



CAM

di Camerino

36

MATEMATICA LOGICA

Docente

Sonia L'Innocente

Studente

Giorgio Della Roscia

Università degli studi di Camerino

Informatica per la Comunicazione Digitale (L-31)

SCUOLA DI SCIENZE E TECNOLOGIE

A.A. 2022/2023

Indice

1	ALGEBRA	1
1.1	Insiemi	1
1.1.1	Cardinalità	1
1.1.1.1	Insieme numerabile	1
1.1.2	Insiemi di numeri	2
1.1.3	Relazioni	2
1.1.3.1	Inclusione	2
1.1.3.1.1	Negazione	2
1.1.3.2	Unione	3
1.1.3.2.1	Proprietà dell'unione	3
1.1.3.3	Intersezione	3
1.1.3.3.1	Proprietà dell'intersezione	3
1.1.3.4	Differenza	3
1.1.3.5	Disgiunzione	4
1.1.3.6	Insieme complementare	4
1.1.3.7	Insieme delle parti	4
1.1.3.8	Partizione di un insieme	4
1.1.4	Prodotto cartesiano	4
1.1.4.1	Sottoinsiemi di prodotti cartesiani	5
1.2	Funzioni	5
1.2.1	Funzione identità	5
1.2.2	Iniettività	5
1.2.3	Suriettività	6
1.2.4	Biiettività	6
1.2.5	Operazioni tra funzioni	6
1.3	Relazioni d'equivalenza	7
1.3.1	Divisibilità	8
1.3.2	Congruenza	8
1.3.3	Classe di equivalenza	8
1.3.3.1	Insieme quoziente	8
1.3.4	Relazioni antisimmetriche	8
1.3.4.1	Massimi e minimi	9
1.3.4.1.1	Minimali e massimali	9
2	LOGICA	11
2.1	Logica proposizionale	11
2.1.1	Formule	12
2.1.2	Preposizione di alfabeti	12
2.1.2.1	Lunghezza di una preposizione	12
2.1.2.2	Altezza di una preposizione	13
2.1.2.3	Analisi sintattica	13
2.1.2.3.1	Albero sintattico	14
2.1.2.3.2	Albero binario	14
2.1.3	Semantica	14
2.2	Formule CNF e DNF	15
2.3	Deduzione naturale	15

2.3.1	Deduzione naturale con operatore $\wedge$	16
2.3.2	Deduzione naturale con operatore $\neg$	16
2.3.3	Deduzione naturale con operatore $\Rightarrow$	16
2.3.4	Deduzione naturale con operatore $\vee$	16
2.4	Predicati del primo ordine	16
2.4.1	Formalizzazione	17

Figure

1.1	Diagrammi di Eulero-Venn	1
1.2	Diagramma di Venn per l'unione	3
1.3	Diagramma di Venn per l'intersezione	3
1.4	Diagramma di Venn per la differenza	3
1.5	Modello f iniettiva	5
1.6	Modello f suriettiva	6
1.7	Modello f biiettiva	6

Tabelle

2.1	Tavole di verità dei connettivi logici	11
2.2	Legge contronominale	11

Approfondimenti

Definizione (insieme)	1
Definizione (cardinalità)	1
Definizione (insieme numerabile)	1
Definizione (insieme più che numerabile)	1
Definizione (sottoinsieme)	2
Definizione (sottoinsieme proprio)	2
Esempio (insieme delle parti)	4
Definizione (partizione di un insieme)	4
Definizione (prodotto cartesiano)	4
Esercizio (prodotto cartesiano)	4
Definizione (relazione)	5
Definizione (applicazione)	5
Definizione (funzione iniettiva)	5
Definizione (funzione suriettiva)	6
Definizione (funzione biiettiva)	6
Definizione (composizione)	6
Definizione (funzione inversa)	7
Esercizio (relazione d'equivalenza)	7
Definizione (congruenza)	8
Definizione (classe di equivalenza)	8
Definizione (insieme quoziente)	8
Definizione (relazione antisimmetrica)	8
Definizione (relazione di ordine parziale)	8
Definizione (relazione di ordine totale)	8
Definizione (minimo elemento)	9
Definizione (massimo elemento)	9
Definizione (elemento minimale)	9
Esempio (minimale)	9
Definizione (elemento massimale)	9
Teorema (leggi di De Morgan)	11
Definizione (formula soddisfacibile)	12
Definizione (tautologia)	12
Definizione (formula non soddisfacibile)	12
Definizione (contraddizione)	12
Esempio (lunghezza di una proposizione)	12
Esercizio (altezza di una preposizione)	13
Esempio (analisi sintattica)	13
Esempio (insieme soddisfacibile)	14
Definizione (formula CNF)	15
Definizione (formula DNF)	15
Esempio (formule CNF e DNF)	15
Esercizio (formalizzazione numero primo)	17

Sezione 1

ALGEBRA

In questa prima parte si fermano alcuni preconcetti matematici per poi ampliare sul ramo algebrico.

