Francesco Ciraulo

Dispense del corso di
Elementi di Logica Matematica

Per i corsi di laurea triennale in
Matematica per l'Informatica e la Comunicazione Scientifica
e
Matematica
Facoltà di Scienze MM. FF. NN.
Università degli Studi di Palermo

A. A. 2007/08

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 quei ragionamenti che possono essere formulati nel nostro linguaggio naturale (cioè l'Italiano) 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, se... allora, 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:

costanti : $\top$ ("il vero"), $\bot$ ("il falso");

variabili proposizionali : p, q, r, s, t, ...

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

parentesi : (,).

Le costanti e le variabili rappresentano delle proposizioni "atomiche", cioè non contenenti alcun connettivo. I connettivi sono da intendersi come operazioni nell'insieme delle proposizioni o "formule" (vedi definizione successiva). 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:*

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

Il sottoinsieme di Frm formato dalle variabili proposizionali e da $\bot$ e $\top$ è l'insieme delle formule atomiche*. Tutte le altre formule vengono dette "composte".*

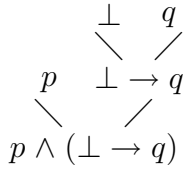
Per esempio, se p e q sono due variabili di $\mathcal{L}$ allora l'espressione (cioè la sequenza di simboli)

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

è una formula. Invece, l'espressione $(p \to) q \neg \wedge \bot$ no lo è.

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 in assoluto, ma soltanto se sia 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[1], detto *albero di costruzione* della formula, che ne descrive la costruzione, appunto, a partire dalle formule atomiche. Ad esempio, l'albero di costruzione di $p \wedge (\bot \to q)$ è il seguente.



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

[1] Vedi pagina 83 per una definizione formale.

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 $p \wedge (\bot \to q)$ sono p, q, $\bot$, $\bot \to q$ e $p \wedge (\bot \to q)$; al contrario, $p \wedge \bot$ *non* è una sottoformula della formula data.

Si definisce *complessità* (o *lunghezza*) di una formula la profondità del corrispondente albero di costruzione, cioè la lunghezza (= numero di tratti) del suo ramo più lungo. Ad esempio, la complessità di una formula atomica è 0, le formule che contengono un solo connettivo hanno complessità 1, mentre la formula dell'esempio precedente ha complessità 2. Nota che la complessità di una formula non coincide con il numero di connettivi che vi compaiono. Ad esempio, la formula $(p \wedge \bot) \vee (p \to q)$ ha profondità 2, anche se contiene 3 connettivi. In altre parole, la complessità non misura semplicemente quanti connettivi ci sono in una formula, ma piuttosto qual è il numero massimo di *annidamenti* fra i connettivi.

Capitolo 2

Semantica: tavole di verità.

In questo capitolo definiremo i connettivi $\wedge$, $\vee$, $\rightarrow$, $\neg$ (e anche le costanti $\top$ e $\bot$) 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.[1] 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.[2] Ovviamente, qualora le formule da considerare siano più di una, le classi di interpretazioni da considerare saranno più di due.

[1] Vedi pagina 68 (logica intuizionistica) per un diverso approccio al concetto di verità.

[2] In certi testi, viene usato 0 al posto di F e 1 al posto di V.

Ad esempio, se abbiamo due formule A e B, allora 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 delle costanti tramite la seguente tavola.

Definizione semantica di connettivi e costanti

A	B	$A \wedge B$	$A \vee B$	$A \to B$	$\neg A$	$\top$	$\bot$
V	V	V	V	V	F	V	F
V	F	F	V	F	F	V	F
F	V	F	V	V	V	V	F
F	F	F	F	V	V	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.

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).

Senza dubbio, la tavola di verità più difficile da digerire è quella relativa all'implicazione. Soprattutto risulta difficile accettare che una cosa falsa implichi qualsiasi cosa. Le seguenti argomentazioni potrebbero essere di aiuto.

