Francesco Ciraulo

Dispense del corso di
Elementi di Logica Matematica

Per i corsi di laurea in M.I.C.S e Matematica
Università degli Studi di Palermo

A. A. 2006/07

Indice

Introduzione

La *logica* (dal greco *logos*=ragione/parola) è la scienza del ragionamento. Nasce come branca della filosofia (vedi Aristotele prima e i logici medievali poi) e solo successivamente (dall'Ottocento in poi) diviene campo di studio da parte anche dei matematici.

La fase non-matematica della logica è tutta tesa ad una classificazione delle possibili forme di ragionamento, mentre il punto di vista matematico evidenzierà simmetria e organicità.

Famosi sono rimasti alcuni principi formulati in ambito medievale:

il principio d'identità : da ogni affermazione segue se stessa;

il principio di non contraddizione : un'affermazione e la sua negazione non possono essere vere contemporaneamente;

il principio del terzo escluso : o un'affermazione è vera o lo è la sua negazione;

ex falso quodlibet : dal falso segue tutto.

Si deve, invece, ai primi logici matematici (vedi Boole) l'introduzione dei simboli per i connettivi e il riconoscimento di come la logica avesse un'intrinseca struttura matematica e che perciò potesse essere studiata con mezzi matematici. Si deve dire, inoltre, che nell'Ottocento la logica assunse un ruolo fondante nella matematica grazie (e contribuendo) allo sviluppo dell'assiomatica moderna.

L'approccio matematico alla logica ha portato a notevoli risultati sia di carattere tecnico che di puro interesse teorico; primi fra tutti i due celebrati teoremi di incompletezza di Gödel, ma anche il suo teorema di completezza per la logica del primo ordine, il teorema di compattezza e i teoremi di Löwenheim-Skolem.

Parte I

Logica proposizionale classica

Capitolo 1

Il linguaggio e le formule

La logica proposizionale si propone di formalizzare e quindi analizzare i ragionamenti che, nel nostro linguaggio naturale, possono essere formulati ricorrendo ad affermazioni (quindi niente esclamazioni, domande, ecc.) composte fra loro usando particelle come: e, o, sia…sia, né…né, ma non, o…o, e/o, ecc..

Il linguaggio della logica proposizionale (cioè l'insieme dei segni convenzionali che vengono usati nella trattazione matematica della logica) è composto dai seguenti gruppi di simboli:

variabili proposizionali : p, q, r, s, t, … (rappresentano delle proposizioni "atomiche", cioè non contenenti alcun connettivo);

connettivi : $\wedge$ (congiunzione), $\vee$ (disgiunzione), $\rightarrow$ (implicazione);

costante per il falso : $\bot$;

parentesi : (,).

I connettivi sono da intendersi come operazioni binarie nell'insieme delle formule (vedi definizione successiva). Oltre ai suddetti connettivi, si definiscono $\neg$, $\top$ e $\leftrightarrow$ come

$$\neg A := A \rightarrow \bot \qquad \top := \bot \rightarrow \bot = \neg \bot \qquad A \leftrightarrow B := (A \rightarrow B) \wedge (B \rightarrow A)$$

per A e B formule. Il significato dei connettivi, cioè la loro semantica, è studiato nel prossimo capitolo. In prima approssimazione, possiamo dire che $\wedge$ corrisponde alla congiunzione italiana "e", $\vee$ corrisponde alla "o" (non esclusiva, il latino *vel*), $\rightarrow$ alla locuzione "se…allora" e $\neg$ a "non".

Definizione 1.1 *Sia $\mathcal{L}$ un linguaggio proposizionale. L'insieme delle* formule proposizionali *nel linguaggio $\mathcal{L}$ è indicato col simbolo $Frm_{\mathcal{L}}$ (o, semplicemente, con Frm) ed è definito ricorsivamente dalle seguenti condizioni:*

- *le variabili proposizionali appartengono a Frm;*
- *$\perp \in Frm$;*
- *se $A \in Frm$ e $B \in Frm$ allora anche $(A \wedge B)$, $(A \vee B)$ e $(A \to B)$ appartengono a Frm.*

Il sottoinsieme di Frm formato dalle variabili proposizionali e da $\perp$ è l'insieme delle formule atomiche.

Per esempio, se p e q sono due variabili di $\mathcal{L}$ allora l'espressione (= sequenza di simboli)

$$(p \wedge (\perp \to q))$$

è una formula.

Ogni formula è suscettibile di diverse interpretazioni; infatti, ogni variabile proposizionale può rappresentare differenti affermazioni. Ad esempio, p potrebbe stare per la frase "$e^{i\pi} + 1 = 0$" o anche per "È impossibile passare l'esame di Logica". Pertanto non ha senso chiedersi se una formula sia vera o falsa, ma soltanto se è vera o falsa relativamente ad una particolare interpretazione. Il concetto di interpretazione sarà formalizzato meglio nel prossimo capitolo.

Ad ogni formula può essere associato un albero (vedi appendice) che ne descrive la costruzione a partire dalle formule atomiche. Ad esempio, l'albero di costruzione di $p \wedge (\perp \to q)$ è il seguente.

$$\begin{tikzcd}
 & \perp \arrow[dr, dash] & & q \arrow[dl, dash] \\
p \arrow[dr, dash] & & \perp \to q \arrow[dl, dash] & \\
 & p \wedge (\perp \to q) & &
\end{tikzcd}$$

Come si vede dall'esempio, la radice dell'albero è la formula in considerazione, le foglie sono le formule atomiche che compaiono in essa, mentre ad ogni passaggio di livello corrisponde l'introduzione di un connettivo. Le formule che occupano i nodi dell'albero vengono chiamate le *sottoformule* della formula data. Quindi, per esempio, le sottoformule di $p \wedge (\perp \to q)$ sono p, q, $\perp$,

$\perp \to q$ e la formula stessa; al contrario, $p \wedge q$ non è una sottoformula della formula data.

Si definisce *complessità* di una formula la profondità del corrispondente albero di costruzione, cioè la lunghezza (= numero di tratti) del suo ramo più lungo.

Ad esempio, la profondità di una formula atomica è 0, mentre le formule che contengono un solo connettivo hanno profondità 1.

Capitolo 2

Semantica: tavole di verità.

In questo capitolo definiremo i connettivi $\wedge$, $\vee$, $\rightarrow$ (e anche la costante $\perp$) da un punto di vista semantico. Data una certa formula A ci sono, ovviamente, infiniti modi possibili di interpretarla. In altre parole A può rappresentare una frase qualsiasi (o quasi) della nostra lingua. Abbiamo già detto che le frasi che vogliamo studiare sono le affermazioni; quindi la formula A non può rappresentare frasi interrogative o esclamative. Inoltre, per semplicità, assumiamo che le nostre affermazioni abbiano un chiaro e oggettivo significato. Ad esempio, tutte le affermazioni che si incontrano in matematica vanno bene. Al contrario, non possiamo prendere in considerazioni frasi dal significato ambiguo o soggettivo come, ad esempio, "L'Hard Rock è sublime". Da quanto abbiamo deciso, segue che le formule possono essere interpretate soltanto in affermazioni suscettibili di essere soltanto o vere o false. Ciò non significa, però, che dobbiamo limitarci a considerare soltanto frasi di cui già conosciamo la verità o la falsità. Ad esempio, abbiamo tutto il diritto di considerare la frase "Gli alieni esistono" perchè essa può essere soltanto vera o falsa, anche se attualmente non sappiamo quale dei due casi si presenta.

Da quanto detto finora, segue che tutte le interpretazioni di una formula A si dividono in due classi, quelle che rendono A vera e quelle che rendono A falsa. Quando A risulta vera in una certa interpretazione, diremo che il suo valore di verità in quella interpretazione è V; in caso contrario, il valore di verità di A sarà F. Ovviamente, qualora le formule da considerare siano più di una, le classi di interpretazioni da considerare saranno più di due. Ad esempio, se abbiamo due formule A e B ci saranno quattro classi di interpretazioni per tenere conto delle quattro combinazioni possibili dei valori di verità di A e B. In questo caso la situazione sarà schematizzata con una tabella del tipo

A	B
V	V
V	F
F	V
F	F

che viene chiama "tavola di verità". Nota che ogni riga della tavola di verità non rappresenta una singola interpretazione bensì una classe di interpretazioni. Ad esempio la penultima riga rappresenta la classe di tutte le interpretazioni in cui A è falsa, ma B è vera. In questo modo è possibile schematizzare la definizione semantica dei connettivi e di $\perp$ tramite la seguente tavola.

Definizione semantica dei connettivi e del falso

A	B	$A \wedge B$	$A \vee B$	$A \rightarrow B$	$\perp$
V	V	V	V	V	F
V	F	F	V	F	F
F	V	F	V	V	F
F	F	F	F	V	F

Il significato della tavola può essere chiarito da un esempio. Consideriamo il connettivo $\wedge$ e osserviamo le prime tre colonne della tavola. Il loro significato è: la formula $A \wedge B$ è vera in quelle interpretazioni in cui sia A che B sono vere ed è falsa in tutti gli altri casi.

Ricordando che $\neg A$ è definito come $A \rightarrow \perp$, è facile ricavare la tavola di verità di $\neg A$. Come c'era da aspettarsi, $\neg A$ risulterà vera esattamente in quelle interpretazioni in cui A risulta falsa.

La tavola di verità di un connettivo deve essere considerata come la sua definizione. Per esempio, la quarta colonna definisce il simbolo $\vee$. Nota come quest'ultimo non corrisponda in tutto e per tutto alla "o" italiana; sarebbe meglio immaginarlo come la "e/o" che compare in certi moduli. In ogni caso, è da notare che la disgiunzione esclusiva delle frasi tipo "o A o B" può essere rappresentata dalla formula

$$(A \vee B) \wedge \neg (A \wedge B) \qquad (\textit{disgiunzione esclusiva})$$

(per rendersene conto basta costruire la relativa tavola di verità).

Definizione 2.1 *Si dice che una formula A è una* tautologia *e si scrive* $\models A$ *se A risulta vera in ogni interpretazione.*

2.1 Esempi

Esempio 2.2 *Costruire la tavola di verità della formula:*

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

Soluzione. Per prima cosa bisogna riconoscere quali sono le sottoformule della formula data. In realtà, bisognerebbe sapere che struttura hanno le formule A e B; possiamo, però, trattarle come atomiche. Quindi le sottoformule sono (in ordine di complessità) A, B, $A \vee B$, $A \wedge B$, $\neg (A \wedge B)$ e, infine, la formula stessa. Nella tavola di verità bisogna inserire una colonna per ogni sottoformula.

A	B	$A \vee B$	$A \wedge B$	$\neg (A \wedge B)$	$(A \vee B) \wedge \neg (A \wedge B)$
V	V	V	V	F	F
V	F	V	F	V	V
F	V	V	F	V	V
F	F	F	F	V	F

Quindi la formula è vera se e solo se una e una sola fra A e B è vera. □

Esempio 2.3 *Costruire la tavola di verità del connettivo $\leftrightarrow$ (doppia implicazione) definito da:*

$$A \leftrightarrow B \quad \equiv \quad (A \to B) \wedge (B \to A).$$

Soluzione.

A	B	$A \to B$	$B \to A$	$A \leftrightarrow B$
V	V	V	V	V
V	F	F	V	F
F	V	V	F	F
F	F	V	V	V

Quindi $A \leftrightarrow B$ è vera quando A e B hanno lo stesso valore di verità. □

Esempio 2.4 *Provare che la formula*

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

è una tautologia.

Soluzione.

A	B	$A \to B$	$A \wedge (A \to B)$	$(A \wedge (A \to B)) \to B$
V	V	V	V	V
V	F	F	F	V
F	V	V	F	V
F	F	V	F	V

□

Capitolo 3

Sintassi: il calcolo della deduzione naturale.

In questo capitolo descriveremo un approccio alternativo alla logica proposizionale. Anzichè definire i connettivi semanticamente, daremo delle regole dimostrative che ci diranno quali sono i modi corretti di fare una deduzione. Anche se questo approccio potrà sembrare più laborioso, rimarra in effetti l'unico praticabile quando introdurremo i quantificatori.

In generale, una regola è qualcosa del tipo

$$\frac{A_1 \quad \cdot \quad \cdot \quad \cdot \quad A_n \quad \begin{matrix}[B_1]' \\ \vdots \\ C_1\end{matrix} \quad \cdot \quad \cdot \quad \cdot \quad \begin{matrix}[B_m]' \\ \vdots \\ C_m\end{matrix}}{D},$$

dove le A_i sono le premesse della regola e D è la conclusione; le formule B_j racchiuse fra parentesi quadre rappresentano delle premesse momentanee che spariscono in corrispondenza del passaggio dove si trova l'apice (o, in caso di più apici, il numero corrispondente). In definitiva, la regola sopra esprime quanto segue: *se da ogni B_j segue il corrispondente C_j, allora da tutte le A_i prese assieme segue D.*

Le regole del calcolo della deduzione naturale (per la logica proposizionale classica) sono le seguenti nove:

$$\frac{A \quad B}{A \wedge B} \wedge\ i \qquad \frac{A \wedge B}{A} \wedge\ e\ (sx) \quad \frac{A \wedge B}{B} \wedge\ e\ (dx)$$

$$\frac{A}{A \lor B}\ \lor\ i\ (sx) \qquad \frac{B}{A \lor B}\ \lor\ i\ (dx) \qquad \frac{\begin{array}{c}[A]' \\ \vdots \\ C\end{array} \quad \begin{array}{c}[B]' \\ \vdots \\ C\end{array} \quad A \lor B}{C}\ '\ \lor\ e$$

$$\frac{\begin{array}{c}[A]' \\ \vdots \\ B\end{array}}{A \to B}\ '\ \to\ i \qquad \frac{A \quad A \to B}{B}\ \to\ e \qquad \frac{\begin{array}{c}[\neg\, A]' \\ \vdots \\ \bot\end{array}}{A}\ '\ a$$

dove A, B e C sono formule arbitrarie, i sta per "introduzione", e per "eliminazione" e a per "assurdo" (perchè la regola a cui si riferisce viene chiamata di riduzione all'assurdo). Quindi le regole di introduzione sono quelle in cui il connettivo non è presente nelle premesse, ma appare nella conclusione; viceversa, le regole di eliminazione sono quelle in cui il connettivo è presente in una delle premesse, ma scompare nella conclusione.

Una dimostrazione (nel calcolo della deduzione naturale) della formula B a partire dalle premesse A_1, …, A_n è un albero la cui radice è B, le cui foglie sono (non necessariamente tutte) le A_i (anche ripetute più volte) ed eventuali altre formule che servono da premesse momentanee; inoltre, tutti i nodi sono formule e le regole del calcolo sono i possibili legami fra di essi. Per esempio gli alberi

$$\frac{\dfrac{A \land B}{A}\ \scriptstyle{\land\ e\ (sx)}}{A \lor B}\ \scriptstyle{\lor\ i\ (sx)} \qquad \frac{\dfrac{A \land B}{B}\ \scriptstyle{\land\ e\ (dx)}}{A \lor B}\ \scriptstyle{\lor\ i\ (dx)}$$

sono due diverse dimostrazioni del fatto che da $A \land B$ segue $A \lor B$, mentre l'albero

$$\frac{\dfrac{\dfrac{\bot \qquad [\neg\, A]^1}{\bot \land (\neg\, A)}\ \scriptstyle{\land\ i}}{\bot}\ \scriptstyle{\land\ e\ (sx)}}{A}\ \scriptstyle{1\ \ a}$$

dimostra che dal falso segue tutto. Quando la formula B è dimostrabile a partire dalle ipotesi A_1, …, A_n scriveremo

$$A_1, \ldots, A_n \vdash B$$

(il simbolo $\vdash$ non è un connettivo, bensì un legame meta-linguistico).[1] In particolare, $\vdash A$ significa che la formula A è dimostrabile (senza premesse). Nel caso in cui $A \vdash B$ e anche $B \vdash A$ scriveremo $A \equiv B$.

Teorema 3.1 (di deduzione) *Per ogni $A_1, \ldots, A_n, B, C \in Frm$ si ha:*

$$A_1, \ldots, A_n, B \vdash C \quad \textit{se e solo se} \quad A_1, \ldots, A_n \vdash (B \rightarrow C) \quad .$$

In particolare, $A \vdash B$ se e solo se $\vdash (A \rightarrow B)$.

Dim: I due versi della prova sono riassunti dalle seguenti figure.

$$\dfrac{\begin{array}{c} A_1 \quad \cdot \quad \cdot \quad \cdot \quad A_n \quad [B]^1 \\ \vdots \ \textit{ipotesi} \\ C \end{array}}{B \rightarrow C}\ {\scriptstyle 1 \rightarrow i} \qquad\qquad \dfrac{B \qquad \begin{array}{c} A_1 \quad \cdot \quad \cdot \quad \cdot \quad A_n \\ \vdots \ \textit{ipotesi} \\ B \rightarrow C \end{array}}{C}\ {\scriptstyle \rightarrow e}$$

c.v.d.

3.1 Esempi

Esempio 3.2 *Dimostrare che $\wedge$ e $\vee$ sono operazioni commutative sull'insieme $Frm/\equiv$ delle formule modulo equivalenza.*

Soluzione. Ovviamente basta dimostrare che $A \wedge B \vdash B \wedge A$ e che $A \vee B \vdash B \vee A$.

$$\dfrac{\dfrac{A \wedge B}{B}\ {\scriptstyle \wedge e} \qquad \dfrac{A \wedge B}{A}\ {\scriptstyle \wedge e}}{B \wedge A}\ {\scriptstyle \wedge i} \qquad\qquad \dfrac{\dfrac{[A]^1}{B \vee A}\ {\scriptstyle \vee i} \qquad \dfrac{[B]^1}{B \vee A}\ {\scriptstyle \vee i} \qquad A \vee B}{B \vee A}\ {\scriptstyle 1 \vee i}$$

□

Esempio 3.3 *Provare che $\wedge$ e $\vee$ sono idempotenti, cioè che vale $A \wedge A \equiv A$ e $A \vee A \equiv A$.*

[1] Nota che, durante una dimostrazione, non si ha nessun obbligo di usare tutte le ipotesi. Quindi se vale $A_1, \ldots, A_n \vdash B$, a maggior ragione vale anche $C, A_1, \ldots, A_n \vdash B$ e così via.

Soluzione. Ovviamente, $A \wedge A \vdash A$ segue dalle regole di $\wedge$ -eliminazione; l'altro verso vale per $\wedge$ -introduzione a partire dall'ipotesi A ripetuta due volte.