1.1 Insiemi

Definizione (insieme). Arbitraria collezione di elementi.

Vengono indicati con lettere maiuscole dell'alfabeto latino, mentre gli oggetti che sono contenuti in essi con quelle minuscole. Per rappresentare un insieme esistono diverse possibilità:

1. lineare $A = \{a, b, c, d\}$
2. utilizzo di una proprietà $A = \{a : a \in \mathbb{R}\}$
3. diagrammi di Venn

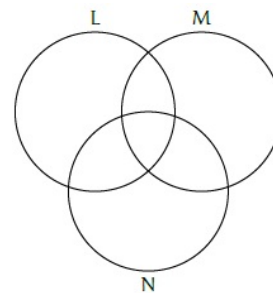


Figura 1.1: Diagrammi di Eulero-Venn

1.1.1 Cardinalità

Definizione (cardinalità). Dato un insieme finito A , si dice cardinalità $|A|$ il numero dei suoi elementi.

1.1.1.1 Insieme numerabile

Definizione (insieme numerabile). Dato un insieme A , esso viene detto numerabile se, e solo se, è equipotente ad $\mathbb{N}$: $A \approx \mathbb{N}$. Sapendo che $|\mathbb{N}| = \aleph_0$.

Definizione (insieme più che numerabile). Dato un insieme B , esso viene detto più che numerabile se, e solo se, è equipotente a $\mathbb{R}$: $B \approx \mathbb{R}$. Sapendo che $|\mathbb{R}| = 2^{\aleph_0}$.

1.1.2 Insiemi di numeri

Esistono infiniti insiemi contenenti numeri, ma alcuni si caratterizzano maggiormente rispetto agli altri.

- **Naturali** – comprendono i numeri maggiori e uguali a zero senza virgole:

$$\mathbb{N} = [0, 1, 2, 3, 4, \dots, +\infty)$$

- **Interi** – comprendono i naturali ed i loro negati:

$$\mathbb{Z} = (-\infty, \dots, -2, -1, 0, 1, 2, \dots, +\infty)$$

- **Razionali** – comprendono gli interi e le altre combinazioni ottenibili tramite frazioni:

$$\mathbb{Q} = \left(-\infty, \dots, -\frac{55}{55}, \frac{1}{10}, \frac{11}{53}, \frac{2}{3}, \frac{3}{2}, \dots, +\infty\right)$$

- **Reali** – comprendono i razionali ed anche quei numeri non ottenibili con frazioni:

$$\mathbb{R} = \left(-\infty, \dots, -\sqrt{2}, \frac{1}{3}, 2, \frac{5}{2}, \dots, +\infty\right)$$

- **Complessi** – aggiungono ai reali una seconda parte, immaginaria:

$$\mathbb{C} = \left(-\infty, \dots, (3, 4i), (22, i), \left(-7, -\frac{2}{4}i\right), \dots, +\infty\right)$$

1.1.3 Relazioni

Fra gli insiemi si formano vari rapporti.

1.1.3.1 Inclusione

Qualora un insieme A sia totalmente racchiuso in un secondo insieme B si avrà un'inclusione.

Definizione (sottoinsieme). Dati due insiemi A e B , si dice che il primo è sottoinsieme del secondo se ogni elemento di A lo è anche di B .

$$A \subset B$$

Si deduce che potrebbero essere anche uguali: $A \subseteq B$.

Definizione (sottoinsieme proprio). Presi i due insiemi precedenti, un sottoinsieme è dichiarato proprio se esiste almeno un elemento di B che non appartiene anche ad A .

$$A \subsetneq B$$

Ciò indica che A e B sono obbligatoriamente diversi.

1.1.3.1.1 Negazione

Se, d'altro canto, nessun elemento di A è contenuto in B si ha la seguente relazione: $A \not\subseteq B$.

1.1.3.2 Unione

Dati i due insiemi A e B si ha la loro unione prendendo tutti gli elementi che li compongono: $A \cup B$.