Intanto, è bene notare che una frase vera è sempre implicata da qualsiasi altra frase, anche falsa. Infatti, supponiamo di stare parlando di numeri interi e sia B la frase "$x^2 \geq 0$", che è vera (qualsiasi sia x); inoltre sia A la frase "$x < 0$". Chiaramente, la frase $A \to B$, cioè "se $x < 0$ allora $x^2 \geq 0$" è (banalmente) vera, perchè lo è già B senza bisogno dell'ipotesi A.

Quindi se B è vera, a maggior ragione lo è $A \to B$. In particolare, una frase falsa implica una frase vera. Del resto "falso implica falso" lo si crede facilmente; è quindi spiegata la tavola dell'implicazione.

Un altro modo per convincersi che la tavola di $A \to B$ sia corretta è di considerare il seguente esempio. Supponiamo di parlare di numeri naturali e consideriamo la frase:

$$\text{se } x \text{ è divisibile per 10 allora } x \text{ è pari}$$

che è ovviamente vera, qualsiasi sia x. Ma se prendiamo come x, rispettivamente, 20, 4 e 3 allora ci accorgiamo che l'antecedente e il conseguente hanno valori di verità, rispettivamente, V e V, F e V, F e F (e nonostante ciò, la frase in totale è vera perchè abbiamo detto che è vera per ogni valore di x).

In definitiva, dire che $A \to B$ è vera significa soltanto dire che non può presentarsi il caso in cui A sia vera, ma B falsa. In altre parole, anziché definire quando $A \to B$ è vera, è più facile definire quando è falsa: $A \to B$ è falsa quando A è vera e B falsa; cioè:

$$\neg\,(A \to B) \quad \textit{è equivalente a} \quad A \wedge (\neg\, B)\ .$$

Un modo un pò meno formale, ma sicuramente più divertente, di capire perchè dal falso segue tutto è di riflettere sul seguente ipotetico dialogo fra due amici:

```
A: Sai che sono capace di diventare invisibile?!
B: Si, certo! E io sono Babbo Natale!
```

Per ultimo, è sicuramente utile (oltre che divertente) leggere la seguente storia (si dice che sia un fatto realmente accaduto).
Durante una conferenza, un famoso matematico enuncia il celebre principio

ex falso quodlibet (dal falso segue tutto). Una persona fra il pubblico, scettica sulla validità di tale principio, sfida il matematico a dimostrare che da $0 = 1$ segue che lui sia Babbo Natale. "Facile!" esclama il matematico; "se $0 = 1$ allora, sommando 1 ad entrambi i membri, anche $1 = 2$. Quindi lei e Babbo Natale, che siete 2 persone, in realtà siete 1 persona sola!"

Da un punto di vista intuitivo, fare un'interpretazione significa attribuire un significato alle formule, cioè sostituirle con delle frasi italiane di senso compiuto. Da un punto di vista matematico, però, è più semplice immaginare una fissata interpretazione come una funzione che associa ad ogni formula un valore di verità.

Definizione 2.1 *Un'interpretazione (o "valutazione") è una funzione*

$$val \ : \ Frm \ \longrightarrow \ \{V, F\}$$

che rispetta le definizioni dei connettivi; cioè:

- $val(\top) = V$ *e* $val(\bot) = F$*;*
- $val(A \wedge B) = V$ *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* $val(B) = V$*;*
- $val(A \to B) = F$ *se e solo se* $val(A) = V$ *e* $val(B) = F$*;*
- $val(\neg\, A) = V$ *se e solo se* $val(A) = F$*;*

per ogni $A, B \in Frm$*.*

Si può intuire facilmente, che per descrivere una funzione di valutazione, è sufficiente assegnare un valore di verità alle variabili proposizionali; tutto il resto viene di conseguenza. Ad esempio, se $A = (p \to \bot) \wedge \neg\, q$ allora il valore $val(A)$ dipende dalla scelta di $val(p)$ e $val(q)$. Ad esempio, se $val(p) = F$ e $val(q) = V$ allora risulta $val(A) = F$.

