tree associato alla proposizione A.

(1) Sia c_A il numero dei connettivi di A e v_A il numero delle variabili di A. Sia $n_{T(A)}$ il numero dei nodi dell'albero $T(A)$. Allora
$$c_A + v_A \leq n_{T(A)}.$$
(2) Sia s_A il numero di sottoformule di A. Allora
$$s_A \leq n_{T(A)}.$$
(3) La lunghezza di un ramo in un albero è definita come il numero di nodi presenti nel ramo meno 1. Allora
$$r(A) = \text{ lunghezza massima di un ramo in } T(A).$$
(4) $c_A + v_A \leq 2^{r(A)+1} - 1$.

Esercizio 13.3. Se A contiene n connettivi, allora ha contiene $\leq 2n + 1$ sottoformule.

Esercizio 13.4. Definire per ricorsione una funzione $S : \text{PROP} \to \mathcal{P}(PROP)$ tale che $S(A) = \{B : B \text{ è sottoformula di } A\}$.

Esercizio 13.5. Dimostrare che

(1) $v(A \wedge B) = v(A) \cdot v(B)$,
(2) $v(A \vee B) = v(A) + v(B) - v(A) \cdot v(B)$,
(3) $v(A \to B) = 1 - v(A) + v(A) \cdot v(B)$,
(4) $v(A \leftrightarrow B) = 1 - |v(A) - v(B)|$.

Esercizio 13.6. Dimostrare che se $\models (A \to B)$ allora $\models (A \wedge B) \leftrightarrow A$ e $\models (A \vee B) \leftrightarrow B$.