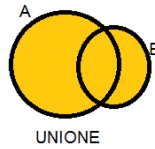


Figura 1.2: Diagramma di Venn per l'unione

1.1.3.2.1 Proprietà dell'unione

Dati i tre insiemi A , B e C , vigono le seguenti proprietà:

$$\begin{array}{ll} \text{commutativa} & \rightarrow A \cup B = B \cup A \\ \text{associativa} & \rightarrow A \cup (B \cup C) = (A \cup B) \cup C \\ \text{secondarie} & \rightarrow A \cup A = A \quad A \cup A' = S \end{array}$$

1.1.3.3 Intersezione

Dati gli insiemi A e B si ha la loro intersezione prendendo gli elementi presenti in entrambi: $A \cap B$.

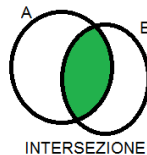


Figura 1.3: Diagramma di Venn per l'intersezione

1.1.3.3.1 Proprietà dell'intersezione

Dati i tre insiemi A , B e C , vigono le seguenti proprietà:

$$\begin{array}{ll} \text{commutativa} & \rightarrow A \cap B = B \cap A \\ \text{associativa} & \rightarrow A \cap (B \cap C) = (A \cap B) \cap C \\ \text{secondarie} & \rightarrow A \cap A = A \quad A \cap \{\emptyset\} = \emptyset \quad A \cap A' = \{\emptyset\} \end{array}$$

1.1.3.4 Differenza

Dati i due insiemi A e B si ha la loro differenza, ad esempio quella di A rispetto a B , prendendo tutti gli elementi che compongono A sottratti quelli che appartengono anche a B : $A - B$.

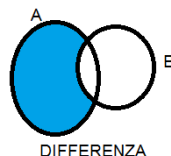


Figura 1.4: Diagramma di Venn per la differenza

1.1.3.5 Disgiunzione

Dati i due insiemi A e B si ha la loro disgiunzione se $A \cap B = \emptyset$. Dunque nessun elemento di uno lo è al contempo dell'altro. Il connettivo relativo alla disgiunzione è indicato con il seguente simbolo: $\vee$. Ciò equivale ad un **or** logico.

1.1.3.6 Insieme complementare

Dato un insieme A si ha il suo complementare prendendo quell'insieme che racchiude l'intero insieme universo S meno i componenti appartenenti ad A .

$$A' = \{x \in S : x \notin A\} = S - A$$

1.1.3.7 Insieme delle parti

Dato un insieme A si definisce insieme delle sue parti, e si indica con $\wp(A)$, quello formato da tutti i sottoinsiemi di sé stesso.

Esempio (insieme delle parti). Si ha l'insieme A e il rispettivo insieme delle parti $\wp(A)$.

$$A = \{0, 1\} \quad \wp(A) = \{\{\emptyset\}, \{0\}, \{1\}, \{0, 1\}\}$$

1.1.3.8 Partizione di un insieme

Definizione (partizione di un insieme). Dato un insieme A si ha un secondo insieme P con elementi pari a sottoinsiemi di A con tali caratteristiche:

- non vuoti;
- disgiunti;
- $\bigcup \equiv A$.

$$P = \{A_i : A_i \subseteq A \quad i \in I\}$$

$$A_i \neq \emptyset \quad A_i \cap A_j = \emptyset, i \neq j \quad \bigcup_{i \in I} A_i = A$$

Riguarda una collezione di sottoinsiemi non vuoti, disgiunti fra loro e la cui unione garantisce l'insieme padre.

1.1.4 Prodotto cartesiano

Definizione (prodotto cartesiano). Dati due insiemi A e B si dice prodotto cartesiano tra loro, $A \times B$, il seguente insieme: $A \times B = \{(a, b) : a \in A, b \in B\}$

Occorre notare però che:

- l'ordine è importante $(a, b) \neq (b, a)$;
- due coppie $(a, b), (a', b')$ sono uguali se $a = a'$ e $b = b'$.

Esercizio (prodotto cartesiano). Dati i due insiemi A e B calcolare i due prodotti cartesiani.

$$A = \{1, 2\} \quad B = \{3, 4\}$$

$$\dots\dots\dots A \times B = \{(1, 3), (1, 4), (2, 3), (2, 4)\} \quad B \times A = \{(3, 1), (3, 2), (4, 1), (4, 2)\}$$

1.1.4.1 Sottoinsiemi di prodotti cartesiani

Definizione (relazione). Siano A e B due insiemi, si definisce relazione tra loro un qualunque sottoinsieme del prodotto cartesiano $A \times B$.

$$R \subseteq A \times B$$

1.2 Funzioni

Definizione (applicazione). Siano A e B due insiemi, si definisce applicazione di A in B una relazione $f (\subseteq A \times B)$ tale che:

$$\forall a \in A \exists ! b \in B : \begin{cases} (a, b) \in f \\ a f b \\ f(a) = b \end{cases}$$

Data $f \in \mathbb{R} : A \rightarrow B$ si ha l'insieme A riguardo il dominio, mentre B il codominio: $\mathfrak{I}(f)$.