Le funzioni *val* possibili dipendono dal numero di variabili proposizionali che compaiono nel linguaggio. In generale, se in un linguaggio ci sono n variabili proposizionali, allora il numero delle funzioni *val* sarà 2^n. In pratica, ogni funzione di valutazione corrisponde ad una riga della tavola di verità.

Per convenzione, se $\Gamma \subseteq Frm$, scriviamo

$$val(\Gamma) = V$$

come abbreviazione di: "$val(C) = V$ per ogni $C \in \Gamma$".

Definizione 2.2 *Siano A una formula e Γ un insieme di formule (cioè $\Gamma \subseteq Frm$). Con il simbolo $\Gamma \models A$ intendiamo che A risulta vera in ogni interpretazione in cui tutte le formule di Γ risultano vere.*

In altre parole, la scrittura $\Gamma \models A$ abbrevia la frase italiana: "non esiste una riga della tavola di verità in cui A sia falsa e tutte le formule di Γ siano vere". Un altro modo equivalente di leggere $\Gamma \models A$ è "per ogni interpretazione, se $val(\Gamma) = V$ allora anche $val(A) = V$".

Si dice che una formula A è una *tautologia* e si scrive $\models A$ se A risulta vera in ogni interpretazione. Si dice che una formula A è una *contraddizione* se A risulta falsa in ogni interpretazione.[3]

Se due formule A e B hanno la stessa tavola di verità, cioé se sono vere esattamente nelle stesse interpretazioni, allora si dicono *(semanticamente) equivalenti* e si scive $A \equiv_{sem} B$. Chiaramente, $A \equiv_{sem} B$ equivale a dire che $A \models B$ e $B \models A$.

2.1 Esempi

Esempio 2.3 *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. □

[3] Attenzione: per dire che A è una contraddizione, si scrive $\models \neg A$. Invece, il simbolo $\not\models A$ significa semplicemente che A non è una tautologia, cioè che esiste almeno una interpretazione in cui A è falsa (ma non è detto che A sia sempre falsa).

Esempio 2.4 *Costruire la tavola di verità del connettivo $\leftrightarrow$ (doppia implicazione) definito da:*

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

Soluzione.

A	B	$A \rightarrow B$	$B \rightarrow A$	$A \leftrightarrow B$
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 2.5 *Sia $\Gamma = A, A \rightarrow B$; dimostrare che $\Gamma \models B$.*

Soluzione. Bisogna provare che $val(B) = V$ ogni volta che val è tale che $val(\Gamma) = V$. Pertanto, supponiamo di avere una funzione val tale che $val(\Gamma) = V$. Per definizione di $val(\Gamma) = V$, si ha sia $val(A) = V$ che $val(A \rightarrow B) = V$. Supponiamo per assurdo che $val(B) = F$. Allora da $val(A) = V$ e $val(B) = F$ seguirebbe $val(A \rightarrow B) = F$, per definizione di $val(A \rightarrow B)$. Ma questo è assurdo, perché va contro l'ipotesi $val(A \rightarrow B) = V$.

□

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 di dimostrazione; cioè stabiliremo quali sono i modi corretti di fare un ragionamento. Anche se questo approccio potrà sembrare più laborioso, sarà in effetti più comodo quando introdurremo i quantificatori.