Similmente, $A \vdash A \vee A$ segue dalle regole di $\vee$ -introduzione, mentre l'altro verso si può dimostrare così:

$$\dfrac{[A]^1 \quad [A]^1 \quad A \vee A}{A}\ {\scriptstyle 1 \vee e}$$

(notare come A è sia un'ipotesi momentanea, sia ciò che segue da essa; in altre parole, le A, B e C della regola di $\vee$ -eliminazione coincidono, in questo caso, tutte con A.) □

Esempio 3.4 (Proprietà associative di $\wedge$ e $\vee$)

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

Soluzione. Come esempio, proviamo $A \vee (B \vee C) \vdash (A \vee B) \vee C$.

$$\dfrac{\dfrac{\dfrac{[A]^2}{A \vee B}}{(A \vee B) \vee C} \qquad \dfrac{\dfrac{\dfrac{[B]^1}{A \vee B}}{(A \vee B) \vee C} \quad \dfrac{[C]^1}{(A \vee B) \vee C} \quad [B \vee C]^2}{(A \vee B) \vee C}\ {\scriptstyle 1} \qquad A \vee (B \vee C)}{(A \vee B) \vee C}\ {\scriptstyle 2}$$

□

Esempio 3.5 (Proprietà distributive)

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

Soluzione. Proviamo che $A \wedge (B \vee C) \vdash (A \wedge B) \vee (A \wedge C)$.

$$\dfrac{\dfrac{\dfrac{\dfrac{A \wedge (B \vee C)}{A} \quad [B]^1}{A \wedge B}}{(A \wedge B) \vee (A \wedge C)} \qquad \dfrac{\dfrac{\dfrac{A \wedge (B \vee C)}{A} \quad [C]^1}{A \wedge C}}{(A \wedge B) \vee (A \wedge C)} \qquad \dfrac{A \wedge (B \vee C)}{B \vee C}}{(A \wedge B) \vee (A \wedge C)}\ {\scriptstyle 1}$$

□

Esempio 3.6 (Leggi di assorbimento)

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

Soluzione. Dimostriamo, per esempio, che $A \vee (A \wedge B) \vdash A$.

$$\dfrac{[A]^1 \qquad \dfrac{[A \wedge B]^1}{A}\wedge e \qquad A \vee (A \wedge B)}{A}\ 1 \vee e$$

□

Esempio 3.7 (Principio d'identità) $\vdash (A \to A)$

Soluzione.

$$\dfrac{[A]^1}{A \to A}\ 1 \to i$$

□

Esempio 3.8 (Principio di non contraddizione) $\vdash \neg (A \wedge \neg A)$

Soluzione.

$$\dfrac{\dfrac{\dfrac{[A \wedge \neg A]^1}{A}\wedge e \qquad \dfrac{[A \wedge \neg A]^1}{\neg A}\wedge e}{\perp}\to e}{\neg (A \wedge \neg A)}\ 1 \to i$$

(Ricordare che $\neg A$ è uguale, per definizione, ad $A \to \perp$.) □

Esempio 3.9 (Principio del terzo escluso) $\vdash (A \vee \neg A)$

Soluzione.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\neg A]^1}{A \vee \neg A}\vee i \qquad [\neg (A \vee \neg A)]^3}{\perp}\to e}{A}\ 1\ a \qquad \dfrac{\dfrac{\dfrac{[A]^2}{A \vee \neg A}\vee i \qquad [\neg (A \vee \neg A)]^3}{\perp}\to e}{\neg A}\ 2 \to i}{\perp}\to e}{A \vee \neg A}\ 3\ a$$

□

Esempio 3.10 (Principio della doppia negazione) $(\neg\neg A) \equiv A$

Soluzione.

$$\dfrac{\dfrac{A \quad [\neg A]^1}{\perp}\to e}{\neg\neg A}\ 1 \to i \qquad\qquad \dfrac{\dfrac{[\neg A]^1 \quad \neg\neg A}{\perp}\to e}{A}\ 1\ a$$

□

Esempio 3.11 (Leggi di De morgan)

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

Soluzione. La dimostrazione più difficile è quella di $\neg\,(A \wedge B) \vdash (\neg\,A \vee \neg\,B)$; ne diamo due prove diverse.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[A]^2 \quad [B]^1}{A \wedge B} \qquad \neg\,(A \wedge B)}{\bot}}{\neg\,B}\;{\scriptstyle 1}}{\neg\,A \vee \neg\,B} \qquad \dfrac{[\neg\,A]^2}{\neg\,A \vee \neg\,B} \qquad \begin{matrix}\vdots\ \text{terzo escluso}\\ A \vee \neg\,A\end{matrix}}{\neg\,A \vee \neg\,B}\;{\scriptstyle 2}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\neg\,A]^1}{\neg\,A \vee \neg\,B} \quad [\neg\,(\neg\,A \vee \neg\,B)]^3}{\bot}}{A}\;{\scriptstyle 1} \qquad \dfrac{\dfrac{\dfrac{[\neg\,B]^2}{\neg\,A \vee \neg\,B} \quad [\neg\,(\neg\,A \vee \neg\,B)]^3}{\bot}}{B}\;{\scriptstyle 2}}{A \wedge B} \qquad \neg\,(A \wedge B)}{\dfrac{\bot}{\neg\,A \vee \neg\,B}\;{\scriptstyle 3}}$$

□

Esempio 3.12 *Per ogni $A_1, \ldots, A_n, B \in Frm$ si ha:*

$$A_1, \ldots, A_n \vdash B \quad \textit{se e solo se} \quad A_1 \wedge \ldots \wedge A_n \vdash B \quad .$$

Capitolo 4

Il teorema di validità e completezza

In questo capitolo dimostreremo l'equivalenza fra le nozioni semantiche (tavole di verità) e quelle sintattiche (calcolo della deduzione naturale) introdotte, rispettivamente, nei capitoli 2 e 3. Il teorema che esprime questa equivalenza fra semantica e sintassi sarà chiamato teorema di validità e completezza (o, per brevità, teorema di completezza).

4.1 L'enunciato del teorema di completezza

Nella sua forma più semplice, l'enunciato del teorema di completezza è il seguente.

Teorema 4.1 (Teorema di completezza) [1]
Per ogni formula A, $\vdash A$ se e solo se $\models A$.

Cioè, una formula è dimostrabile (nel calcolo della deduzione naturale) se e solo se è una tautologia. I due versi dell'equivalenza espressa dal teorema esprimono, rispettivamente, la validità e la completezza del calcolo.

$$\vdash A \quad \Longrightarrow \quad \models A \qquad \text{(teorema di validità)}$$

$$\models A \quad \Longrightarrow \quad \vdash A \qquad \text{(teorema di completezza)}$$

[1] Il nome completo di questo teorema è "Teorema di validità e completezza del calcolo della deduzione naturale per la logica proposizionale classica".

Il teorema di validità esprime il fatto che tutto ciò che è dimostrabile con le regole del calcolo è vero; in altre parole, le regole del calcolo sono corrette. Il teorema di completezza, invece, afferma che le regole sono anche sufficienti a dimostrare ogni verità; cioè non abbiamo bisogno di aggiungere ulteriori regole.

Per potere enunciare il teorema di completezza in un'altra forma (che sarà più comoda in seguito), diamo prima la seguente definizione.

Definizione 4.2 *Sia Γ un insieme finito di formule. Con il simbolo $\&\Gamma$ intendiamo la formula (a meno di equivalenza) definita da:*

$$\&\Gamma = \begin{cases} \top & \textit{se } \Gamma = \emptyset \ ; \\ C_1 \wedge \ldots \wedge C_n & \textit{se } \Gamma = \{C_1, \ldots, C_n\} \ . \end{cases}$$

Teorema 4.3 (Teorema di completezza - seconda forma) *Per ogni formula A e per ogni insieme finito di formule Γ, vale:*

$$\Gamma \vdash A \qquad \textit{se e solo se} \qquad \models \&\Gamma \to A \ .$$

Che le due forme sono equivalenti lo si vede facilmente; basta notare che $\Gamma \vdash A$ è equivalente a $\&\Gamma \vdash A$ che, per il teorema di deduzione, non è altro che $\vdash \&\Gamma \to A$.

4.2 Teorema di validità: dimostrazione.

In questa sezione dimostreremo il teorema di validità nella seconda forma; cioè:

$$\Gamma \vdash A \qquad \Longrightarrow \qquad \models \&\Gamma \to A$$

con $A \in Frm$ e Γ sottoinsieme finito di Frm.

Dim: Per induzione (seconda forma) sulla lunghezza n della dimostrazione di $\Gamma \vdash A$.

1. Se $n = 0$, allora la dimostrazione di $\Gamma \vdash A$ è semplicemente

   $$A$$

   e deve essere $A \in \Gamma$. Quindi possiamo immaginare Γ come l'unione $\Gamma' \cup \{A\}$. Di conseguenza $\&\Gamma$ non è altro (a meno di equivalenze) che $(\&\Gamma') \wedge A$ e quindi $\&\Gamma \to A$ è una tautologia.

2. Adesso supponiamo che il teorema sia vero per tutte le prove di lunghezza minore di n e dimostriamolo per n. Distinguiamo sette casi a seconda dell'ultima regola usata nella derivazione.

   (a) Se l'ultima regola usata è quella di $\wedge$-introduzione, allora A deve essere del tipo $B \wedge C$ e la dimostrazione di $\Gamma \vdash A$ avrà una struttura del tipo

$$\frac{\begin{array}{cc}\Gamma & \Gamma \\ \vdots & \vdots \\ B & C\end{array}}{B \wedge C}$$

   dove le due dimostrazioni di $\Gamma \vdash B$ e $\Gamma \vdash C$ hanno lunghezza minore di n. Per l'ipotesi induttiva, sappiamo che sia $\&\Gamma \to B$ che $\&\Gamma \to C$ sono tautologie. Vogliamo provare che anche $\&\Gamma \to A$ è una tautologia. Nelle interpretazioni in cui $\&\Gamma$ è falsa, sicuramente $\&\Gamma \to A$ è vera. Consideriamo quindi il caso in cui $\&\Gamma$ risulta vera. In questo caso sia B che C devono essere vere perchè $\&\Gamma \to B$ e $\&\Gamma \to C$ sono tautologie; di conseguenza anche $B \wedge C$ è vera. Quindi anche in questo caso $\&\Gamma \to A$ risulta vera.

   (b) Se l'ultima regola usata è una di $\wedge$-eliminazione, allora la prova è del tipo

$$\frac{\begin{array}{c}\Gamma \\ \vdots \\ A \wedge B\end{array}}{A}$$

   per qualche B. Per ipotesi induttiva, $\&\Gamma \to (A \wedge B)$ è una tautologia. Pertanto, nelle interpretazioni in cui $\&\Gamma$ è vera, anche $A \wedge B$ è vera e quindi A. In altre parole, $\&\Gamma \to A$ è una tautologia.

   (c) Nel casi in cui l'ultima regola sia una di $\vee$-introduzione, la prova è del tipo

$$\frac{\begin{array}{c}\Gamma \\ \vdots \\ B\end{array}}{B \vee C}$$

   con $A = (B \vee C)$. Per ipotesi induttiva, $\&\Gamma \to B$ è una tautologia; cioè, ogni volta che $\&\Gamma$ è vera, anche B lo è e, quindi, anche A. Pertanto, $\&\Gamma \to A$ è una tautologia.

(d) Nell caso in cui l'ultima regola usata è quella di $\vee$-eliminazione, la prova appare così:

$$\frac{\begin{array}{c}\Gamma,[B]'\\ \vdots\\ A\end{array}\quad \begin{array}{c}\Gamma,[C]'\\ \vdots\\ A\end{array}\quad \begin{array}{c}\Gamma\\ \vdots\\ B\vee C\end{array}}{A}\ {}'$$

con B e C ipotesi momentanee. Per ipotesi induttiva, si ha che le formule $(\&\Gamma \wedge B) \to A$, $(\&\Gamma \wedge C) \to A$ e $\&\Gamma \to (B \vee C)$ sono tutte tautologie. Se adesso supponiamo $\&\Gamma$ vera, dalla terza tautologia segue che almeno una fra B e C deve essere pure vera; in entrambi i casi, le prime due tautologia danno che A deve essere vera. Quindi $\&\Gamma \to A$ è una tautologia.

(e) Supponiamo adesso che l'ultima regola applicata sia quella di $\to$-introduzione, quindi $A = (B \to C)$ e la prova di $\Gamma \vdash A$ appare così:

$$\frac{\begin{array}{c}\Gamma,[B]'\\ \vdots\\ C\end{array}}{B \to C}\ {}'\ .$$

Per ipotesi induttiva, la formula $(\&\Gamma \wedge B) \to C$ è una tautologia; in altre parole, se $\&\Gamma$ e B sono entrambe vere allora anche C è vera. Noi vogliamo provare che $\&\Gamma \to (B \to C)$ è una tautologia. Al solito, se $\&\Gamma$ è falsa allora l'implicazione è automaticamente vera. Se $\&\Gamma$ è vera, ma B è falsa, allora $B \to C$ è vera e, quindi, anche la formula che a noi interessa risulta vera. Infine, se $\&\Gamma$ e B sono entrambe vere allora, per quanto detto sopra, anche C è vera e, quindi, anche $B \to C$ e $\&\Gamma \to (B \to C)$ sono vere.

(f) Supponiamo che l'ultima regola nella derivazione di $\Gamma \vdash A$ sia quella di $\to$-eliminazione:

$$\frac{\begin{array}{c}\Gamma\\ \vdots\\ B\end{array}\quad \begin{array}{c}\Gamma\\ \vdots\\ B\to A\end{array}}{A}$$

per qualche B e C in Frm. L'ipotesi induttiva ci assicura che $\&\Gamma \to B$ e $\&\Gamma \to (B \to A)$ sono entrambe tautologia. Se $\&\Gamma$ è vero allora sia B che $B \to A$ devono essere vere, quindi A deve necessariamente essere vera.

(g) Infine, consideriamo il caso della regola di riduzione all'assurdo.

$$\dfrac{\begin{array}{cc} \Gamma & [\neg\, A]' \\ & \vdots \\ & \perp \end{array}}{A} \, ,$$

Per provare che $\&\Gamma \to A$ è una tautologia, basta far vedere che è impossibile che $\&\Gamma$ sia vera, ma A falsa. Infatti, se $\&\Gamma$ fosse vera e A falsa, allora sia $\&\Gamma$ che $\neg\, A$ sarebbero vere e, per ipotesi induttiva, seguirebbe che $\perp$ dovrebbe essere vera.

c.v.d.

4.3 Teorema di completezza: dimostrazione.

Prima di potere dimostrare il teorema abbiamo bisogno di provare due lemmi.

Lemma 4.4 *Se* $\Gamma, B \vdash A$ *e* $\Gamma, \neg\, B \vdash A$ *sono entrambi dimostrabili allora anche* $\Gamma \vdash A$ *lo è.*

Dim:

$$\dfrac{\begin{array}{ccc} \Gamma, [B]' & \Gamma, [\neg\, B]' & \\ \vdots & \vdots & \vdots \\ A & A & B \vee \neg\, B \end{array}}{A} \, ,$$

c.v.d.

Nel prossimo lemma useremo la seguente notazione. Data una formula A e fissata una particolare interpretazione, definiamo $\widetilde{A}$ essere A stessa, se A risulta vera nell'interpretazione fissata, $\neg\, A$ in caso contrario.

Lemma 4.5 *Sia* A *una formula e sia* $P_A = \{p_1, \ldots, p_n\}$ *la lista delle formule atomiche che compaiono in* A. *Sia fissata, inoltre, un'interpretazione e sia* $\widetilde{P_A}$ *l'insieme delle formule* $\widetilde{p_i}$. *Sotto queste premesse, è dimostrabile che* $\widetilde{P_A} \vdash \widetilde{A}$.

Dim: Per induzione sulla complessità n della formula A.

1. Se $n = 0$, cioè A è una formula atomica, allora $P_A = \{A\}$ e la tesi diventa $\widetilde{A} \vdash \widetilde{A}$ che è banalmente vera.

2. Supponiamo che il lemma sia vero per formule di complessità minore di n e dimostriamolo per n. Distinguiamo tre casi a seconda che A sia del tipo $B \wedge C$, o $B \vee C$, o $B \to C$. In tutti questi casi, è ovvio che le formule atomiche che compaiono in A si ottengono facendo l'unione fra quelle di B e quelle di C; in simboli $P_A = P_B \cup P_C$. In ogni caso, per l'ipotesi induttiva, si ha $\widetilde{P_B} \vdash \widetilde{B}$ e $\widetilde{P_C} \vdash \widetilde{C}$.

   ($A = B \wedge C$) Se B e C sono entrambe vere (nell'interpretazione fissata) allora $\widetilde{B} = B$, $\widetilde{C} = C$ e $\widetilde{A} = B \wedge C$. Da $\widetilde{P_B} \vdash \widetilde{B}$ segue $\widetilde{P_B} \vdash B$ e, a maggior ragione, $\widetilde{P_A} \vdash B$. Similmente $\widetilde{P_A} \vdash C$ e quindi $\widetilde{P_A} \vdash B \wedge C$ per $\wedge$-introduzione.

   Se, invece, B è falso allora $\widetilde{A} = \neg (B \wedge C)$. Il seguente albero prova che $\widetilde{P_B} \vdash \neg (B \wedge C)$

$$\dfrac{\dfrac{\dfrac{[B \wedge C]'}{B} \qquad \begin{matrix}\widetilde{P_B}\\ \vdots \\ \neg B\end{matrix}}{\perp}}{\neg (B \wedge C)},$$

   grazie all'ipotesi induttiva; di conseguenza anche $\widetilde{P_A} \vdash \widetilde{A}$. Analogamente se C è falso.

   ($A = B \vee C$) Se almeno una fra B e C risulta vera allora $\widetilde{A} = B \vee C$. Ad esempio, se B è vera allora $\widetilde{P_B} \vdash B$ e quindi $\widetilde{P_A} \vdash B \vee C$ per $\vee$-introduzione. Similmente se è C ad essere vera.

   Se, invece, sia B che C sono false allora l'albero

$$\dfrac{\dfrac{\dfrac{[B]^1 \qquad \begin{matrix}\widetilde{P_B}\\ \vdots \\ \neg B\end{matrix}}{\perp} \qquad \dfrac{[C]^1 \qquad \begin{matrix}\widetilde{P_C}\\ \vdots \\ \neg C\end{matrix}}{\perp} \qquad [B \vee C]^2}{\perp}\,1}{\neg (B \vee C)}\,2$$

   dimostra che $\widetilde{P_A} \vdash \widetilde{A}$.

$(A = B \to C)$ I due alberi

$$\dfrac{\begin{matrix}\widetilde{P}_C\\ \vdots\\ C\end{matrix}}{B \to C} \qquad \dfrac{\dfrac{\dfrac{[B]' \quad \begin{matrix}\widetilde{P}_B\\ \vdots\\ \neg B\end{matrix}}{\bot}}{C}}{B \to C}\ ,$$

dimostrano che $\widetilde{P}_A \vdash \widetilde{A}$ sia se C è vero che se B è falso. Il caso in cui B sia vera, ma C falsa, cioè $\widetilde{B} = B$, $\widetilde{C} = \neg C$ e quindi $\widetilde{A} = \neg (B \to C)$, è provato dal seguente albero.

$$\dfrac{\dfrac{\dfrac{\begin{matrix}\widetilde{P}_B\\ \vdots\\ B\end{matrix} \quad [B \to C]'}{C} \qquad \begin{matrix}\widetilde{P}_C\\ \vdots\\ \neg C\end{matrix}}{\bot}}{\neg (B \to C)}\ ,$$

c.v.d.

Adesso siamo pronti, finalmente, a provare il teorema di completezza, cioè:

$$\models A \qquad \Longrightarrow \qquad \vdash A$$

per ogni formula A.