1.2.1 Funzione identità

Si ha un'applicazione che restituisce esattamente i dati in entrata:

$$id_A : A \rightarrow A \quad \forall a \in A, id_A(a) = a$$

1.2.2 Iniettività

Definizione (funzione iniettiva). Dati i due insiemi A e B , la funzione $f : A \rightarrow B$ si dice iniettiva se, e solo se:

$$\forall a_1, a_2 \in A, \text{ se } a_1 \neq a_2 \implies f(a_1) \neq f(a_2)$$

Non possono esistere due punti con la stessa immagine ma potrebbe accadere che alcuni elementi non ce l'abbiano affatto.

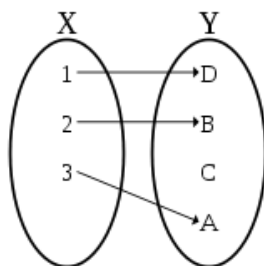


Figura 1.5: Modello f iniettiva

1.2.3 Suriettività

Definizione (funzione suriettiva). Dati gli insiemi A e B , la funzione $f : A \rightarrow B$ si dice suriettiva se, e solo se:

$$\mathfrak{I}(f) = B, \forall b \in B \exists a \in A : b = f(a)$$

Potrebbero esistere elementi con la medesima immagine.

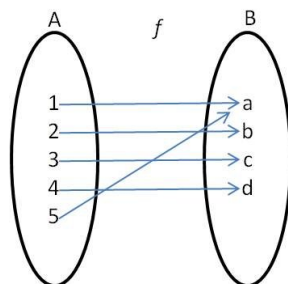


Figura 1.6: Modello f suriettiva

1.2.4 Biiettività

Definizione (funzione biiettiva). Dati i due insiemi A e B , la funzione $f : A \rightarrow B$ si dice biiettiva se, e solo se:

$$\forall b \in B \exists ! a \in A$$

Ogni elemento ha una, e una sola, immagine.

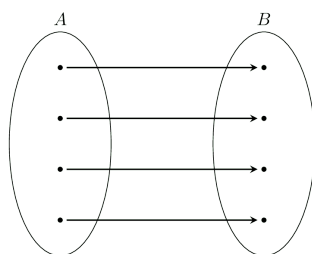


Figura 1.7: Modello f biiettiva

1.2.5 Operazioni tra funzioni

Definizione (composizione). Presi tre insiemi A , B , C tali che

$$f : A \rightarrow B, \quad g : B \rightarrow C$$

si definisce composizione di f con g , $f \circ g$, l'operazione definita nel seguente modo:

$$\forall a \in A, g \circ f(a) = g(f(a))$$

Chiaramente $\mathfrak{I}(f \circ g)$ deve coincidere con $\mathfrak{I}(g)$.

Definizione (funzione inversa). Siano A e B due insiemi ed R una relazione fra loro, si definisce relazione inversa, R^{-1} , rispetto ad R la dicitura:

$$(b, a) \in R^{-1} \iff (a, b) \in R$$

Data $f : A \rightarrow B$ è possibile definire la funzione inversa $f^{-1} : B \rightarrow A$ se, e solo se, f è biiettiva.

1.3 Relazioni d'equivalenza

Dato un insieme A ed R una relazione binaria applicata ad esso: $R \subseteq A \times A$. Si dice che R è una relazione di equivalenza se sono soddisfatte le seguenti proprietà:

1. **riflessiva** $\forall a \in A, a R a$
ogni elemento è in relazione con sé stesso
2. **simmetrica** $\forall a, b \in A \quad a R b \implies b R a$
dati due elementi in relazione fra loro, allora tale legame è equivalente per ogni verso
3. **transitiva** $\forall a, b, c \in A \quad a R b, b R c \implies a R c$
se un elemento è in relazione con altri due allora questi ultimi lo saranno tra loro

Se l'operazione coinvolge un'eguaglianza le tre proprietà vengono velocemente dimostrate sfruttando le proprietà dell'uguaglianza stessa.