In generale, una regola è qualcosa del tipo

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

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 è un'abbreviazione della seguente frase italiana: *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:

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

$$\frac{A}{A \vee B} \vee i\,(sx) \qquad \frac{B}{A \vee B} \vee i\,(dx) \qquad \frac{\begin{array}{ccc}[A]' & [B]' & \\ \vdots & \vdots & \\ C & C & A \vee B\end{array}}{C}\ ' \vee e$$

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

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

$\frac{A}{\top}$ (*il vero segue da qualsiasi cosa*) $\qquad \frac{\bot}{A}$ (*dal falso segue tutto*)

$$\frac{\begin{array}{c}[\neg A]' \\ \vdots \\ \bot\end{array}}{A}\ ' \text{ (}regola\ di\ riduzione\ all'asurdo\text{)}$$

dove A, B e C sono formule arbitrarie; i sta per "introduzione" ed e per "eliminazione". 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.

Ovviamente, ogni regola non è altro che la scrittura simbolica di una frase italiana. Ad esempio, la $\wedge\ i$ dice:

($\wedge\ i$) se come ipotesi ho sia A che B allora posso concludere $A \wedge B$.

Più precisamente, la regola di $\wedge\ i$ andrebbe letta così: *se da certe ipotesi* Γ_1 *posso derivare* A *e da certe ipotesi* Γ_2 *posso derivare* B *allora dall'insieme*

di ipotesi $\Gamma_1 \cup \Gamma_2$ *posso dimostrare* $A \wedge B$. In altre parole, la forma più completa della regola di $\wedge$-introduzione è :

$$\dfrac{\begin{array}{cc}\Gamma_1 & \Gamma_2 \\ \vdots & \vdots \\ A & B\end{array}}{A \wedge B} \ .$$

Per un altro esempio, consideriamo la regola di $\rightarrow \ i$. Essa è semplicemente un modo simbolico di abbreviare la seguente frase: se da certe ipotesi Γ e dall'ipotesi A, prese assieme, posso derivare B, allora dalle sole ipotesi Γ (senza A) posso derivare $A \rightarrow B$ (ma in generale non posso derivare B).

Come ultimo esempio, guardiamo la regola di $\vee \ e$: se da Γ_1 e A posso derivare C, da Γ_2 e B posso derivare C e da Γ_3 posso derivare $A \vee B$, allora C lo posso derivare direttamente dalle ipotesi $\Gamma_1 \cup \Gamma_2 \cup \Gamma_3$. Per capire meglio la $\vee$-eliminazione è utile leggerla senza le ulteriori ipotesi Γ_i: se da A posso derivare C, ma anche da B posso derivare C, allora C lo posso derivare direttamente da $A \vee B$. In altre parole, se come ipotesi ho $A \vee B$ e voglio dimostrare la tesi C, allora (visto che non so quale fra A e B sia vera) devo far vedere che posso arrivare a C sia nel caso in cui A sia vera, sia nel caso in cui sia B ad essere vera.

Una dimostrazione (nel calcolo della deduzione naturale) della formula B a partire dalle premesse $A_1, \ldots, A_n$ 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

$$\dfrac{\dfrac{A \wedge B}{A}\ \wedge\ e\ (sx)}{A \vee B}\ \vee\ i\ (sx) \qquad \dfrac{\dfrac{A \wedge B}{B}\ \wedge\ e\ (dx)}{A \vee B}\ \vee\ i\ (dx)$$

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

$$\dfrac{\dfrac{\dfrac{\bot \qquad [\neg A]^1}{\bot \wedge (\neg A)}\ \wedge\ i}{\bot}\ \wedge\ e\ (sx)}{A}\ 1\ (rid.\ assurdo)$$

dimostra che dal falso segue tutto (quindi la regola "dal falso segue tutto" è superflua). Quando la formula B è dimostrabile a partire dalle ipotesi A_1, $\ldots$, A_n scriveremo

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

Nota che il simbolo $\vdash$ non è un connettivo, bensì un legame meta-linguistico; in altre parole è solo un'abbreviazione di una frase italiana. Quindi $A \vdash B$ *non* è una formula, cioè non appartiene a Frm, ma è soltanto la frase: "dalla formula A è possibile derivare la formula B". Di conseguenza, $A \vdash B$ è qualcosa che non ha bisogno di essere interpretata perché ha di per sé un suo significato, cioé è gia vera o falsa.