Dim: Siano $p_1, \ldots, p_n$ le formule atomiche che compaiono in A. Il lemma precedente ci assicura che $\widetilde{p}_1, \ldots, \widetilde{p}_n \vdash \widetilde{A}$ per ognuna delle 2^n (classi di) interpretazioni di A. Per ipotesi A è vera in ogni interpretazione, quindi $\widetilde{A}$ è sempre uguale ad A. Pertanto abbiamo le 2^n condizioni:

$$\begin{array}{c}
p_1, \ldots, \quad p_{n-1}, \quad p_n \vdash A\ ; \\
p_1, \ldots, \quad p_{n-1}, \neg p_n \vdash A\ ; \\
p_1, \ldots, \neg p_{n-1}, \quad p_n \vdash A\ ; \\
p_1, \ldots, \neg p_{n-1}, \neg p_n \vdash A\ ; \\
\vdots \qquad \vdots \qquad \vdots \qquad \vdots\ ; \\
\neg p_1, \ldots, \neg p_{n-1}, \quad p_n \vdash A\ ;
\end{array}$$

$$\neg\, p_1, \ldots, \neg\, p_{n-1}, \neg\, p_n \vdash A\ .$$

Dalle prime due, per il primo lemma di questa sezione, segue

$$p_1, \ldots, p_{n-1} \vdash A\ ;$$

dalla terza e la quarta segue

$$p_1, \ldots, \neg\, p_{n-1} \vdash A$$

e cosi via fino a

$$\neg\, p_1, \ldots, \neg\, p_{n-1} \vdash A$$

che segue dalle ultime due. Pertanto dopo n applicazioni del primo lemma ci ritroviamo con 2^{n-1} condizioni. Ripetendo il procedimento se ne ottengono 2^{n-2} e così via. Dopo $n-1$ passaggi si arriva alle due condizioni

$$p_1 \vdash A \qquad \text{e} \qquad \neg\, p_1 \vdash A$$

dalle quali, applicando per l'ultima volta il primo lemma, segue $\vdash A$. c.v.d.

Parte II

La logica dei predicati

Capitolo 5

Linguaggi del primo ordine

Lo scopo principale della logica dei predicati è la formalizzazione delle frasi del linguaggio naturale in cui compaiono dei quantificatori, cioè delle espressioni del tipo "per ogni", "tutti", "alcuni" e così via. Esistono diverse logiche dei predicati a seconda dell'insieme di elementi ai quali si applicano i quantificatori: se si quantifica *solo* su elementi di un certo dominio si parla di logica del primo ordine; se la quantificazione viene estesa *anche* a proprietà degli elementi (o, equivalentemente, a sottoinsiemi) allora la logica corrispondente viene detta del secondo ordine e così via. Ad esempio, la frase "ogni numero reale non nullo ammette inverso" è formalizzabile al primo ordine, mentre "ogni sottoinsieme non vuoto dei reali che sia limitato superiormente ammette estremo superiore" ha bisogno della logica del secondo ordine.

In questo e nei prossimi capitoli verrà trattata esclusivamente la logica dei predicati (classica) del *primo* ordine. Il motivo è che la logica del primo ordine ha proprietà migliori rispetto a quelle di ordine superiore: ad esempio è possibile descriverla tramite un insieme finito (o comunque ricorsivo) di regole e assiomi.

Per cominciare, analizziamo il seguente esempio: "il quadrato di un numero reale non nullo è sempre positivo". Di solito esso viene scritto simbolicamente così:

$$(\forall x \in \mathbb{R})(x \neq 0 \rightarrow x^2 > 0) \ .$$

In questo esempio compaiono tutti gli elementi tipici di un linguaggio predicativo del primo ordine: $\forall$ (leggi "per ogni") è un quantificatore; x è una variabile, cioè un generico elemento del dominio (che , in questo caso, è $\mathbb{R}$); 0 è una costante, cioè un elemento particolare del dominio; $>$ è una relazione, cioè un predicato binario; anche $=$ è un predicato binario, ma ha un ruolo particolare, come vedremo; infine, x^2 è una funzione (unaria). In generale, quindi, possiamo dare la seguente definizione.

Definizione 5.1 *Un* linguaggio *predicativo del primo ordine è un insieme che contiene i seguenti elementi:*

- *una quantità infinita (anche non numerabile) di variabili, in genere indicate con $x_1, \ldots, x_n, \ldots$ o, anche, con $x, y, z, \ldots$;*
- *un numero arbitrario (anche infinito) di costanti $a, b, c, \ldots$;*
- *un numero arbitrario (anche infinito) di funzioni $f, g, \ldots$ ognuna con la sua molteplicità (o* arietà*);*
- *un numero arbitrario (anche infinito) di predicati $P, Q, \ldots$ ognuna con la sua molteplicità (o* arietà*);*
- *i connettivi e il simbolo per il falso;*
- *i due quantificatori $\forall$ e $\exists$;*
- *le parentesi.*

Una sequenza arbitraria di simboli del linguaggio è un'espressione. Ovviamente non tutte le espressioni hanno senso, cioè sono *ben formate.* Ci sono due tipi di espressioni ben formate: quelle che descrivono degli elementi del dominio (termini) e quelle che esprimono delle frasi (formule).

Definizione 5.2 *Sia $\mathcal{L}$ un linguaggio.*

- *L'insieme dei termini sul linguaggio $\mathcal{L}$, indicato con $Trm_{\mathcal{L}}$ (o, semplicemente, con Trm) è definito per ricorsione dalle seguenti clausole:*
  - *ogni variabile è un termine;*
  - *ogni costante è un termine;*
  - *se $t_1, \ldots, t_n \in Trm$ e f è un simbolo di funzione n-aria di $\mathcal{L}$ allora anche $f(t_1, \ldots, t_n) \in Trm$.*
- *L'insieme delle formule sul linguaggio $\mathcal{L}$, indicato con $Frm_{\mathcal{L}}$ (o, semplicemente, con Frm) è definito per ricorsione dalle seguenti clausole:*

– $\bot \in Frm$;

– *se* $t_1, \ldots, t_n \in Trm$ *e* P *è un simbolo di predicato* n*-ario di* $\mathcal{L}$ *allora* $P(t_1, \ldots, t_n) \in Frm$;

– *se* $A, B \in Frm$ *allora* $(A \wedge B), (A \vee B), (A \to B) \in Frm$;

– *se* $A \in Frm$ *e* x *è una variabile allora* $(\forall x A)$ *e* $(\exists x A)$ *sono formule.*

Le formule del tipo $P(t_1, \ldots, t_n)$, con P predicato n-ario e $t_1, \ldots, t_n$ termini, vengono chiamate *atomiche* [1], perchè non contengono né connettivi, né quantificatori quindi non sono ulteriormente scomponibili.

Come esempio, consideriamo il linguaggio $\mathcal{L} = \{\cdot, e, ^{-1}\}$ della teoria dei gruppi (è sottinteso che $\mathcal{L}$ contiene le variabili e l'=), dove: $\cdot$ è un operazione (cioè una funzione binaria), $^{-1}$ è una funzione unaria, mentre e è una costante (elemento neutro). In questo linguaggio, l'espressione $) \cdot x \to \bot$ non è ben formata, $(x \cdot e)^{-1}$ è un termine e $(\forall x (\exists y (x \cdot y = e)))$ è una formula.

Per evitare troppe parentesi adottiamo la seguente convenzione: hanno precedenza i quantificatori e la negazione, poi vengono la congiunzione e la disgiunzione, infine l'implicazione. Ad esempio la formula

$$\forall x \neg A(x) \to \exists y B(y) \vee C$$

è un'abbreviazione per:

$$(\forall x (A(x) \to \bot)) \to ((\exists y B(y)) \vee C) \ .$$

5.1 Variabili libere e variabili legate

Le variabili vengono usate nella pratica matematica con due funzioni diverse. Per esempio, nell'espressione

$$F(x) = \int_0^x f(t) \ \mathrm{d}t$$

possiamo sostituire ad x un valore particolare, ad esempio 1; otteniamo così il numero $F(1)$. Invece non possiamo sostituire un numero al posto della variabile t; infatti, se per esempio sostituiamo 1 al posto di t otteniamo

[1] Alcuni autori includono $\bot$ fra le formule atomiche, ma noi preferiamo non farlo.

$\int f(1)\ \mathrm{d}1$ che è un'espressione priva di senso. In questo caso, si dice che la variabile x è *libera*, mentre la variabile t è *legata* (o, semplicemente, *non libera*).

Vediamo un altro esempio nel caso che più ci interessa: quello della logica dei predicati. Nella formula:

$$\forall x(P(x,y) \wedge \exists z Q(x,z))$$

la y è una variabile libera, mentre x e z non lo sono; infatti, se sostituisco a y una costante, ad esempio un numero, la formula risultante continua ad avere senso.

In una formula è possibile cambiare il nome delle variabili legate senza con ciò cambiare il significato globale della formula, come dimostreremo nel prossimo capitolo. Ad esempio, l'espressione $\int f(x)\ \mathrm{d}x$ è equivalente a: $\int f(t)\ \mathrm{d}t$.

Una formula in cui non compaiono variabili libere (cioè in cui tutte le variabili sono legate) viene detta *chiusa*. Viceversa, una formula contenente almeno una variabile libera si dice *aperta*.

Capitolo 6

Semantica: interpretazioni.

In questo capitolo definiremo in maniera formale il concetto di verità di una formula. Tutti abbiamo un'idea intuitiva di cosa significhi "verità". Ad esempio siamo tutti d'accordo a ritenere che $1+1=2$, a condizione che questi simboli siano usati con il loro significato solito. La questione si complica un po' quando, come nel caso della logica, si vogliono usare dei simboli in maniera astratta senza riferimento ad una loro *interpretazione* fissata. Per esempio, come si fa a capire se la formula

$$\forall x\ [f(x,y) = a \to P(x)]$$

è vera o falsa? Dovrebbe essere chiaro che la domanda non è ben posta. Infatti per indagare la verità di una formula abbiamo bisogno di conoscere il significato dei simboli che in essa compaiono, cioè abbiamo bisogno di fare un'*interpretazione*. Qundi dobbiamo sapere: chi è l'insieme di cui stiamo parlando, chi è la costante a, chi è la funzione $f(x,y)$ e, infine, chi è il predicato $P(x)$. In realtà, serve pure conoscere il valore di y. Supponiamo, per esempio, che l'insieme di cui stiamo parlando sia $\mathbb{R}$ (l'insieme dei numeri reali) e che a sia il numero 1; supponiamo, inoltre che la funzione f sia l'operazione di prodotto e che $P(x)$ significhi "x è diverso da zero". Sotto queste ipotesi la fase diventa: "preso un $x \in \mathbb{R}$, se $x \cdot y = 1$ allora x è diverso da zero" che, ovviamente, è una frase vera (a prescindere da chi sia y). Se, invece, prendiamo $a = 0 = y$ la frase diventa: "preso un $x \in \mathbb{R}$, se $x \cdot 0 = 0$ allora x è diverso da zero" che è falsa.

Riassumendo, la verità di una formula dipende dall'interpretazione dei simboli che compaiono nelle formula e (se la formula è aperta) dal valore (*assegnazione*) delle variabili libere che in essa compaiono.

Definizione 6.1 *Sia $\mathcal{L}$ un linguaggio e sia Var l'insieme delle variabili di $\mathcal{L}$. Un'*interpretazione *è costituita da:*

- *un insieme non vuoto D (*dominio *dell'interpretazione);*
- *una funzione $\sigma : Var \longrightarrow D$ (*assegnazione di variabili*);*
- *una costante $a_D \in D$ per ognuna delle costanti a di $\mathcal{L}$;*
- *una funzione n-aria $f_D : D^n \longrightarrow D$ per ognuna delle funzioni n-arie f di $\mathcal{L}$ (per ogni n);*
- *un predicato n-ario P_D (cioè un sottoinsieme di D^n) per ognuno dei predicati n-ari P di $\mathcal{L}$ (per ogni n).*

Ogni assegnazione di variabili può essere estesa in modo naturale ad una funzione da $Trm_{\mathcal{L}}$ in D. Ad esempio se $D = \mathbb{N}$, $a_D = 1$ e $f_D(x, y) = x + y$ allora al termine $f(x, f(x, a))$ viene assegnato il valore $\sigma(x) + (\sigma(x) + 1)$ (che ovviamente dipende dall'assegnazione σ). Per comodità, la funzione su Trm che si ottiene estendendo σ la indicheremo pure con σ.

A questo punto è possibile definire la verità (o *valutazione*) di una formula. Per comodità, scriviamo D, σ per indicare un'interpretazione, sottintendendo le costanti, le funzioni e i predicati.

Definizione 6.2 *Sia D, σ un'interpretazione relativa ad un linguaggio $\mathcal{L}$. Si dice* valutazione *(rispetto all'interpretazione D, σ) la funzione*

$$val : Frm_{\mathcal{L}} \longrightarrow \{V, F\}$$

definita ricorsivamente dalle seguenti clausole:

- *$val(\perp) = F$;*
- *se $P(t_1, \ldots, t_n)$ è una formula atomica, allora: $val(P(t_1, \ldots, t_n)) = V$ se e solo se $P_D(\sigma(t_1), \ldots, \sigma(t_n))$ è vera;*
- *$val(A \wedge B) = V$ se e solo se $val(A) = V$ e $val(B) = V$;*
- *$val(A \vee B) = V$ se e solo se $val(A) = V$ e/o $val(B) = V$;*
- *$val(A \rightarrow B) = V$ se e solo se $val(A) = F$ e/o $val(B) = V$;*[1]

[1] In altre parole, nel caso in cui il segno principale di una formula sia un connettivo, basta guardare la tavola di verità del connettivo in questione.

- *$val(\forall x\ A(x)) = V$ se, presa comunque un'altra assegnazione di variabile σ' diversa da σ al massimo solo su x, si ha che $val'(A(x)) = V$ essendo val' la valutazione relativa a D, σ';*[2]

- *$val(\exists x\ A(x)) = V$ se è possibile trovare un'altra assegnazione di variabile σ', diversa da σ al massimo solo su x, tale che $val'(A(x)) = V$, dove val' è la valutazione relativa a D, σ'.*

Per comodità, se $\Gamma \subseteq Frm$, scriveremo $val(\Gamma) = V$ per esprimere che $val(C) = V$ per ogni $C \in \Gamma$. Se $val(\Gamma) = V$ si dice che l'insieme di formule Γ è *valido* (o *vero*) nell'interpretazione D, σ e l'interpretazione D, σ viene detta un *modello* di Γ.

Definizione 6.3 *Siano $A \in Frm$ e $\Gamma \subseteq Frm$.*

- *A si dice* logicamente *(o* universalmente*)* valida *(o, semplicemente,* valida*) se è valida in tutte le interpretazioni;*

- *Γ si dice* soddisfacibile *se ha almeno un modello.*

Definizione 6.4 *Due formule A e B si dicono (semanticamente)* equivalenti*, e si scrive $A \equiv B$, se $val(A) = val(B)$ in ogni interpretazione D, σ.*

Se $A \in Frm$ e $\Gamma \subseteq Frm$, si scrive $\Gamma \models A$ (che si legge "A è una conseguenza di Γ" o "da Γ segue A") se in ogni interpretazione in cui $val(\Gamma) = V$ anche $val(A) = V$.

Ovviamente, $A \equiv B$ si può vedere come un'abbreviazione di "$A \models B$ e $B \models A$".

Proposizione 6.5 *Per ogni $A \in Frm$ e per ogni $x, y \in Var$, si ha che $\forall x A(x) \equiv \forall y A(y)$ e che $\exists x A(x) \equiv \exists y A(y)$.*

Dim: Cominciamo dal caso del $\forall$; ovviamente è sufficiente dimostrare che $\forall x A(x) \models \forall y A(y)$, essendo x e y arbitrari. Sia D, σ un'interpretazione in cui $val(\forall x A(x)) = V$; cioè $val'(A(x)) = V$ in ogni interpretazione D, σ' con σ' che differisce da σ solo (al massimo) su x. Dobbiamo dimostrare che

[2] È un modo formale per dire che $A(x)$ è vera qualsiasi cosa sostituiamo al posto di x, senza però toccare le altre variabili.

$val(\forall y A(y)) = V$ in D, σ, cioè che $val''(A(y)) = V$ in ogni interpretazione D, σ'' con σ'' che differisce da σ solo (al massimo) su y. Pertanto fissiamo una qualsiasi assegnazione σ'' e scegliamo σ' tale che $\sigma'(x) = \sigma''(y)$. Allora $val'(A(x)) = V$ per ipotesi; cioè $A(x)$ è vera quando sostituiamo $\sigma'(x)$ al posto di x, cioè $A(x)$ è vera quando sostituiamo $\sigma''(y)$ al posto di x. In altre parole, $A(y)$ è vera quando sostituiamo $\sigma''(y)$ al posto di y; cioè $val''(A(y)) = V$.

Il caso dell'$\exists$ è molto simile. Per ipotesi sappiamo che $val'(A(x)) = V$ per qualche σ' e dobbiamo provare che $val''(A(y)) = V$ per qualche σ''. Basta porre $\sigma''(y) = \sigma'(x)$. c.v.d.

Questa proposizione ci permette di cambiare a piacimento il nome delle variabili legate. Quindi possiamo supporre che ogni quantificatore presente in una formula si riferisca ad una variabile che né è quantificata da altri quantificatori, né compare libera. Ad esempio, nella formula

$$A(x) \wedge \forall x B(x) \rightarrow \exists x C(x)$$

la variabile x assume tre ruoli diversi contemporaneamente: è libera, è legata dal $\forall$ ed è legata dall'$\exists$. Sappiamo che cambiando nome alle variabili legate otteniamo una formula equivalente. Per convenzione, scegliamo i nomi delle variabili legate in modo che una stessa variabile non compaia legata da più di un quantificatore. Ad esempio, possiamo riscrivere la formula data come:

$$A(x) \wedge \forall y B(y) \rightarrow \exists z C(z) \ .$$

Questo ci permetterà di evitare noiose distinzioni; quindi, nel seguito, supporremo sempre che ogni variabile legata sia diversa da quelle libere e appaia legata ad un solo quantificatore.