Esercizio (relazione d'equivalenza). Determinare se la seguente relazione, $R \in \mathbb{Z}$, è di equivalenza:

$$\forall a, b \in \mathbb{Z} \quad a R b \iff a + b \text{ è pari}$$

-
1. riflessiva

$$\forall a \in \mathbb{Z} \quad a R a? \quad a + a = \text{pari?} \quad a + a = 2a \implies a \text{ pari } \forall a \in \mathbb{Z}$$

2. simmetrica

$$\forall a, b \in \mathbb{Z} \quad a R b \implies b R a? \quad a + b = \text{pari} \implies b + a = \text{pari?}$$

$$a R b \implies a + b = \text{pari} \implies \underbrace{a + b = 2k \quad k \in \mathbb{Z}}_{\text{definizione di numero pari}}$$

$$\underbrace{b + a = 2k \quad k \in \mathbb{Z}}_{\text{commutativa addizione}} \implies b + a = \text{pari} \implies b R a$$

3. transitiva

$$\forall a, b, c \in \mathbb{Z} \quad a R b, b R c \implies a R c?$$

$$\begin{cases} a R b \implies a + b = \text{pari} \implies a + b = 2k \quad k \in \mathbb{Z} \\ b R c \implies b + c = \text{pari} \implies b + c = 2k' \quad k' \in \mathbb{Z} \end{cases}$$

$$a + b + b + c = 2k + 2k' \implies a + c = 2k + 2k' - 2b$$

$$a + c = \underbrace{2(k + k' - b)}_{k'' \in \mathbb{Z}} = a + c = 2k'' \quad \text{pari} \implies a R c$$

1.3.1 Divisibilità

Dato l'insieme dei naturali $\mathbb{N}$ ed una relazione R di divisibilità si ha

$$\forall a, b \in \mathbb{N} \quad a \mid b \iff \exists q \in \mathbb{N} : b = a \cdot q$$

Da tale relazione si intende se un certo numero è divisibile per un altro.

1.3.2 Congruenza

Definizione (congruenza). Dati l'insieme degli interi $\mathbb{Z}$ ed un qualunque valore intero $m \in \mathbb{Z}$, si definisce congruenza modulo m la seguente relazione:

$$\forall a, b \in \mathbb{Z} \quad a \equiv b \pmod{m} \iff m \mid a - b \implies \exists q \in \mathbb{Z} : a - b = m \cdot q$$

1.3.3 Classe di equivalenza

Definizione (classe di equivalenza). Sia A un insieme ed R una relazione d'equivalenza applicata su di esso, allora A sarà l'insieme definito come segue:

$$[a]_R = \{b \in A : a R b\} \subseteq A$$

Si ha dunque un insieme formato da tutti gli elementi b di A che sono in relazione con l'elemento a .

1.3.3.1 Insieme quoziente

Definizione (insieme quoziente). L'insieme di tutte le classi dell'insieme A rispetto ad una relazione d'equivalenza R :

$$A/R = \{[a]_R : a \in A\}$$

1.3.4 Relazioni antisimmetriche

Definizione (relazione antisimmetrica). Dato un insieme A ed R una relazione applicata su di esso, questa si dice antisimmetrica se, e solo se:

$$\forall a, b \in A \quad a R b, b R a \implies a = b$$

Definizione (relazione di ordine parziale). Dato un insieme A ed R una relazione applicata su di esso, questa si dice di ordine parziale se, e solo se, valgono le seguenti proprietà:

- | | |
|--------------------|---|
| i. riflessiva | $\forall a \in A \quad a R a$ |
| ii. antisimmetrica | $\forall a, b \in A \quad a R b, b R a \implies a = b$ |
| iii. transitiva | $\forall a, b, c \in A \quad a R b, b R c \implies a R c$ |

Definizione (relazione di ordine totale). Una relazione di ordine parziale viene mutata in ordine totale se vale questa quarta condizione:

- | | |
|----------------|--|
| iv. dicotomica | $\forall a, b \in A \quad a R b \text{ oppure } b R a$ |
|----------------|--|

1.3.4.1 Massimi e minimi

Definizione (minimo elemento). Dato un insieme A ed una relazione, di ordine almeno parziale, su di esso definita. Sia poi $a \in A$, si dice che a è un minimo elemento se, e solo se:

$$\forall b \in A \quad a R b \quad a = \min_R A$$

Dunque preso l'elemento a , esso è in relazione con tutti gli elementi appartenenti ad A .

Definizione (massimo elemento). Dato un insieme A ed una relazione, di ordine almeno parziale, su di esso definita. Sia poi $a \in A$, si dice che a è un massimo elemento se, e solo se:

$$\forall b \in A \quad b R a \quad a = \max_R A$$

Dunque preso l'elemento a , esso è in relazione a tutti gli elementi appartenenti ad A .

Chiaramente, se esistono, i massimo e minimo elementi sono unici.