La scrittura $\vdash A$ significa che la formula A è dimostrabile (senza premesse). Nel caso in cui $A \vdash B$ e anche $B \vdash A$ scriveremo $A \equiv B$ (o, meglio, $A \equiv_{sint} B$ per distinguerla dall'equivalenza semantica).

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.

Teorema 3.1 (di deduzione) *Per ogni $A, B \in Frm$ e ogni $\Gamma \subseteq Frm$ si ha:*

$$\Gamma, A \vdash B \quad \textit{se e solo se} \quad \Gamma \vdash (A \to B) \quad .$$

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

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

$$\dfrac{\Gamma \quad \begin{array}{c}[A]^1 \\ \vdots \\ B\end{array}}{A \to B}\ {\scriptstyle 1 \to i} \qquad \dfrac{\begin{array}{c}\Gamma \\ \vdots \\ A \quad A \to B\end{array}}{B}\ {\scriptstyle \to e}$$

ipotesi (per entrambe le figure)

c.v.d.

Proposizione 3.2 *Per ogni $A_1, \ldots, A_n, B \in Frm$ si ha:*

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

Dim: Per semplicità dimostriamo solo il caso $n = 2$.

$$\dfrac{\dfrac{A_1 \wedge A_2}{A_1} \quad \dfrac{A_1 \wedge A_2}{A_2}}{\begin{array}{c}\vdots \\ B\end{array}}\ \textit{ipotesi} \qquad \dfrac{\dfrac{A_1 \quad A_2}{A_1 \wedge A_2}}{\begin{array}{c}\vdots \\ B\end{array}}\ \textit{ipotesi}$$

c.v.d.

3.1 Esempi

Esempio 3.3 *Dimostrare che $\wedge$ e $\vee$ sono operazioni commutative sull'insieme delle formule (modulo equivalenza).*

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

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

□

Esempio 3.4 *Provare che $\wedge$ e $\vee$ sono idempotenti, cioè che vale $A \wedge A \equiv A$ e $A \vee A \equiv A$.*

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 3.5 (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 $A \vee (B \vee C) \vdash (A \vee B) \vee C$.

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

□

Esempio 3.6 (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 $A \wedge (B \vee C) \vdash (A \wedge B) \vee (A \wedge C)$.

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

□

Esempio 3.7 (Leggi di assorbimento)

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

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

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

□

Esempio 3.8 (Principio d'identità) $\vdash (A \to A)$

Soluzione.

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

□

Esempio 3.9 (Principio di non contraddizione) $\vdash \neg\, (A \wedge \neg\, A)$

Soluzione.

$$\dfrac{\dfrac{[A \wedge \neg\, A]^1}{A}\ {}^{\wedge\, e} \quad \dfrac{[A \wedge \neg\, A]^1}{\neg\, A}\ {}^{\wedge\, e}}{\dfrac{\bot}{\neg\, (A \wedge \neg\, A)}\ {}^{1\ \to\, i}}\ {}^{\to\, e}$$

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

Esempio 3.10 (Principio del terzo escluso) $\vdash (A \vee \neg\, A)$

Soluzione.

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

□

Esempio 3.11 (Principio della doppia negazione) $(\neg\neg A) \equiv A$

Soluzione.