Esempio 6.6 *Se $t \in Trm$, la formula $\forall x A(x) \rightarrow A(t)$ è valida.*

Soluzione. Grazie alla proposizione precedente, possiamo supporre che x non compaia in t. Dobbiamo fare vedere che la formula è valida in ogni interpretazione. Pertanto fissiamo un'interpretazione D, σ arbitraria. Se succede che $val(\forall x\ A(x)) = F$ abbiamo finito. Sia, quindi, $val(\forall x\ A(x)) = V$. Questo significa che $val'(A(x)) = V$ in ogni interpretazione D, σ' con σ' che differisce da σ solo (al massimo) su x. Scegliamo σ' tale che $\sigma'(x) = \sigma(t)$ $(\in D)$. Allora $val'(A(x)) = V$ significa che $A(x)$ è vera quando sostituiamo $\sigma'(x) = \sigma(t)$ al posto di x, cioè precisamente che $val(A(t)) = V$. $\square$

Esempio 6.7 *Se $t \in Trm$, la formula $A(t) \to \exists x A(x)$ è valida.*

Soluzione. Simmetrica rispetto alla precedente. □

Proposizione 6.8 *Sia $A(x)$ una formula che contiene x come variabile libera. Allora:*

- *$A(x)$ è valida se e solo se $\forall x A(x)$ è valida;*
- *$A(x)$ è soddisfacibile se e solo se $\exists x A(x)$ è soddisfacibile.*

Dim: Sia D, σ un'interpretazione arbitraria; vogliamo provare che $\forall x A(x)$ è valida in tale interpretazione. Pertanto, sia σ' un'assegnazione che differisce da σ solo su x. Per ipotesi $A(x)$ è (universalmente) valida; in particolare è valida in D, σ', cioè $A(\sigma'(x))$ è vera in D. Viceversa, dal fatto che $\forall x A(x)$ è valida segue, in particolare, che $A(\sigma(x))$ è vera in D; cioè $A(x)$ è valida in D, σ, con D, σ arbitraria.

Se D, σ è un'interpretazione in cui $A(x)$ è valida allora $A(\sigma(x))$ è vera in D; quindi anche $\exists x A(x)$ è valida in D, σ. Viceversa, se $\exists x A(x)$ è valida in D, σ allora esiste una σ' tale che $A(\sigma'(x))$ è vera in D e quindi $A(x)$ è valida in D, σ'. c.v.d.

Definizione 6.9 *Sia $A(x_1, \ldots, x_n)$ una formula le cui variabili libere sono $x_1, \ldots, x_n$. Allora:*

- *la formula $\forall x_1 \cdots \forall x_n A(x_1, \ldots, x_n)$ viene detta la* chiusura universale *di A;*
- *la formula $\exists x_1 \cdots \exists x_n A(x_1, \ldots, x_n)$ viene detta la* chiusura esistenziale *di A.*

La proposizione precedente ci dice che una formula è valida se e solo se è valida la sua chiusura universale, mentre è soddisfacibile se e solo se lo è la sua chiusura esistenziale.

Capitolo 7

Sintassi: deduzione naturale per la logica predicativa.

In questo capitolo amplieremo il calcolo della deduzione naturale aggiungendo altre quattro regole relative ai quantificatori $\forall$ e $\exists$. Come ci si può aspettare, due regole saranno di introduzione e due di eliminazione.

7.1 Le regole per i quantificatori

I due esempi a conclusione del capitolo precedente suggeriscono di dare le due seguenti regole:

$$\frac{\forall x A(x)}{A(t)}\ \forall\text{-eliminazione} \qquad\qquad \frac{A(t)}{\exists x A(x)}\ \exists\text{-introduzione}$$

dove t è un termine (quasi) qualsiasi.[1] Più difficile è capire quali debbano essere le regole di $\forall$-introduzione e di $\exists$-eliminazione. Concentriamoci, per il momento, sul caso del $\forall$. Vogliamo una regola che abbia $\forall x A(x)$ come conclusione; allora ci chiediamo: come si fa di solito a dimostrare una frase

[1] Queste due apparentemente semplici regole presentano delle insidie nascoste. Supponiamo che sia vera la formula $\forall x \exists y P(x, y)$ e applichiamo $\forall$-eliminazione con il termine $t = y$; otteniamo $\exists y P(y, y)$ che non è detto che sia vera. Quindi, se t contiene variabili, ad esempio y, che compaiono legate in $A(x)$ dobbiamo prima cambiare nome a quest'ultime. Nell'esempio in questione, prima dobbiamo riscrivere l'ipotesi come $\forall x \exists z P(x, z)$ e poi possiamo sostituire t, cioè y, al posto di x e otteniamo: $\exists z P(y, z)$. Si dice che il termine t deve essere *libero per x in $A(x)$*.

di questo tipo? Il modo più naturale è dimostrare $A(x)$, qualsiasi sia x. In altre parole, dimostrare $\forall x A(x)$ equivale a dimostrare $A(x)$ senza avere alcuna ipotesi particolare su x. Questo può essere scritto formalmente così:

$$\dfrac{\begin{array}{c}\Gamma \\ \vdots \\ A(z)\end{array}}{\forall x A(x)}\ \scriptstyle{\forall\text{-introduzione}} \qquad (z \text{ non libero in } \Gamma)$$

cioè: se riusciamo a dimostrare $A(z)$ partendo dalle ipotesi Γ che non contengono informazioni su z, allora vuol dire che $A(z)$ vale per uno z arbitrario. Similmente, la regole di eliminazione dell'$\exists$ sarà:

$$\dfrac{\begin{array}{c}\Gamma, [A(z)]' \\ \vdots \\ B\end{array} \qquad \exists x A(x)}{B}\ {}'\ \scriptstyle{\exists\text{-eliminazione}} \qquad (z \text{ non libero in } \Gamma, B)$$

che significa: per dimostrare B partendo da $\exists x A(x)$, devo riuscire a farlo qualsiasi sia lo z che soddisfa $A(z)$.

Similmente al caso proposizionale, dati $\Gamma \subseteq Frm$ e $A \in Frm$, si scrive

$$\Gamma \vdash A$$

(e si legge "A è dimostrabile a partire dalle ipotesi Γ" o "da Γ si può derivare A") quando esiste una dimostrazione formale (cioè un albero) che ha come conclusione (cioè come radice) la formula A e le cui ipotesi (cioè le foglie non scaricate) sono formule appartenenti a Γ [2]. Nel caso in cui $\Gamma \vdash \bot$ è dimostrabile, si dice che l'insieme Γ è *contraddittorio*; si dice non contraddittorio, o *consistente*, in caso contrario.

Al solito si può definire un'equivalenza sintattica (che per comodità indicheremo con lo stesso simbolo di quella semantica) ponendo:

$$A \equiv B \qquad \text{se e solo se} \qquad A \vdash B \text{ e } B \vdash A$$

$(A, B \in Frm)$.

Dal fatto che ogni dimostrazione formale è un albero *finito* (e quindi ha un numero finito di foglie) segue immediatamente il seguente importante teorema.

[2] Non necessariamente tutte le formule di Γ devono comparire (Γ potrebbe essere infinito).

Teorema 7.1 (di finitezza) *Per ogni $\Gamma \subseteq Frm$ e $A \in Frm$, $\Gamma \vdash A$ è dimostrabile se e solo se esiste un sottoinsieme finito di Γ, diciamo K, tale che sia dimostrabile $K \vdash A$.*

Dim: Un verso è banale. Per l'altro verso, basta prendere come K l'insieme delle formule che compaiono come foglie (non scaricate) nell'albero di una prova di $\Gamma \vdash A$. c.v.d.

7.2 Esempi

Esempio 7.2 *Dimostrare che: $\neg \forall x A(x) \vdash \exists x \neg A(x)$, per ogni formula A.*

Soluzione.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{[\neg A(z)]^1}{\exists x \neg A(x)} \quad [\neg \exists x \neg A(x)]^2}{\bot}}{A(z)}\,{}^{1}}{\forall x A(x)} \qquad \neg \forall x A(x)}{\bot}}{\exists x \neg A(x)}\,{}^{2}$$

Con z libero per x in $A(x)$. □

Esempio 7.3 *Dimostrare che: $\forall x(A(x) \vee B) \vdash \forall x A(x) \vee B$ (se x non compare libera in B).*

Soluzione. Grazie a opportuni teoremi delle logica proposizionale è sufficiente provare che $\forall x(\neg B \to A(x)) \vdash \neg B \to \forall x A(x)$ che è facilissimo.

$$\dfrac{\dfrac{\dfrac{[\neg B]^1 \quad \dfrac{\forall x(\neg B \to A(x))}{\neg B \to A(z)}}{A(z)}}{\forall x A(x)}}{\neg B \to \forall x A(x)}\,{}^{1}$$

Con z libero per x in A. □

Capitolo 8

Il teorema di completezza per la logica del primo ordine

In questo capitolo proveremo il teorema di (validità e) completezza per il calcolo della deduzione naturale nel caso predicativo. L'enunciato del teorema è il seguente.

Teorema 8.1 *Sia $\mathcal{L}$ un linguaggio del primo ordine. Allora:*

$$\Gamma \vdash A \qquad \textit{se e solo se} \qquad \Gamma \models A$$

per ogni $A \in Frm_{\mathcal{L}}$ e per ogni $\Gamma \subseteq Frm_{\mathcal{L}}$ (arbitrario, anche infinito).

8.1 La dimostrazione del teorema di validita

Teorema 8.2 (validità)

$$\Gamma \vdash A \qquad \Longrightarrow \qquad \Gamma \models A$$

Dim: Per induzione sula lunghezza n della dimostrazione di $\Gamma \vdash A$.

- Se $n = 0$ allora la dimostrazione di $\Gamma \vdash A$ deve essere del tipo

$$A$$

  e quindi $A \in \Gamma$ (A deve essere sia la conclusione che una delle ipotesi). Dobbiamo provare che $\Gamma \models A$, cioè che $val(A) = V$ in ogni interpretazione tale che $val(C) = V$ per ogni $C \in \Gamma$; ma questo è ovvio dato che $A \in \Gamma$.

- Sia $n > 0$ e supponiamo che il teorema sia vero per tutte le prove di lunghezza minore di n. Distinguiamo 11 casi a seconda dell'ultima regole usata nella dimostrazione di $\Gamma \vdash A$.

  $\wedge$-introduzione . In questo caso $A = B \wedge C$ e la prova di $\Gamma \vdash A$ sarà del tipo

$$\frac{\begin{array}{c}\Gamma\\ \vdots\\ B\end{array} \quad \begin{array}{c}\Gamma\\ \vdots\\ C\end{array}}{A}$$

  dove le prove di $\Gamma \vdash B$ e $\Gamma \vdash C$ avranno lunghezza minore di n e quindi, per ipotesi induttiva, si avrà: $\Gamma \models B$ e $\Gamma \models C$. Consideriamo un'interpretazione in cui $val(\Gamma) = V$; allora anche $val(B) = V = val(C)$ grazie all'ipotesi induttiva. Quindi $val(A) = V$ per la definizione di $val(B \wedge C)$. In altre parole, abbiamo dimostrato che $\Gamma \models A$.

  $\wedge$-eliminazione (per brevità trattiamo assieme il caso a sinistra e quello a destra). La prova sarà del tipo:

$$\frac{\begin{array}{c}\Gamma\\ \vdots\\ A \wedge B\end{array}}{A}$$

  e quindi $\Gamma \models A \wedge B$. Se $val(\Gamma) = V$ allora $val(A \wedge B) = V$ e quindi $val(A) = V$.

  $\vee$-introduzione (sia a destra che a sinistra). Questa volta A sarà del tipo $B \vee C$ con

$$\frac{\begin{array}{c}\Gamma\\ \vdots\\ B\end{array}}{A}$$

  e quindi $\Gamma \models B$. Se $val(\Gamma) = V$ allora $val(B) = V$ e quindi anche $val(A) = V$.

  $\vee$-eliminazione . In questo caso la prova avrà il seguente aspetto:

$$\frac{\begin{array}{c}\Gamma, [B]'\\ \vdots\\ A\end{array} \quad \begin{array}{c}\Gamma, [C]'\\ \vdots\\ A\end{array} \quad \begin{array}{c}\Gamma\\ \vdots\\ B \vee C\end{array}}{A} \; ,$$

con $\Gamma \models B \vee C$, $\Gamma, B \models A$ e $\Gamma, C \models A$ (per ipotesi induttiva). Supponiamo $val(\Gamma) = V$; allora la prima ipotesi ci assicura che $val(B \vee C) = V$. Per definizione, questo significa che $val(B) = V$ oppure $val(C) = V$; in ogni caso le altre ipotesi ci assicurano che $val(A) = V$.

$\rightarrow$-introduzione .

$$\begin{array}{c} \Gamma, [B]' \\ \vdots \\ \dfrac{C}{A} \end{array} ,$$

con $A = B \rightarrow C$. Sia $val(\Gamma) = V$; se $val(B) = F$ allora $val(A) = V$ e abbiamo finito. Se, invece, $val(B) = V$ allora anche $val(C) = V$ grazie all'ipotesi induttiva e possiamo concludere che $val(A) = V$.

$\rightarrow$-eliminazione .

$$\dfrac{\begin{array}{c} \Gamma \\ \vdots \\ B \end{array} \quad \begin{array}{c} \Gamma \\ \vdots \\ B \rightarrow A \end{array}}{A}$$

Da $val(\Gamma) = V$ segue $val(B) = V$, ma anche $val(B \rightarrow A) = V$; quindi deve essere $val(A) = V$.

Riduzione all'assurdo . Avremo:

$$\begin{array}{c} \Gamma, [\neg\, A]' \\ \vdots \\ \dfrac{\bot}{A} \end{array} ,$$

e $\Gamma, \neg\, A \models \bot$. Sia $val(\Gamma) = V$ e supponiamo per assurdo che $val(A) = F$; allora $val(\neg\, A) = V$ e quindi si avrebbe $val(\bot) = V$, che è assurdo.

$\forall$-introduzione . In questo caso abbiamo $A = \forall x B(x)$ e

$$\begin{array}{c} \Gamma \\ \vdots \\ \dfrac{B(z)}{A} \end{array}$$

con z variabile non libera in Γ (cambiando nome alle variabili legate di Γ possiamo supporre che z non compaia in Γ). Al solito, visto che la prova di $\Gamma \vdash B(z)$ ha lunghezza minore di n, l'ipotesi induttiva ci assicura che $\Gamma \models B(z)$. Sia D, σ un'interpretazione in cui $val(\Gamma) = V$ e sia σ' un'assegnazione diversa da σ solo (al più) su x. Dobbiamo provare che $B(\sigma'(x))$ è vera. Consideriamo un'assegnazione σ'' uguale a σ tranne per il fatto che $\sigma''(z) = \sigma'(x)$. In questa nuova interpretazione D, σ'', Γ continuerà ad essere vera (perchè non contiene z) e quindi anche $B(\sigma''(z)) = B(\sigma'(x))$ sarà vera.

$\forall$-eliminazione . Avremo $A = B(t)$ con $t \in Trm$ e

$$\frac{\begin{matrix}\Gamma \\ \vdots \\ \forall x B(x)\end{matrix}}{A}$$

e quindi $\Gamma \models \forall x B(x)$ per ipotesi induttiva. Se $val(\Gamma) = V$ in D, σ allora anche $val(\forall x B(x)) = V$; cioè $B(\sigma'(x))$ è vera qualsiasi sia l'assegnazione σ' uguale a σ tranne (al più) su x. Quindi basta scegliere $\sigma'(x) = t$.

$\exists$-introduzione . Si ha $A = \exists x B(x)$ e

$$\frac{\begin{matrix}\Gamma \\ \vdots \\ B(t)\end{matrix}}{A}$$

con $t \in Trm$. Sia D, σ tale che $val(\Gamma) = V$; allora anche $val(B(t)) = V$ per ipotesi induttiva, cioè $B(\sigma(t))$ è vera. Allora basta porre $\sigma'(x) = \sigma(t)$ (e $\sigma'(y) = \sigma(y)$ per ogni altra $y \in Var$) per avere che esiste un'assegnazione σ' (diversa da σ solo su x) tale che $val(B(x)) = V$ in D, σ'. In altre parole, abbiamo provato che $val(\exists x B(x)) = V$ in D, σ.

$\exists$-eliminazione . La prova sarà del tipo:

$$\frac{\begin{matrix}\Gamma, [B(z)]' \\ \vdots \\ A\end{matrix} \qquad \begin{matrix}\Gamma \\ \vdots \\ \exists x B(x)\end{matrix}}{A}\ ,$$

con z non libero (anzi non presente) in Γ e A. Sia $val(\Gamma) = V$ in una certa interpretazione D, σ. Allora anche $val(\exists x B(x)) = V$ e quindi esiste una σ' (diversa da σ solo su x) tale che $val(B(x)) = V$ in D, σ'. Consideriamo l'interpretazione D, σ'' con $\sigma''(z) = \sigma'(x)$ (e per il resto uguale a σ). Siccome Γ non contiene z, si avrà $val(\Gamma) = V$ anche in D, σ''. Ma in questa interpretazione si avrà anche $val(B(z)) = V$ perchè $val(B(x)) = V$ in D, σ' e $\sigma''(z) = \sigma'(x)$. Quindi $val(A) = V$ in D, σ'' per ipotesi induttiva e $val(A) = V$ anche in D, σ visto che A non contiene z.

c.v.d.

8.2 La prova del teorema di completezza

In questa sezione proveremo il teorema di completezza:

$$\Gamma \models A \qquad \Longrightarrow \qquad \Gamma \vdash A$$

per ogni $A \in Frm$ e $\Gamma \subseteq Frm$. In realtà lo dimostreremo in una forma equivalente.

Proposizione 8.3 *Le seguenti sono equivalenti:*

1. *per ogni* $\Gamma \subseteq Frm$ *e* $A \in Frm$*, se* $\Gamma \models A$ *allora* $\Gamma \vdash A$*;*
2. *per ogni* $\Gamma \subseteq Frm$*, se* $\Gamma \nvdash \bot$ *allora* Γ *è soddisfacibile.*

Dim:

1 $\Rightarrow$ 2). Sia $A = \bot$. Da $\Gamma \models \bot \Longrightarrow \Gamma \vdash \bot$ segue $\Gamma \nvdash \bot \Longrightarrow \Gamma \not\models \bot$. Ma $\Gamma \not\models \bot$ significa che non è vero che tutti i modelli di Γ sono modelli di $\bot$; cioè, esiste un modello di Γ che rende falso $\bot$. Siccome tutte le interpretazioni sono contromodelli di $\bot$, il simbolo $\Gamma \not\models \bot$ significa semplicemente che Γ è soddisfacibile.

2 $\Rightarrow$ 1). Supponiamo $\Gamma \models A$ e supponiamo per assurdo che $\Gamma \nvdash A$. Siccome $\Gamma \vdash A$ è equivalente a $\Gamma, \neg A \vdash \bot$, otteniamo $\Gamma, \neg A \nvdash \bot$. Allora, grazie alla 2, $\Gamma, \neg A$ ammette un modello; cioè esiste un D, σ tale che $val(\Gamma) = V$ e $val(A) = F$ contraddicendo l'ipotesi $\Gamma \models A$. c.v.d.

Quindi, per provare il teorema di completezza, sarà sufficiente dimostrare che ogni sottoinsieme non contraddittorio è soddisfacibile, cioè ha un modello. Ci serviranno alcuni risultati preliminari.

Definizione 8.4 $\Gamma \subseteq Frm$ *si dice* consistente massimale *se:*

1. *Γ è consistente; cioè $\Gamma \nvdash \perp$;*

2. *Γ è massimale; cioè, se $\Gamma' \supsetneqq \Gamma$ allora Γ' è contraddittorio (cioè $\Gamma' \vdash \perp$).*

Proposizione 8.5 *Per ogni Γ consistente, esiste un $\Delta \subseteq Frm$ consistente massimale tale che $\Gamma \subseteq \Delta$ (cioè ogni sottoinsieme consistente può essere esteso ad un sottoinsieme consistente massimale).*

Dim: Si applica il lemma di Zorn (vedi appendice sulla teoria degli insiemi) alla famiglia $F = \{\Gamma' \subseteq Frm \ : \ \Gamma' \text{ è consistente e } \Gamma \subseteq \Gamma'\}$. L'insieme F è un sottoinsieme dell'insieme delle parti di Frm; cioè, $F \subseteq \mathcal{P}(Frm)$. Quindi gli elementi di F sono ordinati parzialmente dall'inclusione. Inoltre F non è vuoto perchè $\Gamma \in F$. Vogliamo provare che ogni catena (cioè sottoinsieme totalmente ordinato) di F è limitato superiormente in F.