1.3.4.1.1 Minimali e massimali

Definizione (elemento minimale). Sia A un insieme, R una relazione di equivalenza di ordine parziale ed $a \in A$. Si dice che a è elemento minimale se, e solo se:

$$\forall m \in A : m \neq a \quad m R a \implies m = a$$

Esempio (minimale). Preso un insieme determinarne il minimale per divisibilità.

$$A = \{2, 3, 4\} \quad (\{2, 3, 4\}, |)$$

Sappiamo che il minimo elemento per la divisibilità è 1 ma in questo caso non è presente perciò 2 è definito minimale.

Definizione (elemento massimale). Sia A un insieme, R una relazione di equivalenza di ordine parziale ed $a \in A$. Si dice che a è elemento massimale se, e solo se:

$$\forall M \in A \quad M = a \implies a R M \iff M \neq a \implies a \not R M$$

Sezione 2

LOGICA

Per approcciarsi alla logica è necessario un alfabeto, ossia un insieme non vuoto di simboli formato da variabili, o lettere proposizionali, parentesi e connettivi.

$\neg$ negazione $\wedge$ congiunzione $\vee$ disgiunzione $\implies$ implicazione $\iff$ doppia implicazione

Tabella 2.1: Tavole di verità dei connettivi logici

P	Q	$\neg P$	$\neg Q$	$P \wedge Q$	$P \vee Q$	$P \implies Q$	$Q \implies P$	$P \iff Q$
F	F	V	V	F	F	V	V	V
F	V	V	F	F	V	V	F	F
V	F	F	V	F	V	F	V	F
V	V	F	F	V	V	V	V	V

L'implicazione è particolare in quanto unidirezionale. Se n è il numero di parametri coinvolti, allora 2^n saranno le righe della tavola di verità.

2.1 Logica proposizionale

Una proposizione è una frase a cui è assegnabile un valore di validità: vero o falso. Se essa contiene una variabile si chiama predicato.

Teorema (leggi di De Morgan). Per negare una proposizione si riscrive la stessa, negata, sostituendo la congiunzione.

I^a legge: $\neg(P \wedge Q) \equiv \neg(P) \vee \neg(Q)$

II^a legge: $\neg(P \vee Q) \equiv \neg(P) \wedge \neg(Q)$

A volte si potrebbe incappare in delle eguaglianze di risultato da formule diverse, un caso basilare:

$$A \iff B \equiv (A \implies B) \wedge (B \implies A)$$

Tabella 2.2: Legge contronominale

Vi è poi la cosiddetta legge contronominale, dove si nota un capovolgimento dell'implicazione una volta negati i rispettivi termini.

A	B	$A \implies B$	$\neg B \implies \neg A$
0	0	1	1
0	1	1	1
1	0	0	0
1	1	1	1

2.1.1 Formule

Lo svolgimento di proposizioni tramite l'utilizzo delle tavole di verità è detto formula.

Definizione (formula soddisfacibile). Una formula è detta soddisfacibile se, e solo se, almeno una volta nell'ultima colonna della sua tavola di verità compare un vero.

Definizione (tautologia). Se una formula non solo è soddisfacibile ma presenta tutti unì sull'ultima colonna della rispettiva tavola di verità allora è detta tautologia.

Definizione (formula non soddisfacibile). Una formula è detta non soddisfacibile, o contraddizione, quando l'ultima colonna della sua tavola di verità compaiono solo falsi.

Definizione (contraddizione). Se una formula non solo non è soddisfacibile ma presenta tutti zeri sull'ultima colonna della rispettiva tavola di verità allora è detta contraddizione.

2.1.2 Preposizione di alfabeti

Sia L un insieme non vuoto i cui elementi si chiamano lettere. L'insieme $Prop(L)$ delle preposizioni su L è un sottoinsieme di tutte le combinazioni del seguente insieme:

$$(L \cup \{ (,), \neg, \wedge, \vee, \implies, \iff \})$$

Di seguito alcune condizioni valide per le preposizioni basate su un alfabeto:

$$A \in L \implies (A) \in Prop(L)$$

$$P \in Prop(L) \implies (\neg P) \in Prop(L)$$

$$P, Q \in Prop(L) \implies (P \blacksquare Q) \in Prop(L)$$

2.1.2.1 Lunghezza di una preposizione

Si tratta di un naturale pari al numero dei simboli presenti nella stringa.