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

□

Esempio 3.12 (Leggi di De morgan)

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

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

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

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

□

Esempio 3.13 $(A \to B) \equiv (\neg A \vee B)$

Soluzione.

$$\dfrac{\dfrac{\dfrac{[A]^1 \quad A \to B}{B}\ \to e}{\neg A \vee B}\ \vee i \qquad \dfrac{\dfrac{[\neg A]^1}{\neg A \vee B}\ \vee i \qquad \begin{array}{c}\emptyset \\ \vdots \\ A \vee \neg A\end{array}\ \textit{terzo escluso}}{\neg A \vee B}\ {}_1\ \vee e$$

$$\dfrac{\dfrac{\dfrac{[A]^1 \quad [\neg A]^2}{\dfrac{\bot}{B}}\ \neg e}{A \to B}\ {}_1\ \to i \qquad \dfrac{[B]^2}{A \to B}\ \to i \qquad \neg A \vee B}{A \to B}\ {}_2\ \vee e$$

□

Capitolo 4

Complementi

4.1 Forma normale congiuntiva

Definizione 4.1 *Sia A una formula proposizionale. Si dice che A è in* forma normale congiuntiva *(abbreviato f.n.c.) 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.

Cioè A è in f.n.c. se è *una congiunzione di disgiunzioni di letterali*, dove un letterale è una formula atomica o una negazione di una formula atomica.

Definizione 4.2 *Se $A \equiv B$ e B è in f.n.c. si dice che B è* una f.n.c. *di A.*

Il prossimo teorema afferma che ogni formula ammette una f.n.c.. Nota che ogni formula ammette infinite f.n.c. (ovviamente tutte fra loro equivalenti). Ad esempio $\neg\, p \vee q$ è una f.n.c. di $p \rightarrow q$, ma anche $(\neg\, p \vee q) \wedge (r \vee \neg\, r)$ lo è.

Teorema 4.3 *Ogni formula ammette una f.n.c.. Più precisamente, esiste un algoritmo, che è il seguente, che permette di passare da una formula ad una sua f.n.c.:*

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

2. *si sostituisce ogni sottoformula del tipo* $\neg (A \wedge B)$ *con* $\neg A \vee \neg B$ *e ogni* $\neg (A \vee B)$ *con* $\neg A \wedge \neg B$*; si ripete questo punto tutte le volte necessarie;*

3. *si sostituisce ogni sottoformula del tipo* $A \vee (B \wedge C)$ *con* $(A \vee B) \wedge (A \vee C)$*; si ripete tutte le volte necessarie;*

4. *si sostituisce ogni* $\neg\neg A$ *con* A*; si ripete se necessario;*

(per semplicità, è sottointeso che si possono applicare le proprietà commutativa e associativa di $\wedge$ *e* $\vee$ *ogni volta che si vuole).*

Dim: Intanto notiamo che ogni passo dell'algoritmo trasforma una formula in un'altra equivalente; quindi l'output dell'algoritmo sarà senza'altro una formula equivalente a quella di partenza.

Per dimostrare il teorema occorre provare due cose: primo, che l'algoritmo veramente termina dopo un numero finito di passi, cioè che non può mai succedere di dovere applicare uno stesso punto infinite volte; secondo, che l'output dell'algoritmo è veramente una formula in f.n.c..

Il primo punto dell'algoritmo si applica sicuramente per un numero finito di volte (= il numero degli $\to$ che compaiono nella formula di partenza).

Il secondo passaggio è più problematico perchè toglie un $\neg$ e ne fa comparire due: come facciamo ad essere sicuri che prima o poi finiremo? Possiamo ragionare così. Consideriamo una sottoformula del tipo $\neg (A \wedge B)$ (il caso con la $\vee$ è perfettamente simmetrico); in essa il connettivo $\neg$ abbraccia una formula (cioè $A \wedge B$) in cui il connettivo $\wedge$ compare sicuramente un numero maggiore di volte rispetto a quanto succede in A o in B. Per esempio, se in A la $\wedge$ appare tre volte e in B due, allora in $A \wedge B$ appare sei volte. Se sostituiamo $\neg (A \wedge B)$ con $\neg A \vee \neg B$ otteniamo, invece, due $\neg$ che abbracciano formule in cui la $\wedge$ compare meno volte. Così facendo, prima o poi (cioè in un numero finito di passi), otteniamo tanti $\neg$ che abbracciano formule prive di $\wedge$. In altre parole, il secondo punto dell'algoritmo si può applicare solo un numero finito di passi e poi si deve andare necessariamente al punto successivo.