Sia $\{\Gamma_i\}_{i\in I}$ una catena di elementi di F. Per dimostrare che è limitata superiormente (in F) basta esibirne un maggiorante (in F). Sia

$$\overline{\Gamma} = \bigcup_{i\in I} \Gamma_i$$

che ovviamente è maggiore di (cioè contiene) tutti gli elementi della catena. Dobbiamo provare, però, che $\overline{\Gamma}$ appartiene ad F. Che $\Gamma \subseteq \overline{\Gamma}$ è ovvio perchè ogni Γ_i contiene Γ. Resta da provare che $\overline{\Gamma}$ è consistente. Supponiamo per assurdo che non lo sia, cioè che $\overline{\Gamma} \vdash \perp$. Allora, per il teorema di finitezza deve esistere un $K \subseteq \overline{\Gamma}$, K finito, tale che $K \vdash \perp$. Ma se K è finito allora deve esistere un $n \in \mathbb{N}$ tale che $K \subseteq \Gamma_n$ (infatti gli elementi di K possono comparire solo in un numero finito di Γ_i e basta prendere il più grande). Allora, da $K \vdash \perp$ seguirebbe $\Gamma_n \vdash \perp$ che è assurdo perchè $\Gamma_n \in F$. In conclusione $\overline{\Gamma} \in F$.

A questo punto il lemma di Zorn ci assicura che esiste un $\Delta \in F$ massimale (secondo l'ordine parziale di F). Ovviamente Δ sarà consistente e conterrà Γ. Vogliamo provare che è consistente massimale.

Sia $\Gamma' \supsetneqq \Delta$ e supponiamo per assurdo che Γ' sia consistente. Allora Γ' apparterrebbe ad F (perchè $\Gamma \subseteq \Delta \subseteq \Gamma'$) che è assurdo, perchè contraddice la massimalità di Δ. c.v.d.

Lemma 8.6 *Sia $\Delta \subseteq Frm$ consistente massimale. Allora da $\Gamma \subseteq \Delta$ e $\Gamma \vdash A$ segue $A \in \Delta$.*

Dim: Supponiamo per assurdo che $A \notin \Delta$. Allora $\Delta \cup \{A\}$ sarebbe contraddittorio, perchè Δ è consistente massimale; cioè si avrebbe $\Delta, A \vdash \perp$ che è equivalente a $\Delta \vdash \neg A$. Ma per ipotesi $\Gamma \vdash A$ con $\Gamma \subseteq \Delta$; quindi anche $\Delta \vdash A$. In definitiva si avrebbe $\Delta \vdash (A \wedge \neg A)$ e quindi $\Delta \vdash \perp$, che e assurdo perchè Δ è consistente. c.v.d.

In particolare, prendendo $\Gamma = \emptyset$, si ottiene che tutte le formule dimostrabili (cioè le A tali che $\vdash A$) appartengono a tutti gli insiemi consistenti massimali.

Un'altra facile conseguenza di questo lemma è che se una formula appartiene ad un certo sottoinsieme consistente massimale, allora ci stanno tutte quelle equivalenti ad essa. Infatti se $A \in \Delta$ e $A \equiv B$ allora $A \vdash B$ e quindi $B \in \Delta$.

Corollario 8.7 *Sia $A \in Frm$ e Δ consistente massimale. Allora o $A \in \Delta$ oppure $\neg A \in \Delta$.*

Dim: Se $A \in \Delta$ abbiamo finito. Se invece $A \notin \Delta$ allora $\Delta \cup \{A\}$ è contraddittorio e quindi $\Delta, A \vdash \perp$. In altre parole si ha $\Delta \vdash \neg A$ e quindi $\neg A \in \Delta$ per il lemma precedente. c.v.d.

Come conseguenza si ha che $A \notin \Delta$ se e solo se $\neg A \in \Delta$.

Proposizione 8.8 *Se $\Delta \subseteq Frm$ è consistente massimale allora:*

1. $\perp \notin \Delta$;
2. $A \wedge B \in \Delta$ *se e solo se* $A \in \Delta$ *e* $B \in \Delta$;
3. $A \vee B \in \Delta$ *se e solo se* $A \in \Delta$ *o* $B \in \Delta$;
4. $A \to B \in \Delta$ *se e solo se* $A \notin \Delta$ *o* $B \in \Delta$;
5. $\forall x A(x) \in \Delta$ *solo se* $A(t) \in \Delta$ *per ogni* $t \in Trm$;
6. $\exists x A(x) \in \Delta$ *se esiste un* $t \in Trm$ *tale che* $A(t) \in \Delta$.

Dim:

1. Ovvio, perchè Δ è consistente.
2. Visto che $A \wedge B \vdash A$, $A \wedge B \vdash B$ e $A, B \vdash A \wedge B$ basta applicare il lemma precedente.

3. Il verso da destra a sinistra vale grazie al lemma precedente perchè $A \vdash A \vee B$ e $B \vdash A \vee B$. Per quanto riguarda l'altro verso, procediamo per assurdo. Se né A né B appartengono a Δ allora sia $\neg A$ che $\neg B$ devono starci; allora $(\neg A) \wedge (\neg B) \in \Delta$ grazie al punto precedente. Ma quest'ultima formula è equivalente a $\neg (A \vee B)$ che non può appartenere a Δ perchè $A \vee B \in \Delta$ per ipotesi (e Δ è consistente).

4. Supponiamo che $A \to B \in \Delta$; se $A \notin \Delta$ abbiamo finito; se, invece, anche $A \in \Delta$ allora pure $B \in \Delta$ perchè $A, A \to B \vdash B$. Per quanto riguarda l'altro verso, da $A \notin \Delta$ o $B \in \Delta$ segue $\neg A \in \Delta$ o $B \in \Delta$; quindi $\neg A \vee B \in \Delta$ grazie al punto precedente.

5. Sia $\forall x A(x) \in \Delta$ e sia $t \in Trm$ qualsiasi; allora $A(t) \in \Delta$ perchè $\forall x A(x) \vdash A(t)$.

6. Sia $t \in Trm$ tale che $A(t) \in \Delta$; allora $\exists x A(x) \in \Delta$ perchè $A(t) \vdash \exists x A(x)$.

c.v.d.

Per potere invertire le ultime due condizioni della proposizione precedente è necessario fare un altro po' di lavoro. Si vede facilmente che le due condizioni sui quantificatori sono equivalenti (grazie al fatto che $\forall = \neg \exists \neg$); possiamo concentrarci su quella riguardante l'esiste. Vorremmo che dal fatto che $\exists x A(x)$ appartenga a Δ seguisse che anche $A(t)$ appartenesse a Δ per qualche $t \in Trm$. Questo, purtroppo, dipende dall'insieme dei termini e quindi dal linguaggio in considerazione. Vogliamo quindi far vedere come è possibile aggiungere delle costanti al linguaggio in modo che ad ogni formula del tipo $\exists x A(x)$ corrisponda una costante $c_{A,x}$ che soddisfi $A(c_{A,x})$ nel caso in cui $\exists x A(x)$ sia vera.

Costruiamo una catena di linguaggi nel seguente modo. Sia $L_0 = \mathcal{L}$ e consideriamo tutte le formule $A(x) \in Frm_{L_0}$ con x come variabile libera. Per ognuna di queste formule aggiungiamo al linguaggio un nuovo simbolo di costante $c_{A,x}$ e facciamo lo stesso per ogni altra variabile.[1] Chiamiamo L_1 il linguaggio così ottenuto. Ovviamente $L_0 \subseteq L_1$ e quindi anche $Trm_{L_0} \subseteq Trm_{L_1}$ e $Frm_{L_0} \subseteq Frm_{L_1}$. Quindi è possibile che esistano nuove formule aventi una variabile libera e appartenenti a Frm_{L_1}, ma non a Frm_{L_0}.

[1] Se, per esempio, una formula A contiene due variabili libere, diciamo x e y, allora aggiungeremo due nuove costanti $c_{A,x}$ e $c_{A,y}$.

Anche per queste nuove formule aggiungiamo un nuovo simbolo di costante; otteniamo così il linguaggio L_2; e così via. Iterando il procedimento si ottiene una catena

$$\mathcal{L} = L_0 \subseteq L_1 \subseteq L_2 \subseteq \ldots \subseteq L_n \subseteq \ldots$$

di linguaggi. Se poniamo

$$\overline{\mathcal{L}} = \bigcup_{i \in \mathbb{N}} L_i$$

otteniamo un linguaggio che contiene una costante per ogni formula con una variabile libera. Infatti, sia $A(x) \in Frm_{\overline{\mathcal{L}}}$ una formula con x come variabile libera; $A(x)$ conterrà un numero finito di simboli e quindi esisterà un $n \in \mathbb{N}$ tale che $A(x) \in Frm_{L_n}$. Di conseguenza esisterà un $c_{A,x}$ al piu in L_{n+1} e quindi in $\overline{\mathcal{L}}$.

Il linguaggio $\overline{\mathcal{L}}$ viene chiamato l'*espansione di Henkin* del linguaggio $\mathcal{L}$. Per ognuna delle formule $A(x) \in Frm_{\overline{\mathcal{L}}}$ con x come variabile libera, la formula

$$\exists x A(x) \to A(c_{A,x})$$

viene chiamata l'*assioma di Henkin* relativo alla formula $A(x)$.[2] Indichiamo con H l'insieme di tutti gli assiomi di Henkin.

Lemma 8.9 *Se $\Gamma \subseteq Frm_{\mathcal{L}}$ è consistente allora anche $\Gamma \cup H \subseteq Frm_{\overline{\mathcal{L}}}$ è consistente.*

Dim: Infatti, se per assurdo fosse $\Gamma, H \vdash \perp$ allora, per il teorema di finitezza, esisterebbe un insieme finito K di assiomi di Henkin tale che $\Gamma, K \vdash \perp$. Procediamo per induzione sulla cardinalità n di K. Vogliamo provare che si arriverebbe a un assurdo. Se $n = 0$ si avrebbe $\Gamma \vdash \perp$ che è assurdo perchè Γ è consistente.

Nel caso $n = 1$, sia $\exists x A(x) \to A(c_{A,x})$ l'unico assioma di Henkin in K. Da $\Gamma, \exists x A(x) \to A(c_{A,x}) \vdash \perp$ segue $\Gamma \vdash \neg (\exists x A(x) \to A(c_{A,x}))$ e quindi $\Gamma \vdash \exists x A(x) \wedge \neg A(c_{A,x})$. In altre parole, si avrebbe sia $\Gamma \vdash \exists x A(x)$ che $\Gamma \vdash \neg A(c_{A,x})$. Ma $c_{A,x}$ non compare in Γ quindi la prova di $\Gamma \vdash \neg A(c_{A,x})$ funziona anche se sostituiamo una variabile z (non libera in Γ) al posto della costante $c_{A,x}$. In altre parole è possibile provare che $\Gamma \vdash \neg A(z)$ e quindi (per $\forall$-introduzione) anche $\Gamma \vdash \forall x \neg A(x)$; cioè $\Gamma \vdash \neg \exists x A(x)$. In conclusione si avrebbe $\Gamma \vdash \exists x A(x)$ e $\Gamma \vdash \neg \exists x A(x)$; quindi $\Gamma \vdash \perp$ che è assurdo.

[2] Intuitivamente, l'assioma dice che se $\exists x A(x)$ è vera allora $c_{A,x}$ è un elemento che soddisfa $A(x)$.

Supponiamo adesso che K abbia cardinalità $n+1$ e che $K = K' \cup \{\exists x A(x) \to A(c_{A,x})\}$ (con K' di cardinalità n). Per ipotesi induttiva, $\Gamma \cup K'$ è consistente e quindi, grazie alla prova del caso $n = 1$ riletta con Γ, K' al posto di Γ, si ottiene la tesi. c.v.d.

Lemma 8.10 *Sia $\mathcal{L}$ un linguaggio e $\overline{\mathcal{L}}$ la sua estensione di Henkin. Se $\Delta \subseteq Frm_{\overline{\mathcal{L}}}$ è un sottoinsieme consistente massimale che contiene tutti gli assiomi di Henkin, allora:*

- *se $\exists x A(x) \in \Delta$ allora esiste un $t \in Trm_{\overline{\mathcal{L}}}$ tale che $A(t) \in \Delta$;*
- *se $A(t) \in \Delta$ per ogni $t \in Trm_{\overline{\mathcal{L}}}$ allora anche $\forall x A(x) \in \Delta$.*

per ogni formula $A(x)$ con x come variabile libera.

Dim: Sia $\exists x A(x) \in \Delta$; ma Δ contiene anche l'assioma di Henkin relativo ad $A(x)$ e quindi deve contenere anche $A(c_{A,x})$ che è una loro conseguenza.

Supponiamo adesso che $A(t) \in \Delta$ per ogni t. Se per assurdo $\forall x A(x)$ non stesse in Δ, allora ci dovrebbe stare $\neg \forall x A(x)$ e quindi anche $\exists x \neg A(x)$. Da questo e dal fatto che Δ contiene l'assioma di Henkin relativo a $\neg A(x)$ seguirebbe $\neg A(c_{(\neg A),x}) \in \Delta$. Ma questo è assurdo perchè anche $A(c_{(\neg A),x}) \in \Delta$ per ipotesi. c.v.d.

Adesso siamo pronti a dimostrare il teorema di completezza.

Teorema 8.11 (completezza) *Per ogni $\Gamma \subseteq Frm_{\mathcal{L}}$, se $\Gamma \nvdash \bot$ (cioè Γ è consistente) allora Γ è soddisfacibile (cioè ammette un modello).*

Dim: Sia $\overline{\mathcal{L}}$ l'estensione di Henkin di $\mathcal{L}$ e sia H l'insieme degli assiomi di Henkin relativi a $\overline{\mathcal{L}}$. Sia Δ un sottoinsieme consistente massimale che contiene $\Gamma \cup H$ (quindi $\Delta \subseteq Frm_{\overline{\mathcal{L}}}$). Nel resto della dimostrazione, scriviamo Trm al posto di $Trm_{\overline{\mathcal{L}}}$ e Frm invece di $Frm_{\overline{\mathcal{L}}}$.

Dobbiamo definire un'interpretazione che renda valide tutte le formule di Γ. Consideriamo $D = Trm$ come dominio e interpretiamo ogni funzione ed ogni costante in se stessa. Ad esempio, se f è un simbolo di funzione n-aria lo interpretiamo come la funzione da $D^n = Trm^n$ in $D = Trm$ che ad ogni n-pla $t_1 \dots t_n$ associa $f(t_1, \dots, t_n) \in D = Trm$. Inoltre consideriamo l'identità come assegnazione σ (cioè $\sigma(x) = x$ per ogni x). Ci rimane da definire un predicato su D per ognuno dei simboli di predicato del linguaggio. Sia, quindi, P un simbolo di predicato n-ario; interpretiamo P come il predicato "la formula $P(x_1 \ldots, x_n)$ appartiene a Δ"; cioè, per ogni n-pla $t_1, \ldots, t_n$ di elementi di D, poniamo:

$$val(P(t_1, \ldots, t_n)) = V \qquad \text{se e solo se} \qquad P(t_1, \ldots, t_n) \in \Delta \ .$$

Sia adesso A una formula qualsiasi; vogliamo provare che:

$$val(A) = V \qquad \text{se e solo se} \qquad A \in \Delta \ .$$

Procediamo per induzione sulla complessità di A. Se A è atomica allora la tesi vale per definizione. Il passo induttivo segue dalle proprietà degli insiemi consistenti massimali di $\overline{\mathcal{L}}$.

Per esempio, supponiamo che A sia del tipo $B \to C$. Allora $val(A) = V$ se e solo se $val(\neg B) = V$ oppure $val(C) = V$; cioe se e solo se (per ipotesi induttiva) $\neg B \in \Delta$ oppure $C \in \Delta$, ovvero $\neg B \vee C \in \Delta$. In altre parole $B \to C \in \Delta$; cioè $A \in \Delta$.

Per fare un altro esempio, consideriamo il caso $A = \exists x B(x)$: $val(A) = V$ se e solo se esiste un'assegnazione σ', diversa da σ solo su x tale che $A(\sigma'(x))$ è vera in $D = Trm$. Sia $t = \sigma'(x)$; allora $A(t)$ è valida in D, σ perchè $\sigma(t) = t$. Cioè $val(A) = V$ se e solo se esiste un $t \in Trm$ tale che $val(A(t)) = V$; per l'ipotesi induttiva, questo vale se e solo se $A(t) \in \Delta$. Ma sappiamo che: esiste un $t \in Trm$ tale che $A(t) \in \Delta$ vale se e solo se $\exists x A(x) \in \Delta$.

In definitiva, l'interpretazione D, σ costruita sopra è tale che rende vere tutte e sole le formule di Δ; ma $\Gamma \subseteq \Delta$, quindi D, σ è un modello di Γ. c.v.d.

L'interpretazione D, σ costruita nella prova del teorema di completezza, viene chiamata il modello *canonico* di Γ o, anche, il modello *sintattico* (perchè è costruito a partire dal linguaggio).

8.3 Il teorema di compattezza

Una delle conseguenze più importanti del teorema di completezza per la logica dei predicati del primo ordine è il seguente.

Teorema 8.12 (di compattezza) *Sia $\mathcal{L}$ un linguaggio al primo ordine e sia $\Gamma \subseteq Frm_{\mathcal{L}}$. Supponiamo che ogni sottoinsieme finito di Γ ammetta un modello. Allora esiste un modello per tutto Γ.*

Dim: Supponiamo per assurdo che Γ non sia soddisfacibile. Allora, per il teorema di completezza, $\Gamma \vdash \bot$ deve essere dimostrabile. Applicando il teorema di finitezza si ha che deve esistere $K \subseteq \Gamma$, K finito, tale che $K \vdash \perp$. Da questo segue che K non può avere un modello: in contrasto con l'ipotesi del teorema. c.v.d.

Diamo un esempio di applicazione del teorema di compattezza. Supponiamo di avere un linguaggio con uguaglianza. Allora per ogni numero naturale n è possibile considerare una formula F_n che esprima la frase "esistono al più n elementi":

$$F_n \equiv \exists x_1 \exists x_2 \cdots \exists x_n \forall y (y = x_1 \vee y = x_2 \vee \cdots \vee y = x_n) \ .$$

Ovviamente, la formula $\neg\ F_n$ dirà: "esistono più di n elementi". A questo punto è possibile esprimere al primo ordine il concetto di insieme infinito. Infatti, se $\Gamma = \{\neg\ F_n \ : \ n \in \mathbb{N}\}$ allora un modello di Γ non è altro che un insieme infinito.