Esempio (lunghezza di una proposizione). Data una preposizione del tipo $((A) \implies (B))$ la sua lunghezza equivale al numero dei simboli compresi fra le parentesi della funzione $ln()$:

$$ln(((A) \implies (B))) = 9$$

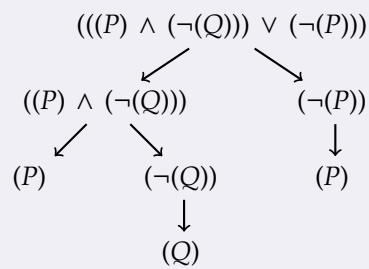
2.1.2.2 Altezza di una preposizione

Si tratta di un naturale pari al livello della preposizione analizzata. Coincide inoltre con quella dell'albero di costruzione.

$$Prop_n(L) \implies ht(Prop_n(L)) = n$$

Esercizio (altezza di una preposizione). Calcolare l'altezza della seguente preposizione:

$$(((\) \wedge (\neg(Q))) \vee (\neg(P)))$$



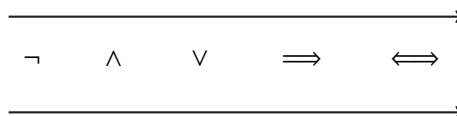
Dal grafico riportato è intuibile che l'altezza è quattro:

$$ht(((P) \wedge (\neg(Q))) \vee (\neg(P))) = 4$$

2.1.2.3 Analisi sintattica

Ad ogni preposizione è possibile associare un albero di costruzione. Per effettuare il procedimento inverso si inseriscono le parentesi nel seguente ordine:

1. lettere proposizionali;
2. negazioni;
3. connettivi binari. Si hanno due regole da rispettare:
 - precedenza a partire da sinistra;
 - rispetto della gerarchia dei connettivi.



Esempio (analisi sintattica). Trasformare la seguente dicitura in preposizione: $A \wedge \neg B \vee \neg A$

1. $(A) \wedge \neg(B) \vee \neg(A)$
2. $(A) \wedge (\neg(B)) \vee (\neg(A))$
3. $((A) \wedge (\neg(B))) \vee (\neg(A))$

2.1.2.3.1 Albero sintattico

L'albero sintattico di una preposizione $P \in Prop(L)$ viene costruito secondo il seguente metodo:

- radice come preposizione $P \in Prop(L)$
- ogni nodo potrebbe
 - i. non avere successori se è proposizione atomica

$$(P)$$

- ii. avere un solo successore immediato

$$\begin{array}{c} (\neg(P)) \\ \downarrow \\ (P) \end{array}$$

- iii. avere due successori immediati

$$\begin{array}{ccc} & (P \blacksquare Q) & \\ \swarrow & & \searrow \\ (P) & & (Q) \end{array}$$

2.1.2.3.2 Albero binario

Si tratta di un insieme parzialmente ordinato dalla relazione che viene indicata con $\leq$ in cui valgono le proprietà: riflessiva, antisimmetrica e transitiva. Gli elementi dell'albero si chiamano nodi. Presi due casualmente, se $x \leq y$ si dice che y è successore, o discendente, di x . Esiste poi un nodo minimo detto radice:

$$r : r \leq x, \forall x$$

I nodi $f : \nexists g \neq f$ per cui $f \leq g$ si dicono foglie. Ogni nodo che non sia al contempo una foglia ha, al massimo, uno o due successori.

2.1.3 Semantica

Viene giudicata vera o falsa una preposizione tramite una valutazione:

$$v : Prop(L) \Rightarrow \{0, 1\}$$

Un insieme di proposizioni si dice soddisfacibile se esiste una valutazione che le soddisfa tutte.

Esempio (insieme soddisfacibile). Dire se l'insieme S definito come segue è soddisfacibile.

$$S = \{\alpha, \alpha \vee \beta, \alpha \Rightarrow \neg\beta\}$$

Si procede costruendo la rispettiva tabella di verità e verificando l'esistenza di una riga composta da tutti uni.

α	β	$\alpha \vee \beta$	$\alpha \Rightarrow \neg\beta$	S
0	0	0	1	0
0	1	1	1	0
1	0	1	1	1
1	1	1	0	0

In questo caso la terza riga lo è, quindi per $\alpha = 1$ e $\beta = 0$.

- $v \models \alpha$ la preposizione è soddisfacibile
- $v \models S$ l'insieme di preposizioni è soddisfacibile
- $S \models \beta$ la preposizione è conseguenza logica dell'insieme

2.2 Formule CNF e DNF

Ogni formula della logica proposizionale ne ha delle equivalenti in dicitura CNF o DNF.

Definizione (formula CNF). Una formula si dice scritta in CNF se, e solo se, è una congiunzione di disgiunzioni di lettere proposizionali o sue negazioni.