In questo caso dobbiamo fare un discorso analogo al precedente, ma guardando ad $\vee$ anziché a $\neg$. Se in A, B e C supponiamo che la $\wedge$ compaia,

rispettivamente, a volte, b volte e c volte, allora in $A \vee (B \wedge C)$ la $\vee$ abbraccia complessivamente $a+b+c+1$ congiunzioni, mentre in $(A \vee B) \wedge (A \vee C)$ compaiono due $\vee$, ma ognuno di essi abbraccia meno di $a + b + c + 1$ congiunzioni (precisamente, il primo $\vee$ ne abbraccierà $a + c$, mentre il secondo $a + b$).

Infine, l'ultimo punto. Chiaramente si può applicare soltanto un numero finito di volte, perché ad ogni passo fa sparire due negazioni e il numero delle negazioni presenti in una formula non può essere infinito.

Ci resta da provare che l'output dell'algoritmo è veramente in f.n.c.. Infatti: non può contenere $\rightarrow$ perchè viene tolto al primo punto; non può contenere dei $\neg$ che abbracciano formule non atomiche, grazie al secondo punto; non può contenere $\vee$ che abbracciano $\wedge$, per il terzo punto; infine, non può comparire la stringa $\neg\neg$, grazie all'ultimo punto. Pertanto, i $\neg$, se ci sono, possono abbracciare soltanto formule atomiche e le $\vee$ solo letterali.

c.v.d.

4.2 Forma normale disgiuntiva

In maniera simmetrica (basta scambiare i ruoli di $\wedge$ e $\vee$) rispetto al caso delle f.n.c. si può definire il concetto di *forma normale disgiuntiva* (f.n.d.) e si può dimostrare che ogni formula ammette f.n.d..

Le f.n.d. di una formula sono intimamente legate alla tavola di verità della formula stessa. Vediamolo con un esempio. Se A è una formula e

$$(p \wedge q \wedge \neg\, r) \vee (p \wedge \neg\, q)$$

è una sua f.n.d. allora la tavola di verità di A sarà:

p	q	r	A
V	V	V	F
V	V	F	V
V	F	V	V
V	F	F	V
F	V	V	F
F	V	F	F
F	F	V	F
F	F	F	F

cioè A è vera solo in due casi: primo, quando $val(p) = val(q) = V$ e $val(r) = F$; secondo, quando $val(p) = V$ e $val(q) = F$ ($val(r)$ qualsiasi).

Viceversa, se di una formula conosciamo la sua tavola di verità, allora ne possiamo subito trovare una sua f.n.d.. Ad esempio, visto che la disgiunzione esclusiva fra p e q è vera esattamente quando $val(p) = val(\neg\, q)$, cioè seconda e terza riga della sua tavola di verità, allora una sua f.n.d. sarà sicuramente:

$$(p \wedge \neg\, q) \vee (\neg\, p \vee q)\ .$$

4.3 Usare soltanto $\bot$ e $\rightarrow$.

L'insieme dei connettivi e delle costanti di un linguaggio $\mathcal{L}$ può essere ridotto al solo $\{\rightarrow, \bot\}$. Per verificarlo, dobbiamo definire tutti gli altri connettivi tramite questi due:

- $\neg\, A = (A \rightarrow \bot)$;
- $\top = \neg\, \bot = (\bot \rightarrow \bot)$;
- $A \vee B = ((\neg\, A) \rightarrow B) = ((A \rightarrow \bot) \rightarrow B)$;
- $A \wedge B = \neg\, (A \rightarrow (\neg\, B)) = (A \rightarrow (B \rightarrow \bot)) \rightarrow \bot$.