Al contrario, vogliamo dimostrare che non è possibile esprimere al primo ordine il concetto di insieme finito, cioè non esiste una lista di assiomi che è soddisfatta da tutti e soli gli insiemi finiti. Supponiamo per assurdo che tale insieme di formule esista e chiamiamolo Δ. Consideriamo l'insieme $\Gamma \cup \Delta$, con Γ definito come sopra, e prendiamo un suo sottoinsieme finito che possiamo immaginare come $K \cup L$, con K sottoinsieme finito di Γ e L sottoinsieme finito di Δ. Se $K = \emptyset$ allora $K \cup L$ ammette come modello un qualsiasi insieme finito (per l'ipotesi di assurdo). Invece, se $K \neq \emptyset$ allora sia m il più grande fra i numeri naturali n tali che $\neg\ F_n$ appartiene a K; in questo caso $K \cup L$ ha come modello un qualsiasi insieme finito con più di m elementi. In ogni caso, ogni sottoinsieme finito di $\Gamma \cup \Delta$ ha un modello e quindi anche $\Gamma \cup \Delta$ ha un modello, grazie al teorema di compattezza. Ma questo è ovviamente assurdo, perchè un modello di $\Gamma \cup \Delta$ dovrebbe essere un insieme contemporaneamente infinito e finito.

Proposizione 8.13 *Sia $\Gamma \subseteq Frm$ e supponiamo che, comunque si fissi $n \in \mathbb{N}$, esista un modello finito di Γ con più di n elementi. Allora Γ ammette un modello infinito.*

Dim: Un modello infinito di Γ non è altro che un modello di $\Gamma \cup \{\neg\ F_n \ : \ n \in \mathbb{N}\}$, con le F_n definite come sopra. A questo punto basta applicare il teorema di compattezza a quest'ultimo insieme di formule. c.v.d.

Parte III

Appendici

Appendice A

Complementi di sintassi

A.1 Forme normali

Definizione A.1 *Sia A una formula proposizionale. Si dice che A è in* forma normale congiuntiva *se A è del tipo*

$$B_1 \wedge B_2 \wedge \ldots \wedge B_n$$

dove ognuna delle formule B_i è del tipo

$$p_1 \vee p_2 \vee \ldots p_n \vee \neg\, q_1 \vee \neg\, q_2 \vee \ldots \vee \neg\, q_m$$

con p_i e q_i atomiche.

Si può dimostrare che ogni formula è equivalente ad una in forma normale congiuntiva. L'algoritmo che permette di passare da una formula ad una sua forma normale congiuntiva è il seguente:

1. si sostituisce ogni sottoformula del tipo $A \to B$ con $\neg\, A \vee B$;

2. si sostituisce ogni $\neg\neg\, A$ con A;

3. si sostituisce ogni sottoformula del tipo $\neg\, (A \wedge B)$ con $\neg\, A \vee \neg\, B$ e ogni $\neg\, (A \vee B)$ con $\neg\, A \wedge \neg\, B$;

4. si sostituisce ogni $\neg\neg\, A$ con A;

5. si sostituisce ogni sottoformula del tipo $A \vee (B \wedge C)$ con $(A \vee B) \wedge (A \vee C)$.

Definizione A.2 *Una formula predicativa si dice in* forma normale prenessa *se è del tipo*

$$Q_1x_1\ Q_2x_2\ \cdots\ Q_nx_n\ A$$

dove ogni Q_i è un quantificatore ($\forall$ o $\exists$) e A è una formula senza quantificatori.

Ogni formula predicativa è equivalente ad una formula in forma normale prenessa, come si può vedere applicando opportunamente le seguenti equivalenze:

1. $\neg\, \forall x A(x) \equiv \exists x \neg\, A(x)$;
2. $\neg\, \exists x A(x) \equiv \forall x \neg\, A(x)$;
3. $A \wedge \forall x B(x) \equiv \forall x(A \wedge B(x))$, se x non è libera in A;
4. $A \vee \forall x B(x) \equiv \forall x(A \vee B(x))$, se x non è libera in A;
5. $A \wedge \exists x B(x) \equiv \exists x(A \wedge B(x))$, se x non è libera in A;
6. $A \vee \exists x B(x) \equiv \exists x(A \vee B(x))$, se x non è libera in A.

A.2 Assiomi sull'uguaglianza

In tutte le teorie matematiche è sempre presente un predicato binario particolare: l'uguaglianza (indicata con $=$). In questa sezione vedremo come è possibile definirne le proprietà. Si possono scegliere due strade equivalenti: o aggiungere nuove regole al calcolo della deduzione naturale oppure stabilire degli assiomi. Seguiamo, per esempio, questa seconda opzione e diamo, quindi, una lista degli assiomi di $=$.

Probabilmente le prime proprietà che vengono in mente su $=$ sono:

(riflessiva) $\forall x(x = x)$;

(simmetrica) $\forall x \forall y(x = y \rightarrow y = x)$;

(transitiva) $\forall x \forall y \forall z(x = y \wedge y = z \rightarrow x = z)$.

Ma siamo sicuri che questi tre assiomi bastino? Ad esempio, consideriamo il seguente ragionamento (che sicuramente è giusto): se f è una funzione allora da $x = y$ segue $f(x) = f(y)$. Formalmente, data una funzione f, vorremmo provare che $\forall x \forall y (x = y \to f(x) = f(y))$ a partire dai tre assiomi dati sopra. Ci si convince facilmente che non c'è modo di dimostrarlo.

Quello appena fatto è un caso molto semplice di una proprietà generale dell'uguaglianza, detta *principio di Leibnitz*: "se $x = y$ allora possiamo sosituire y ad x in *ogni* contesto". Ovviamente questo principio non può corrispondere ad un solo assioma; per esprimerlo abbiamo bisogno di un'infinità di assiomi (oppure, come vedremo dopo, di due nuove regole):

- per ogni termine $t(z)$ contenente almeno una variabile libera z e per ogni termine t' (qualsiasi) aggiungiamo l'assioma

$$\forall x \forall y \big(t(x) = t' \wedge x = y \to t(y) = t'\big) \ ;$$

- per ogni formula $A(z)$ contenente almeno una variabile libera z (e in cui z non compare anche come variabile legata), aggiungiamo l'assioma

$$\forall x \forall y \big(A(x) \wedge x = y \to A(y)\big) \ .$$

Equivalentemente, possiamo aggiungere due nuove regole:

$$\frac{t(x) = t' \quad x = y}{t(y) = t'} \qquad \frac{A(x) \quad x = y}{A(y)}$$

se $t(z)$ e $A(z)$ sono un termine e una formula contenenti almeno una variabile libera z (con z che non compare legata in A) e t' è un termine qulasiasi.

A questo punto, si può vedere che gli assiomi (o le regole) esprimenti il principio di Leibnitz, insieme alla proprietà riflessiva, sono sufficienti per dimostrare anche la proprietà simmetrica e quella transitiva. Infatti, siano x e y elementi generici tali che $x = y$; vogliamo provare che $y = x$. Consideriamo come $t(z)$ il termine z e come t' il termine x; allora $t(x) = t'$ per la proprietà riflessiva e quindi anche $t(y) = t'$ per l'assioma corrispondente (perchè $x = y$). Cioè, $y = x$. Per quanto riguarda la transitiva, siano x, y e z tali che $x = y$ e $y = z$; inoltre, sia $A(z)$ la formula $x = z$. Per ipotesi vale $A(y)$; da questo e dall'altra ipotesi $y = z$, usando l'opportuno assioma, segue che deve valere anche $A(z)$, cioè $x = z$.

Appendice B

Logica intuizionistica

Oltre alla logica classica è possibile definire tantissime altre logiche. Ad esempio, le logiche modali si propongono di studiare formule contenenti espressioni come: "è possibile che", "è necessario che"; le logiche temporali studiano, invece, frasi la cui verità dipende dal tempo; la logica fuzzy analizza espressioni il cui valore di verità è incerto o probabilistico.

In questo capitolo daremo una veloce introduzione alla logica intuizionistica. Essa parte dal presupposto che ci sono formule la cui verità non può essere stabilita in modo algoritmico. Per esempio, se dico "la millesima cifra decimale di $\sqrt{2}$ è 5" ho sicuramente un metodo per decidere se la frase è vera o falsa: basta (!) calcolarsi le prime 1000 cifre di $\sqrt{2}$. Se invece la frase che voglio analizzare è "il numero 7 è una cifra decimale di $\sqrt{2}$" le cose si complicano. Infatti, posso cominciare a cercare le cifre decimali di $\sqrt{2}$: se ad un certo punto trovo un 7 allora posso dire che la frase è vera; ma non potrò mai affermare con certezza che la frase è falsa, perchè le cifre di $\sqrt{2}$ sono infinite. Quindi, in generale, non ho un metodo per capire se una frase è vera o falsa.

La logica intuizionistica si propone di distinguere fra le frasi che sono vere perchè si ha un metodo per deciderlo e quelle che sono vere per altri motivi, ad esempio perchè la loro negazione non può essere vera. Per esempio, consideriamo la frase "esistono due numeri irrazionali a e b tali che a^b è razionale". Questa frase è vera, ma in un modo che non è accettabile dal punto di vista intuizionistico; infatti la prova è: se $\sqrt{2}^{\sqrt{2}}$ è razionale allora prendiamo $a = b = \sqrt{2}$, mentre se $\sqrt{2}^{\sqrt{2}}$ è irrazionale poniamo $a = \sqrt{2}^{\sqrt{2}}$ e $b = \sqrt{2}$. Questa dimostrazione però non fornisce un metodo per stabilire chi sono a e b con certezza: la loro definizione dipende dal sapere se $\sqrt{2}^{\sqrt{2}}$ è razionale oppure no, cosa non semplice da decidere.

Riassumendo, le caratteristiche delle logica intuizionistica sono:

- una formula viene considerata dimostrabile quando c'è un metodo effettivo per decidere che è vera; in particolare non si può dimostrare che vale $A \vee \neg A$, qualsiasi sia A, pechè in generale non c'è un metodo per decidere se A è vera o falsa;

- in generale dal sapere che $\neg A$ è falsa non segue che A è vera, perchè non è detto che abbiamo un metodo per riconoscere che A è vera (per esempio, dal sapere che $\forall x A(x)$ è falsa non segue necessariamente che conosciamo un elemento t tale che $A(t)$ è falsa; cioè, da $\neg \forall x A(x)$ non segue $\exists x \neg A(x)$);

- una formula del tipo $\exists x A(x)$ è dimostrabile solo se possiamo dimostrare $A(t)$ per qualche elemento t; similmente, $A \vee B$ è dimostrabile solo se sappiamo dimostrare A oppure B.

Per ottenere una formalizzazione della logica intuizionistica è sufficiente considerare le regole del calcolo della deduzione naturale classica e sostituire la regola di riduzione all'assurdo con la regola

$$\frac{\perp}{A}$$

che è più debole.

Ovviamente tutto ciò che è dimostrabile in logica intuizionistica vale anche in logica classica, ma non è sempre vero il viceversa. Ad esempio, i seguenti fatti *non* sono dimostrabili in logica intuizionistica:

- $\neg\neg A \vdash A$;

- $\vdash A \vee \neg A$;

- $A \to B \vdash \neg A \vee B$;

- $\neg (A \wedge B) \vdash (\neg A) \vee (\neg B)$;

- $\neg \forall x A(x) \vdash \exists x \neg A(x)$.

Appendice C

I numeri naturali e il teorema di Gödel

Nella prima sezione di questo capitolo definiremo i numeri naturali tramite gli assiomi di Peano, al secondo ordine; in seguito proveremo alcuni fondamentali risultati fra cui la seconda forma del principio di induzione. Nella seconda sezione afronteremo il problema di formalizzare gli assiomi di Peano al primo ordine; questo ci porterà ad enunciare i famosi teoremi di incompletezza di Gödel di cui cercheremo di fornire una rapida ed informale spiegazione.

C.1 Gli assiomi di Peano

Il logico italiano Giuseppe Peano, ponendosi il problema di dare una definizione assiomatica dell'insieme $\mathbb{N} = \{0, 1, 2, \ldots, n, \ldots\}$ dei numeri naturali, propose i seguenti famosi assiomi:

1. $0 \in \mathbb{N}$; cioè $\mathbb{N}$ contiene una costante, chiamata "zero";

2. per ogni $x \in \mathbb{N}$ anche $s(x) \in \mathbb{N}$; cioè esiste una funzione da $\mathbb{N}$ in $\mathbb{N}$, chiamata "successore" (intuitivamente, $s(x) = x + 1$);

3. non esiste un x tale che $s(x) = 0$; cioè 0 non è il successore di alcun numero;

4. se $s(x) = s(y)$ allora $x = y$; cioè la funzione s è iniettiva;

5. (*principio di induzione*) sia $P(x)$ una proposizione tale che:

(a) $P(0)$ è vera,

(b) ogni volta che vale $P(x)$ vale anche $P(s(x))$;

allora $P(x)$ vale per ogni $x \in \mathbb{N}$.

Chiaramente, il numero $s(0)$ viene chiamato 1, il numero $s(s(0))$ viene chiamato 2 e così via.

Peano dimostrò che, a meno di isomorfismi, esiste un solo insieme che soddisfa i cinque assiomi dati sopra. Quindi, dai cinque assiomi di Peano si possono dimostrare tutte le proprietà sui numeri naturali come, ad esempio, l'importantissimo

Proposizione C.1 (Principio del buon ordinamento dei naturali) *Ogni sottoinsieme non vuoto di $\mathbb{N}$ ammette minimo.*

Dim: Sia A un sottoinsieme non vuoto di $\mathbb{N}$ e sia $P(x)$ la proposizione "x è un minorante di A" (vedi l'appendice sulle relazioni d'ordine). Ovviamente $P(0)$ è vera. D'altra parte, esiste sicuramente un x tale che $P(x)$ è falsa. Infatti, sia $a \in A$; allora $a+1$ sicuramente non è un minorante di A. Questo significa che la seconda ipotesi del principio di induzione non può essere vera; cioè, deve esistere un m tale che $P(m)$ è vera , ma $P(m+1)$ è falsa. Vogliamo dimostrare che tale m è il minimo di A. Sicuramente m è un minorante di A, perchè $P(m)$ è vera. Resta da provare che $m \in A$. Se per assurdo m non fosse in A allora si avrebbe $m < x$ per ogni $x \in A$ e quindi anche $m+1$ sarebbe un minorante di A: assurdo. c.v.d.

Come corollario diamo una seconda forma, molto usata nelle dimostrazioni, del principio di induzione.

Proposizione C.2 (seconda forma del principio di induzione) *Sia $P(x)$ una proposizione tale che:*

1. *$P(0)$ è vera;*

2. *se $P(x)$ è vera per tutti gli $x < n$ allora anche $P(n)$ è vera.*

Allora $P(x)$ è vera per ogni $x \in \mathbb{N}$.

Dim: Sia $A = \{x \in \mathbb{N} \ : \ P(x) \text{ è falsa}\}$ e supponiamo per assurdo che A non sia vuoto. Allora esisterà m minimo di A. Tale m non può essere 0 perchè $P(0)$ è vera (mentre $P(m)$ è falsa visto che $m \in A$). Consideriamo, pertanto un qualunque $x < m$. Dato che m è il minimo di A, sicuramente x non starà in A e quindi $P(x)$ è vera (per ogni $x < m$). Allora anche $P(m)$ dovrebbe essere vera (per la seconda ipotesi): assurdo. c.v.d.

C.2 I teoremi di incompletezza di Gödel

Ci chiediamo, adesso, se è possibile formalizzare al primo ordine gli assiomi sui naturali. Per farlo, sembra plausibile considerare un linguaggio $\mathcal{L}$ che contenga una costante 0, una funzione s, il predicato di uguaglianza $=$ e una lista potenzialmente infinita di variabili. Ovviamente, dobbiamo considerare gli assiomi sull'uguaglianza e poi la traduzione dei cinque assiomi di Peano (il primo e il secondo sono impliciti nella scelta del linguaggio):

- $\neg \exists x(s(x) = 0)$;
- $\forall x \forall y(s(x) = s(y) \to x = y)$.

Ma come possiamo formalizzare il principio di induzione? Infatti, esso presenta una quantificazione del tipo "per ogni proposizione $P(x)$" che è del secondo ordine. Quello che si può fare se vogliamo restare al primo ordine è di sostituire il quinto assioma con una lista di assiomi, uno per ogni formula del linguaggio.

Pertanto, se $A(x) \in Frm_{\mathcal{L}}$ è una formula con una sola variabile libera, consideriamo l'assioma:

$$A(0) \wedge \forall x\Big(A(x) \to A\big(s(x)\big)\Big) \ \to \ \forall x A(x)$$

che esprime l'assioma di induzione relativo a $A(x)$.

Il problema è che non tutte le proposizioni $P(x)$ possibili è immaginabili sono esprimibili come una formula $A(x)$ del linguaggio fissato $\mathcal{L}$. Il primo teorema di incompletezza di Gödel dimostra proprio che la formalizzazione al primo ordine non riesce ad esprimere in pieno il quinto assioma di Peano.

Teorema C.3 (primo teorema di incompletezza di Gödel) *Sia* $\mathcal{L} = \{=, 0, s, x_1, \ldots, x_n, \ldots\}$ *il linguaggio al primo ordine per i numeri naturali (come descritto sopra) e sia* $\mathcal{P} \subseteq Frm_{\mathcal{L}}$ *l'insieme degli assiomi al primo ordine proposti sopra. Allora esiste una formula* $G \in Frm_{\mathcal{L}}$ *che ha* $\mathbb{N}$ *come modello (cioè è vera sui naturali), ma non è dimostrabile a partire da* $\mathcal{P}$, *cioè* $\mathcal{P} \nvdash G$.

In altre parole, $\mathbb{N}$ non è l'unico modello di $\mathcal{P}$: esistono altri modelli di $\mathcal{P}$ in cui non vale G.

In realtà il teorema non vale solo per l'insieme di assiomi $\mathcal{P}$; ad esempio, continua a valere anche se si aggiungono (una quantità numerabile di) nuovi assiomi. Quindi, anche se si aggiunge agli assiomi la formula G di cui parla il teorema, dovrà esistere un'altra formula G' vera in $\mathbb{N}$, ma non dimostrabile nemmeno a partire dai nuovi assiomi.

Non diamo una prova di questo teorema, ma soltanto cercheremo di spiegare l'idea che vi sta dietro. Visto che il nostro linguaggio $\mathcal{L}$ è numerabile, è possibile assegnare un numero ad ogni simbolo del linguaggio e, per ricorsione, ad ogni formula di $\mathcal{L}$. Sempre allo stesso modo, si possono numerare le dimostrazioni formali. In questo modo è possibile dimostrare che esiste una formula, diciamo $P(x, y)$, che dica "il numero x corrisponde ad una dimostrazione che ha per conclusione la formula il cui numero è y". Quindi si può esprimere la frase "la formula il cui numero è x è dimostrabile (a partire dagli assiomi $\mathcal{P}$)" tramite la formula $Dim(x) \equiv \exists y P(y, x)$.