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

Definizione (formula DNF). Una formula si dice scritta in DNF se, e solo se, è una disgiunzione di congiunzioni di lettere proposizionali o sue negazioni.

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

Per tramutare formule proposizionali in CNF o DNF si sfrutta i passi del seguente algoritmo:

1. eliminare, se esiste, la doppia implicazione

$$A \iff B \equiv (A \implies B) \wedge (B \implies A)$$

2. eliminare, se esiste, l'implicazione

$$A \implies B \equiv \neg A \vee B$$

3. eliminare, se esiste, la negazione qualora non riguarda direttamente lettere proposizionali

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

4. sostituire i simboli delle congiunzioni e disgiunzioni per poi riportarsi alla formula desiderata applicando la proprietà distributiva

$$\text{CNF} \quad + = \wedge \quad * = \vee$$

$$\text{DNF} \quad * = \wedge \quad + = \vee$$

Esempio (formule CNF e DNF). Ecco la mutazione di due formule nelle sintassi ricercate.

CNF

$$\begin{aligned} &(A \wedge B) \vee C \\ &\quad \downarrow \\ &(A + B) \cdot C \\ &\quad \downarrow \\ &(A + C) \cdot (B + C) \\ &\quad \downarrow \\ &(A \vee C) \wedge (B \vee C) \end{aligned}$$

DNF

$$\begin{aligned} &(A \vee B) \wedge C \\ &\quad \downarrow \\ &(A + B) \cdot C \\ &\quad \downarrow \\ &(A \cdot C) + (B \cdot C) \\ &\quad \downarrow \\ &(A \wedge C) \vee (B \wedge C) \end{aligned}$$

2.3 Deduzione naturale

Tramite le seguenti regole dei connettivi logici si arriva a dimostrare ogni derivazione

$$\frac{A_1 \ A_2 \ \dots \ A_k}{B}$$

La simbologia precedente indica: se $(A_1 \ A_2 \ \dots \ A_k)$ sono verificate, allora si deduce B .

2.3.1 Deduzione naturale con operatore $\wedge$

- Introduzione $\wedge$

$$\frac{A \quad B}{A \wedge B} \quad i \wedge$$

- Eliminazione $\wedge$

$$\frac{A \wedge B}{A} \quad e \wedge_1 \qquad \frac{A \wedge B}{B} \quad e \wedge_2$$

2.3.2 Deduzione naturale con operatore $\neg$

- Introduzione $\neg$

$$\frac{A}{\neg \neg A} \quad i \neg$$

- Eliminazione $\neg$

$$\frac{\neg \neg A}{A} \quad e \neg$$

2.3.3 Deduzione naturale con operatore $\Rightarrow$

- Introduzione $\Rightarrow$

$$\frac{\begin{array}{c} A \\ \vdots \\ B \end{array}}{A \Rightarrow B} \quad i \Rightarrow$$

- Eliminazione $\Rightarrow$

$$\begin{array}{cc} \text{MP (Molus Ponens)} & \text{MT (Molus Tolens)} \\ \frac{A \quad A \Rightarrow B}{B} \quad e \Rightarrow \text{MP} & \frac{\neg B \quad A \Rightarrow B}{\neg A} \quad e \Rightarrow \text{MT} \end{array}$$

2.3.4 Deduzione naturale con operatore $\vee$

- Introduzione $\vee$

$$\frac{A}{A \vee B} \quad i \vee_2 \qquad \frac{B}{A \vee B} \quad i \vee_1$$

- Eliminazione $\vee$

$$\frac{A \vee B \quad \neg B}{A} \quad e \vee_1 \qquad \frac{A \vee B \quad \neg A}{B} \quad e \vee_2$$

2.4 Predicati del primo ordine

Linguaggio formale usato per ufficializzare enunciati e ragionamenti.

- a. costanti b. funzioni o relazioni c. predicati o operazioni

2.4.1 Formalizzazione

Esercizio (formalizzazione numero primo). Dato un qualunque numero, capire se esso sia primo.

«Un numero si dice primo se, e solo se, è maggiore di uno ed è divisibile solamente per uno e per sé stesso.»

.....

$$\mathcal{L} = \{P^1, 1, >, |\}$$

P^1	$\rightarrow$	simbolo di operazione unario interpretato come "essere primo"
1	$\rightarrow$	simbolo di costante interpretato come "1"
$>$	$\rightarrow$	simbolo di relazione binaria interpretato come "essere maggiore"
$ $	$\rightarrow$	simbolo di relazione binaria interpretato come "divisibilità"

$$\forall x (P^1(x) \iff (x > 1 \wedge \forall z (z | x \implies z = 1 \vee z = x)))$$