Si può vedere che tutti i processi algoritmici corrispondono a delle formule. Per esempio, consideriamo il seguente procedimento, che chiamiamo *autosostituzione*. Sia A una formula e sia n il numero di tale formula; sostituiamo n (in realtà dobbiamo sostituire il termine $s(\cdots s(0)))$ con s ripetuto n volte) al posto di tutte le variabili libere di A. La formula che si ottiene è l'autosostituzione di A. Visto che questo procedimento è algoritmico, si può dimostrare che esiste una formula che dica "x è il numero dell'autosostituzione della formula il cui numero è y". Per comodità possiamo immaginare di avere una funzione $sost(x)$ che, data la formula il cui numero sia x, fornisca il numero delle sua autosostituzione.

A questo punto siamo vicinissimi a trovare la formula G di cui parla il teorema. Sia U la formula

$$\neg \Big(Dim\big(sost(x)\big)\Big)$$

(con x come unica variabile libera) e sia u il numero di tale formula. Allora, autosostituendo u, otteniamo la formula chiusa

$$\neg \Big(Dim\big(sost(u)\big)\Big)$$

che chiamiamo G. Questa è proprio la formula di cui parla il teorema. Per prima cosa notiamo che il numero di G è $sost(u)$ perchè G è l'autosotituzione di u. A questo punto possiamo leggere cosa dice G: "la formula che ha per numero $sost(u)$ non è dimostrabile", cioè "la formula G non è dimostrabile". In altre parole, G afferma di non essere dimostrabile. A questo punto è facile convincersi che G debba essere vera, ma non dimostrabile. Infatti, se G fosse dimostrabile (a partire da $\mathcal{P}$) si avrebbe $\mathcal{P} \vdash G$ e quindi anche $\mathcal{P} \models G$; in particolare G dovrebbe essere vera su $\mathbb{N}$. Ma l'interpretazione di G (su $\mathbb{N}$) é la frase: "G non è dimostrabile" che è falsa per ipotesi: assurdo. Quindi l'unica possibilità è che G non sia dimostrabile. Ma questo è proprio ciò che dice l'interpretazione di G su $\mathbb{N}$; quindi G è vera in $\mathbb{N}$.

Ancora più sconvolgente è il secondo teorema di incompletezza di Gödel, che dimostra che è impossibile dimostrare la coerenza (cioè consistenza) di una teoria se si usano soltanto gli assiomi della teoria. Per capire la portata di questo e del primo teorema di incompletezza è necessario ricordare che essi si applicano non solo alla teoria dei numeri naturali, ma anche a teorie più potenti, come quella degli insiemi. Ora, si può dire che la teoria degli insiemi formalizza tutta la matematica immaginata (finora). Quindi, se gli assiomi della teoria degli insiemi non bastano a dimostrarne la coerenza, significa in pratica che tale coerenza non può essere provata affatto!

Appendice D

Complementi di teoria degli insiemi

In questo capitolo vogliamo dare una breve introduzione alla teoria (informale) degli insiemi allo scopo di fornire gli strumenti, primo fra tutti il lemma di Zorn, usati in alcune dimostrazioni del capitolo sul teorema di completezza della logica del primo ordine. Daremo per note la maggior parte delle definizioni di base.

Il concetto di insieme viene di solito dato come primitivo, cioè non esplicitamente definibile. L'idea intuitiva è che un insieme sia una collezione di oggetti. Si chiede soltanto che l'appartenenza di un elemento ad un insieme non sia definita in modo ambiguo o contraddittorio. Ad esempio, le persone simpatiche non formano un insieme, perchè il concetto di simpatico non è oggettivo. Vedremo esempi più interessanti di collezioni che non formano un insieme.

Per chiarire meglio cosa si intenda per insieme è più conveniente stipulare l'esistenza di alcuni insiemi e poi costruire tutti gli altri a partire da questi usando un numero fissato di operazioni. In realtà è sufficiente stipulare l'esistenza dell'insieme vuoto $\emptyset$. Se per esempio vogliamo descrivere il gruppo con due soli elementi, è chiaro che non ha nessuna importanza il nome o l'idea che ho di tali due elementi; la cosa importante sono le loro proprietà (vedi il concetto di *isomorfismo*). Ad esempio, posso pensare che il mio gruppo abbia come elementi $\emptyset$ e $\{\emptyset\}$ e che l'operazione sia l'unione $\cup$. Per fare un altro esempio, è possibile definire i numeri naturali nel seguente modo. Poniamo $0 = \emptyset$, $1 = \{\emptyset\} = \{0\}$, $2 = \{\emptyset, \{\emptyset\}\} = \{0, 1\}$ e così via; in generale $n + 1 = \{0, 1, 2, \ldots, n\}$.

Un insieme può avere altri insiemi come elementi; anzi, gli esempi appena dati suggeriscono che si può fare in modo che ciò accada sempre. Questo permette di evitare una difficile distinzione filosofica fra ciò che è un insieme e ciò che è un elemento: formalmente possiamo immaginare che esistano solo insiemi.

Resta da chiarire quali siano le operazioni che permettono di costruire nuovi insiemi. Sicuramente abbiamo l'unione e l'intersezione anche di famiglie arbitrarie di insiemi (che siano già stati costruiti). Ma anche possiamo considerare l'insieme delle parti di un insieme dato. Oppure, dato un insieme A e una proprietà $P(x)$, possiamo assumere che

$$\{x \in A \ : \ P(x)\}$$

sia un insieme che ha per elementi gli elementi di A che godono della proprietà P. Il paradosso di Russell ci dice che in generale non è possibile considerare l'insieme di tutti gli elementi che godono di una certa proprietà, ma che è importante restringersi agli elementi di un certo insieme A già costruito.

Proposizione D.1 (Paradosso di Russell) *La collezione*

$$R = \{x \ : \ x \notin x\}$$

non è un insieme.

Dim: Se R fosse un insieme allora ci si potrebbe chiedere se $R \in R$ oppure no. Se fosse $R \in R$ allora R dovrebbe godere della proprietà che hanno tutti gli elementi di R e cioè $R \notin R$. Viceversa se fosse $R \notin R$ allora R godrebbe della proprietà che definisce R, quindi $R \in R$. Riassumendo si avrebbe

$$(R \in R) \leftrightarrow \neg\, (R \in R)$$

che è una contraddizione. c.v.d.

Le collezioni, come la R di Russell, che non sono insiemi vengono dette *classi proprie*. Alle classi proprie non è lecito applicare le operazioni fra insiemi (ad esempio fare l'insieme delle parti) perchè altrimenti si cade in contraddizione.

Ci sono altri modi per costruire insiemi; ad esempio, se A e B sono insiemi si indica con $A \times B$ l'insieme (chiamato prodotto cartesiano) delle coppie ordinate di elementi di A e B. Una coppia ordinata è una scrittura formale del tipo (a, b) con $a \in A$ e $b \in B$; due coppie, (a, b) e (a', b') vengono considerate uguali se e solo se $a = a'$ e $b = b'$.

Una relazione fra gli insiemi A e B formalmente è un sottoinsieme di $A \times B$, nel senso che ogni relazione è individuata dalle coppie di elementi che mette in relazione. Una funzione fra A e B è una legge che associa ad ogni elemento di A uno e un solo elemento di B.

Infine, un metodo spesso usato per costruire nuovi insiemi è quello di quozientare un insieme su una relazione di equivalenza. Se A è un insieme e $\sim$ è una relazione di equivalenza (riflessiva, simmetrica e transitiva) su A, allora si indica con $A/\sim$ l'insieme che ha per elementi le classi di equivalenza di A. Se $a \in A$ la classe di equivalenza di a è l'insieme degli elementi che sono in relazione con a (rispetto a $\sim$).

D.1 Relazioni d'ordine

In questa sezione verrà effettuata una veloce rassegna di alcune fondamentali nozioni riguardanti gli insiemi ordinati. Di nuovo, lo scopo principale è fornire gli strumenti necessari a comprendere l'enunciato (e la prova) del lemma di Zorn.

Sia X un insieme e $\leq$ una relazione binaria su X (cioè un sottoinsieme di $X \times X$). Si dice che $\leq$ è una *relazione d'ordine (parziale)* su X se sono verificati i seguenti assiomi:

1. $\forall x(x \leq x)$ (proprietà riflessiva);
2. $\forall x \forall y \forall z(x \leq y \wedge y \leq z \rightarrow x \leq z)$ (proprietà transitiva);
3. $\forall x \forall y(x \leq y \wedge y \leq x \rightarrow x = y)$ (proprietà antisimmetrica).

L'aggettivo "parziale" si riferisce al fatto che possono esistere due elementi x e y non *confrontabili*, cioè tali che né $x \leq y$, né $y \leq x$.

Un insieme dotato di una relazione d'ordine parziale, viene detto un *insieme parzialmente ordinato*.

L'esempio standard di insieme parzialmente ordinato è $\mathcal{P}(A)$, l'insieme delle parti di un insieme A, dove la relazione d'ordine è l'inclusione (non stretta) $\subseteq$. Se ad esempio, $A = \{0, 1\}$ allora $\mathcal{P}(A) = \{\emptyset, \{0\}, \{1\}, A\}$ e $\{0\}$ e $\{1\}$ non sono confrontabili (rispetto a $\subseteq$).

Sia $(X, \leq)$ un insieme parzialmente ordinato, sia $z \in X$ e sia $A \subseteq X$. Si dice che:

- z è un *maggiorante* di A se $(\forall x \in A)(x \leq z)$, cioè $\forall x(x \in A \to x \leq z)$;
- z è un *minorante* di A se $(\forall x \in A)(z \leq x)$, cioè $\forall x(x \in A \to z \leq x)$;
- A è *limitato superiormente* se esiste un maggiorante di A;
- A è *limitato inferiormente* se esiste un minorante di A;
- A è *limitato* se è limitato sia superiormente che inferiormente;
- z è il *massimo* di A se z è un maggiorante di A e $z \in A$;
- z è il *minimo* di A se z è un minorante di A e $z \in A$;
- z è l'*estremo superiore* di A se z è il minimo dell'insieme dei maggioranti di A;
- z è l'*estremo inferiore* di A se z è il massimo dell'insieme dei minoranti di A.

Un elemento $z \in X$ si dice *massimale* se:

$$\forall x(z \leq x \to z = x)$$

(cioè non esistono elementi più grandi di lui). Dualmente si può definire il concetto di *minimale*.

Un insieme si dice *totalmente ordinato* se è parzialmente ordinato ed in più soddisfa il seguente assioma:

$$\forall x \forall y(x \leq y \vee y \leq x)$$

(cioè tutti gli elementi sono confrontabili). Un ordine totale viene anche detto un *ordine lineare*.

Dato $A \subseteq X$, se succede che A è totalmente ordinato (rispetto allo stesso ordine di X) allora si dice che A è una *catena* di X. In altre parole, una catena è un sottoinsieme totalmente ordinato.

D.1.1 Alberi

Un albero è un particolare insieme parzialmente ordinato, i cui elementi vengono chiamati *nodi*, che gode delle seguenti proprietà:

1. esiste il minimo di X; tale minimo viene detto la *radice* dell'albero X;
2. dati $x, y \in X$, se esiste un maggiorante di $\{x, y\}$ allora x e y sono confrontabili.

Gli eventuali elementi massimali di X vengono chiamati *foglie*. Si chiama *ramo* ogni catena di X che sia massimale (nell'insieme, parzialmente ordinato rispetto a $\subseteq$, delle catene di X). In altre parole, un ramo è una sottoinsieme R tale che:

1. R è una catena;
2. la radice appartiene ad R;
3. o R è illimitato superiormente oppure ammette massimo e il suo massimo è una foglia;
4. dati $a, b \in R$, se $x \in X$ è tale che $a \leq x \leq b$ allora $x \in R$.

Nel caso di un albero finito (cioè con un numero finito di nodi), un ramo è semplicemente una sequenza di nodi che parte dalla radice, arriva ad una foglia e contiene tutti i nodi compresi fra la radice e tale foglia. In altre parole, un ramo è costituito da tutti i nodi che si incontrano andando dalla radice ad una foglia.

Si dice *profondità* di un albero finito il numero di nodi del ramo più lungo diminuito di 1.

D.2 Algebre di Boole

Definizione D.2 *Un'*algebra di Boole *è una struttura* $(X, +, \cdot, 0, 1, {}^{-})$ *dove* X *è un insieme,* $+$ *e* $\cdot$ *sono due operazioni binarie,* 0 *e* 1 *sono due costanti e* ${}^{-}$ *è un operazione unaria tali che:*

- $\forall x(x + x = x)$ *e* $\forall x(x \cdot x = x)$ *(proprietà di idempotenza);*
- $\forall x \forall y(x + y = y + x)$ *e* $\forall x \forall y(x \cdot y = y \cdot x)$ *(proprietà commutative);*

- $\forall x \forall y \forall z \big((x+y)+z = x+(y+z)\big)$ *e* $\forall x \forall y \forall z \big((x \cdot y) \cdot z = x \cdot (y \cdot z)\big)$ *(proprietà associative);*
- $\forall x \forall y \big(x + (x \cdot y) = x\big)$ *e* $\forall x \forall y \big(x \cdot (x+y) = x\big)$ *(leggi di assorbimento);*
- $\forall x \forall y \forall z \big(x \cdot (y+z) = (x \cdot y) + (x \cdot z)\big)$ *(proprietà distributiva di* $\cdot$ *rispetto a* $+$*);*
- $\forall x (x + 0 = x)$ *(*0 *è l'elemento neutro rispetto a* $+$*) e* $\forall x (x \cdot 1 = x)$ *(*1 *è l'elemento neutro rispetto a* $\cdot$*);*
- $\forall x (x + \overline{x} = 1)$ *e* $\forall x (x \cdot \overline{x} = 0)$.

Esempio D.3 *In ogni algebra di Boole vale anche la distributiva di* $+$ *rispetto a* $\cdot$*:* $x + (y \cdot z) = (x+y) \cdot (x+z)$.

Soluzione. Partiamo da $x + (y \cdot z)$; per le leggi di assorbimento la possiamo riscrivere come $[x+(x \cdot z)]+(y \cdot z)$ e quindi come $x+[(x \cdot z)+(y \cdot z)]$. Quest'ultima è uguale $x+[(x+y) \cdot z]$ per la distributiva di $\cdot$ rispetto a $+$. Di nuovo grazie alle leggi di assorbimento possiamo riscrivere l'ultima espressione come $[(x+y) \cdot x] + [(x+y) \cdot z]$ che, di nuovo grazie alla distributiva di $\cdot$ rispetto a $+$, diventa $(x+y) \cdot (x+z)$. □

Sia data una certa espressione (un termine o una formula) nel linguaggio delle algebre di Boole. Se sostituiamo ogni $+$ che compare nell'espressione con $\cdot$, ogni $\cdot$ con $+$, ogni 0 con 1 e ogni 1 con 0 otteniamo un'altra espressione che viene detta la *duale* dell'espressione di partenza. Dagli assiomi e dall'esempio precedente è evidente che il duale di un assioma è ancora una formula vera. Ne segue immediatamente il seguente.

(Principio di dualità) Una formula A (nel linguaggio delle algebre di Boole) è vera in ogni algebra di Boole (cioè, è derivabile dagli assiomi) se e solo se lo è la sua duale.

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

$$x \leq y \quad \text{se} \quad x \cdot y = x$$

oppure $x + y = y$.

Proposizione D.4 *La relazione* $\leq$ *definita sopra è una relazione d'ordine parziale.*

Dim: La riflessiva equivale a $\forall x(x \cdot x = x)$ che non è altro che l'idempotenza. Per quanto riguarda l'antisimmetrica, sia $x \leq y$ e $y \leq x$, cioè $x \cdot y = x$ e $y \cdot x = y$; quindi $x = y$ grazie alla commutatività di $\cdot$. Proviamo, infine, la transitiva. Sia $x \leq y$ e $y \leq z$, cioè $x \cdot y = x$ e $y \cdot z = y$. Vogliamo provare che $x \cdot z = x$. Ma $x \cdot z$ è uguale, per la prima ipotesi, a $(x \cdot y) \cdot z$ che sarebbe $x \cdot (y \cdot z)$ grazie alla proprietà associativa di $\cdot$. Applicando la seconda ipotesi otteniamo $x \cdot y$ e quindi x di nuovo per la prima ipotesi. c.v.d.

Si può verificare facilmente che $x+y$ e $x \cdot y$ sono, rispettivamente, l'estremo superiore e l'estremo inferiore del sottoinsieme $\{x, y\}$ rispetto a $\leq$.

Un esempio importante di algebra di Boole è fornito dall'insieme delle parti di un insieme A ponendo: $X = \mathcal{P}(A)$, $+ = \cup$, $\cdot = \cap$, $0 = \emptyset$, $1 = A$ e $^{-}$ l'operazione di complemento. Come è facile verificare, la relazione $\leq$ sarà l'inclusione $\subseteq$.

Un altro esempio notevole si può ottenere a partire dalle formule delle logica classica. Poniamo $X = Frm$ e leggiamo l'uguaglianza di elementi di X come se fosse l'equivalenza fra formule. Inoltre, poniamo $+ =\vee$, $\cdot =\wedge$, $0 = \bot$, $1 = \top(=\neg\bot)$ e $^{-} =\neg$. Di conseguenza si avrà $\leq=\vdash$.

Lemma D.5 *Se $x + y = 1$ e $x \cdot y = 0$ allora $y = \overline{x}$.*

Dim: Da $x + y = 1$ segue $\overline{x} \cdot (x + y) = \overline{x} \cdot 1$, cioè $(\overline{x} \cdot x) + (\overline{x} \cdot y) = \overline{x}$; quest'ultima è $0 + (\overline{x} \cdot y) = \overline{x}$ e quindi $\overline{x} \leq y$.

D'altro canto, da $x \cdot y = 0$ segue $\overline{x}+(x \cdot y) = \overline{x}+0$, cioè $(\overline{x}+x) \cdot (\overline{x}+y) = \overline{x}$; quest'ultima è $1 \cdot (\overline{x} + y) = \overline{x}$ e quindi $y \leq \overline{x}$. c.v.d.

Esempio D.6 *In ogni algebra di Boole valgono le leggi di De Morgan:*

$$\overline{x \cdot y} = \overline{x} + \overline{y} \quad e \quad \overline{x + y} = \overline{x} \cdot \overline{y} \ .$$

Soluzione. Per il principio di dualità basta provarne una sola, ad esempio la prima. Grazie al lemma precedente è sufficiente dimostrare che:

$$(x \cdot y) + (\overline{x} + \overline{y}) = 1 \quad \text{e} \quad (x \cdot y) \cdot (\overline{x} + \overline{y}) = 0 \ .$$

Per la distributiva di $+$ rispetto a $\cdot$, $(x \cdot y) + (\overline{x} + \overline{y})$ è uguale a $[x + (\overline{x} + \overline{y})] \cdot [y + (\overline{x} + \overline{y})]$ che diventa $(1 + y) \cdot (1 + x)$, cioè $1 \cdot 1$ e quindi 1. Invece, $(x \cdot y) \cdot (\overline{x} + \overline{y})$ è uguale a $[(x \cdot y) \cdot \overline{x}] + [(x \cdot y) \cdot \overline{y}]$, cioè $(0 \cdot y) + (0 \cdot x)$ che è uguale a 0. $\square$

D.3 Assioma della scelta e lemma di Zorn

Il concetto di prodotto cartesiano può essere esteso al caso di una famiglia infinita di insiemi. Sia $\{A_i\}_{i\in I}$ una famiglia arbitraria di insiemi e sia $\prod_{i\in I} A_i$ l'insieme di tutte le funzioni f con dominio I e tali che $f(i) \in A_i$, per ogni $i \in I$. Intuitivamente, si può immaginare ognuna di queste funzioni f come una lista di elementi del tipo $f(i)$ ognuno appartenente ad un insieme A_i. Ad esempio, se $I = \mathbb{N}$ si può identificare f con la sua immagine

$$(f(0), f(1), f(2), \ldots, f(n), \ldots) \;\in\; A_0 \times A_1 \times A_2 \times \ldots \times A_n \times \ldots \; .$$

Se $I \neq \emptyset$ e $A_i \neq \emptyset$ per ogni $i \in I$ allora è naturale pensare che anche $\prod_{i\in I} A_i$ debba essere non vuoto. Infatti, si può pensare di costruire una funzione che ad ogni elemento di I associa un elemento di A_i. Questo fatto lo consideriamo come un principio indimostrabile.

Assioma moltiplicativo. Se $\{A_i\}_{i\in I}$ è una famiglia non vuota di insiemi non vuoti allora anche $\prod_{i\in I} A_i$ è non vuoto.

Da questo assioma discende il famoso assioma della scelta.

Proposizione D.7 (Assioma della scelta) *Sia X un insieme non vuoto e sia $\mathcal{P}^*(X)$ l'insieme dei sottoinsiemi non vuoti di X. Allora esiste una funzione*

$$\varphi \;:\; \mathcal{P}^*(X) \;\longrightarrow\; X$$

tale che $\varphi(A) \in A$ per ogni $\emptyset \neq A \subseteq X$.

Dim: Basta applicare l'assioma moltiplicativo con $I = \mathcal{P}^*(X)$ e $A_i = i$ per ogni $\emptyset \neq i \subseteq X$. c.v.d.

La funzione φ della proiposizione precedente viene detta una *funzione di scelta* sull'insieme X. Adesso siamo pronti per dimostrare il lemma di Zorn.

Teorema D.8 *Sia $(X, \leq)$ un insieme non vuoto parzialmente ordinato e supponiamo che ogni catena di X (cioè ogni sottoinsieme di X che sia totalmente ordinato) ammetta almeno un maggiorante (in X). Allora esiste in X almeno un elemento massimale.*

Dim: Sia φ una funzione di scelta su X e sia K una qualsiasi catena di X. Indichiamo con M_K l'insieme (eventualmente vuoto) dei maggioranti *effettivi* di K, cioè gli $y \in X$ tali che $x < y$ per ogni $x \in K$.[1] Infine poniamo:

$$K' = \begin{cases} K & \text{se } M_K = \emptyset \ ; \\ K \cup \{\varphi(M_K)\} & \text{se } M_K \neq \emptyset \ . \end{cases}$$

Per esempio, visto che $M_\emptyset = X$, si ha $\emptyset' = \{\varphi(X)\}$.

Sia Θ l'insieme di catene di X definito per ricorsione dalle seguenti clausole:

1. $\emptyset \in \Theta$;

2. se $K \in \Theta$ allora anche $K' \in \Theta$;

3. se $\{K_i\}_{i\in I}$ è una catena (rispetto a $\subseteq$) di elementi di Θ allora anche $\bigcup_{i\in I} K_i$ è un elemento di Θ.

In altre parole Θ è la piu piccola famiglia di catene di X che soddisfa le proprietà 1, 2 e 3; cioè, Θ è l'intersezione di tutte le famiglie di catene che soddisfano le proprietà richieste.

Vogliamo dimostrare che Θ stessa è una catena rispetto all'inclusione, cioè che tutti gli elementi di Θ sono confrontabili fra loro. Per fare questo consideriamo la famiglia Θ^* che contiene gli elementi di Θ che sono confrontabili con tutti gli altri; cioè, poniamo:

$$\Theta^* = \{K \in \Theta \ : \ (\forall A \in \Theta)(K \subseteq A \vee A \subseteq K)\} \subseteq \Theta$$

e dimostramo che $\Theta = \Theta^*$. Ovviamente basta far vedere che $\Theta \subseteq \Theta^*$ che sarà dimostrato se faremo vedere che Θ^* soddisfa le proprietà 1, 2 e 3 (perchè Θ è la più piccola che le soddisfa).

1. Che $\emptyset \in \Theta^*$ è ovvio (perchè $\emptyset \subseteq A$ per ogni A).

2. Sia $K \in \Theta^*$ e vogliamo provare che anche $K' \in \Theta^*$. Consideriamo la classe:
$$\Psi(K) = \{A \in \Theta \ : \ (A \subseteq K) \vee (K' \subseteq A)\} \subseteq \Theta$$
e proviamo che $\Theta = \Psi(K)$ facendo vedere che $\Psi(K)$ soddisfa le proprietà 1, 2 e 3.

[1] Il simbolo $x < y$ è un'abbreviazione per: $(x \leq y) \wedge (x \neq y)$.

(a) $\emptyset \in \Psi(K)$ perchè $\emptyset \subseteq K$.

(b) Sia $A \in \Psi(K)$ e dimostriamo che anche $A' \in \Psi(K)$. Visto che $K \in \Theta^*$ si possono presentare due casi: $K \subseteq A'$ o $A' \subseteq K$. Nel secondo caso si ha $A' \in \Psi(K)$ e abbiamo finito. Se, invece, $K \subseteq A'$ distinguiamo due sotto casi: $A \subseteq K$ oppure $K' \subseteq A$ (perchè $A \in \Psi(K)$). Nel secondo caso si ha subito che $K' \subseteq A'$ (perchè sempre $A \subseteq A'$) e quindi $A' \in \Psi(K)$. Ci resta quindi da esaminare il caso $A \subseteq K \subseteq A'$. Ma A e A' differiscono al più per un elemento, quindi K deve coincidere con A o con A'. Nel primo caso si ha anche $K' = A'$ e quindi $K' \subseteq A'$. Nel secondo caso si ha in particolare $A' \subseteq K$. Quindi, in ogni caso, vale che: $A' \in \Psi(K)$.

(c) Sia $\{A_i\}_{i \in I}$ una catena (rispetto a $\subseteq$) di elementi di $\Psi(K)$; quindi ognuno degli A_i o è contenuto in K o contiene K'. Se tutti gli A_i sono contenuti in K allora anche $\bigcup_{i \in I} A_i$ è contenuto in K. Se, invece, almeno uno degli A_i contiene K' allora anche $\bigcup_{i \in I} A_i$ contiene K'. In ogni caso, $\bigcup_{i \in I} A_i$ appartiene a $\Psi(K)$.

Visto che Θ è la più piccola famiglia che soddisfa 1, 2 e 3 si ha $\Theta \subseteq \Psi(K)$ e quindi $\Psi(K) = \Theta$ (sotto l'ipotesi che $K \in \Theta^*$). Volevamo provare che $K' \in \Theta^*$, cioè che K' è confrontabile con qualsiasi $A \in \Theta$. Da quanto appena dimostrato segue che $A \in \Psi(K)$; pertanto, o $A \subseteq K$ (e quindi $A \subseteq K'$) o $K' \subseteq A$. In conclusione $K' \in \Theta^*$.

3. Sia $\{K_i\}_{i \in I}$ una catena di elementi di Θ^* e sia A un elemento qualsiasi di Θ. Per ogni K_i si ha: $A \subseteq K_i$ oppure $K_i \subseteq A$. Se succede che tutti i K_i sono contenuti in A, allora anche la loro unione sarà contenuta in A. Se, invece, esiste almeno un K_i che contiene A, allora l'unione di tutti i K_i conterrà A. In ogni caso, si ottiene che $\bigcup_{i \in I} K_i$ è confrontabile con ogni A e quindi appartiene a Θ^*.

In definitiva, Θ^* è una sottofamiglia di Θ che soddisfa le proprietà che definiscono Θ; ne segue che $\Theta = \Theta^*$. Quindi tutti gli elementi di Θ sono confrontabili fra loro; in altre parole, Θ stessa è una catena (rispetto a $\subseteq$). Se poniamo

$$L = \bigcup_{K \in \Theta} K$$

la proprietà 3 ci assicura che $L \in \Theta$ e quindi anche $L' \in \Theta$. Ma L, essendo l'unione di tutti gli elementi di Θ, conterrà anche L' e quindi $L = L'$. Questo significa che M_L, l'insieme dei maggioranti effettivi di L, è vuoto. D'altra parte, L è una catena di elementi di X quindi, per ipotesi, ammette almeno un maggiorante m. Visto che L non ha maggioranti effettivi ne segue che $m \in L$ e quindi m è il massimo di L.

Si vede facilmente che m è un elemento massimale di X. Infatti, se $x \in X$ è tale che $m \leq x$, ma $m \neq x$ allora si avrebbe $m < x$ e quindi x sarebbe un maggiorante effettivo di L, che è assurdo. c.v.d.

In realtà è possibile dimostrare che l'assioma moltiplicativo, l'assioma della scelta e il lemma di Zorn sono tutti equivalenti fra loro.

Esempio D.9 *Ogni spazio vettoriale ammette base.*

Soluzione. Una base è una parte libera massimale. Sia X la famiglia delle parti libere parzialmente ordinata rispetto all'inclusione; X è non vuota perchè $\emptyset$ è una parte libera, cioè $\emptyset \in X$. Sia $\{A_i\}_{i \in I}$ una catena di X e sia $\bar{A}$ l'unione di tutti gli A_i; ovviamente ogni A_i è contenuto in $\bar{A}$. Inoltre, $\bar{A}$ appartiene ad X, cioè è una parte libera; infatti, se così non fosse esisterebbero dei vettori $v_1, \ldots, v_n \in \bar{A}$ linearmente dipendenti. Poichè tali vettori sono un numero finito, sicuramente esisterà un j tale che $v_1, \ldots, v_n \in A_j$, contraddicendo il fatto che A_j è una parte libera.

Riassumendo, X soddisfa le ipotesi del lemma di Zorn e quindi esisterà in X un elemento massimale B. In altre parole B è una parte libera massimale, cioè una base. □

D.4 Cardinalità

Intuitivamente, la cardinalità di un insieme X, indicata con $|X|$, è il numero di elementi di X; ovviamente tale definizione è chiara nel caso di un insieme finito. In questa sezione vedremo i fatti più importanti riguardanti la cardinalità degli insiemi infiniti.

Definizione D.10 *Si dice che due insiemi X e Y (sono* equipotenti *o) hanno la stessa* cardinalità *(o* potenza*), e si scrive $|X| = |Y|$, se esiste una funzione biiettiva fra X e Y (cioè se X e Y possono essere posti in corrispondenza biunivoca).*

Si dice che $|X| \leq |Y|$ se esiste una funzione iniettiva da X verso Y.

Si scrive $|X| < |Y|$ se $|X| \leq |Y|$, ma $|X| \neq |Y|$.

Gli insiemi equipotenti ad $\mathbb{N}$ vengono detti *numerabili*; quelli equipotenti ad $\mathbb{R}$ si dice che hanno la *potenza del continuo*.

Teorema D.11 (di Cantor) *Siano X un insieme e $\mathcal{P}(X)$ il suo insieme delle parti; allora $|X| < |\mathcal{P}(X)|$.*

Dim: Che $|X| \leq |\mathcal{P}(X)|$ è facile; infatti la funzione

$$\begin{array}{ccc} X & \rightarrow & \mathcal{P}(X) \\ x & \mapsto & \{x\} \end{array}$$

è banalmente iniettiva. Rimane da provare che $|X| \neq |\mathcal{P}(X)|$, cioè che non può esistere una biiezione fra X e $\mathcal{P}(X)$. Supponiamo per assurdo che esista una funzione f da X in $\mathcal{P}(X)$ che sia biiettiva e consideriamo il sottoinsieme

$$D = \{x \in X \ : \ x \notin f(x)\} \ .$$

Visto che $D \in \mathcal{P}(X)$ e f è biiettiva esisterà un $d \in X$ tale che $f(d) = D$. Se fosse $d \in D$ allora d dovrebbe godere della proprietà caratteristica degli elementi di D, cioè dovrebbe essere $d \notin f(d)$, cioè $d \notin D$: assurdo. Se, invece, fosse $d \notin D$ allora d soddisferebbe la proprietà caratteristica di D e quindi $d \in D$: assurdo. In ogni caso, si arriva ad un assurdo. c.v.d.

Da questo teorema segue che esistono infinite cardinalità infinite, perchè:

$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < |\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))| < \dots .$$

Si vede facilmente che la relazione $\leq$ fra cardinalità è riflessiva (perchè la funzione identica è iniettiva) e transitiva (perchè la composizione di due funzioni iniettive è anch'essa iniettiva). Si può dimostrare che è anche antisimmetrica (Teorema di Cantor-Berstein).

Corollario D.12 *La classe di tutti gli insiemi non è un insieme.*

Dim: Sia V la classe di tutti gli insiemi. Si consideri la funzione

$$\begin{array}{ccc} \mathcal{P}(V) & \rightarrow & V \\ X & \mapsto & X \end{array}$$

cioè, visto che ogni sottoinsieme di V sarebbe a sua volta un insieme, possiamo associarlo a se stesso. Questa funzione sarebbe banalmente iniettiva e quindi ne seguirebbe $|\mathcal{P}(V)| \leq |V|$ contraddicendo il teorema di Cantor. c.v.d.

Diamo, senza dimostrarla, la seguente caratterizzazione del concetto di insieme infinito.

Teorema D.13 *Dato un insieme X, le tre asserzioni seguenti sono tutte equivalenti fra loro:*

1. *X è infinito;*
2. *X può essere messo in corrispondenza biunivoca con una sua parte propria; cioè, esiste $A \subsetneq X$ tale che $|A| = |X|$;*
3. *X contiene un sottoinsieme numerabile; cioe, $|\mathbb{N}| \leq |X|$.*

Esempio D.14 *L'insieme $\mathbb{N}$ è in corrispondenza biunivoca con una sua parte propria.*

Soluzione. Sia $2\mathbb{N}$ l'insieme dei numeri naturali pari; si vede facilmente che la funzione

$$\begin{array}{ccc} \mathbb{N} & \to & 2\mathbb{N} \\ x & \mapsto & 2x \end{array}$$

è biiettiva. $\square$

Si può vedere facilmente che $\mathbb{Z}$, l'insieme dei numeri interi relativi, è anch'esso numerabile; infatti è possibile pensare i suoi elementi nel modo seguente:

$$0, +1, -1, +2, -2, \ldots, +n, -n, \ldots$$

(cioè si possono numerare). Sorprendentemente, anche l'insieme $\mathbb{Q}$ dei numeri razionali è numerabile. Consideriamo la seguente tabella infinita

$$\begin{array}{llllllll} 0 & & & & & & \\ & \frac{1}{1} & \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \frac{1}{5} & \cdots \\ & \frac{-1}{1} & \frac{-1}{2} & \frac{-1}{3} & \frac{-1}{4} & \frac{-1}{5} & \cdots \\ & \frac{2}{1} & \frac{2}{2} & \frac{2}{3} & \frac{2}{4} & \frac{2}{5} & \cdots \\ & \frac{-2}{1} & \frac{-2}{2} & \frac{-2}{3} & \frac{-2}{4} & \frac{-2}{5} & \cdots \\ & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

che ovviamente contiene tutti i numeri razionali anche con ripetizioni. Se dimostriamo che gli elementi di tale tabella possono essere numerati, a maggior ragione anche $\mathbb{Q}$ sarà numerabile. Partiamo da 0, poi consideriamo $\frac{1}{1}$, quindi $-\frac{1}{1}$ e poi $\frac{1}{2}$; a questo punto mettiamo $\frac{2}{1}$, $-\frac{1}{2}$ e $\frac{1}{3}$ e così via; cioè procediamo sulle diagonali. Si vede subito che così facendo si riescono a numerare tutti gli elementi della tabella; questo procedimento viene detto *metodo diagonale di Cantor*.

In modo simile si riesce a dimostrare che l'insieme $\mathbb{R}$ dei numeri reali non è numerabile, anzi si può provare che $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$.

A questo punto sorge il problema di vedere se esistono delle cardinalità intermedie fra quella del numerabile, di solito indicata con $\aleph_0$ (leggi "alef con zero"), e quella del continuo che, per quanto appena detto, è la cardinalità di $\mathcal{P}(\mathbb{N})$, di solito indicata con $2^{\aleph_0}$ (per analogia con il caso finito). La risposta è che non c'è modo di dimostrare né che tale cardinalità esiste, né che non esiste; in altre parole, gli assiomi della teoria degli insiemi non implicano niente in proposito.[2] Quindi, se si vuole, si può aggiungere come assioma che non esistono cardinalità intermedie fra il continuo e il numerabile; tale assioma è la famosa

(ipotesi del continuo) : non esistono cardinalità k tali che $\aleph_0 < k < 2^{\aleph_0}$.

In altre parole, se si accetta l'ipotesi del continuo, il numero cardinale successivo ad $\aleph_0$ è $2^{\aleph_0}$ che si può quindi indicare con $\aleph_1$.

Si può ipotizzare anche quella che viene chiamata *ipotesi generalizzata del continuo*, cioè che non esistono cardinalità intermedie fra quella di un insieme infinito e quella del suo insieme delle parti. Quindi, per esempio, se vale l'ipotesi del continuo generalizzata si ha:

$$|\mathcal{P}(\mathbb{R})| = 2^{2^{\aleph_0}} = 2^{\aleph_1} = \aleph_2$$

e quindi gli insiemi X tali che $|X| \geq \aleph_2$ sono gli insiemi "più potenti del continuo"!

[2]La situazione è simile a quella che si ha in teoria dei gruppi rispetto all'assioma di commutatività (dell'operazione del gruppo): gli altri assiomi non implicano né che la commutativa valga, né che non valga; quindi è un assioma *indipendente* dagli altri tre.

Bibliografia

[1] G. Boole, *L'analisi matematica della logica*, Bollati Boringhieri, Torino, 1993 [03-A-I-1]

[2] G. Boolos, *The logic of provability*, Cambridge University Press, Cambridge, 1993 [03-B-I-2]

[3] E. Casari, *Lineamenti di logica matematica*, Feltrinelli, Milano, 1960 [C-90 e C-91]

[4] D. R. Hofstadter, *Gödel, Escher, Bach: un'Eterna Ghirlanda Brillante*, Adelphi, Milano, 1984.

[5] S. C. Kleene, *Introduction to metamathematics*, North-Holland, Amsterdam [K-114]

[6] G. Lolli, *Introduzione alla logica formale*, Il Mulino, Bologna, 1991 [03-01-I-2]

[7] G. Lolli, *Incompletezza: saggio su Kurt Gödel*, Il Mulino, Bologna, 1992 [03-D-I-2]

[8] R. Vaught, *Set theory: an introduction*, Birkhäuser, Boston, 1995 [04-00-I-1]

[Fra parentesi quadre la collocazione nella biblioteca del Dipartimento di Matematica ed Applicazioni.]