Inoltre, come regole di deduzione, possiamo usare soltanto le seguenti:

$$\frac{A \quad A \rightarrow B}{B} \rightarrow -e \qquad \frac{\begin{array}{c}[A]\\ \vdots \\ B\end{array}}{A \rightarrow B} \rightarrow -i \qquad \frac{\begin{array}{c}[A \rightarrow \bot]\\ \vdots \\ \bot\end{array}}{A}\ a$$

a patto che facciamo vedere che tutte le altre derivano da queste e dalle definizioni dei connettivi date sopra. Come esempio dimostriamo la $\wedge\, -e$ e la $\vee\, -e$ che, con le definizioni date sopra, diventano:

$$\frac{(A \rightarrow (B \rightarrow \bot)) \rightarrow \bot}{A} \qquad \frac{(A \rightarrow (B \rightarrow \bot)) \rightarrow \bot}{B} \qquad \frac{\begin{array}{cc}[A] & [B]\\ \vdots & \vdots \\ C & C\end{array} \quad (A \rightarrow \bot) \rightarrow B}{C}$$

e si dimostrano così:

$$\dfrac{\dfrac{\dfrac{[A]^1 \quad [A \to \bot]^2}{\bot} \to -e}{B \to \bot} \to -i}{A \to (B \to \bot)}\,{}^{1} \to -i \qquad (A \to (B \to \bot)) \to \bot}{\dfrac{\bot}{A}\,{}^{2}\,a} \to -e$$

$$\dfrac{\dfrac{[B \to \bot]^1}{A \to (B \to \bot)} \to -i \qquad (A \to (B \to \bot)) \to \bot}{\dfrac{\bot}{B}\,{}^{1}\,a} \to -e$$

$$\dfrac{\dfrac{\dfrac{\dfrac{[A]^1}{\vdots\ ipotesi}}{C} \qquad [C \to \bot]^2}{\bot} \to -e}{A \to \bot}\,{}^{1} \to -i \qquad (A \to \bot) \to B}{\dfrac{B}{\dfrac{\vdots\ ipotesi}{C}} \qquad [C \to \bot]^2}{\dfrac{\bot}{C}\,{}^{2}\,a} \to -e} \to -e$$

4.4 Il calcolo alla Hilbert

Solo per conoscenza, accenniamo ad un modo equivalente di presentare la logica proposizionale classica. Possiamo sostituire ogni regola con uno schema di assiomi (uno schema di assiomi è un'infinità di assiomi aventi tutti la stessa forma). Ad esempio, la regola di $\wedge$ i (nella sua forma più generale) può essere resa tramite lo schema: $((C \to A) \wedge (C \to B)) \to (C \to (A \wedge B))$ (un assioma per ogni terna di formule A, B e C).

Grazie al fatto che è possibile usare solo $\to$ e $\bot$, come (schemi di) assiomi si possono prendere i seguenti:

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

2. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$

3. $((A \to \bot) \to (B \to \bot)) \to (B \to A)$

(per ogni A, B e C in Frm).

Ovviamente, i soli assiomi non sono sufficienti; occorre almeno una regola (meta-linguistica). La scelta più naturale è di prendere l'$\to$-eliminazione, che tradizionalmente viene chiamata "modus ponens":

$$\frac{A \quad A \to B}{B}\ MP\ .$$

Esempio 4.4 *Dimostrare $A \to A$, qualsiasi sia A.*

Soluzione. $A \to ((B \to A) \to A)$ è un'istanza dell'assioma 1; per lo schema 2 si ha anche $(A \to ((B \to A) \to A)) \to ((A \to (B \to A)) \to (A \to A))$ e quindi $(A \to (B \to A)) \to (A \to A)$ per modus ponens. Da quest'ultimo e da $A \to (B \to A)$ (schema 1) segue $A \to A$ (modus ponens). □

Per semplificare le dimostrazioni, di solito si usano anche altri schemi di assiomi per gli altri connettivi:

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

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

$A \wedge B \to A \qquad A \wedge B \to B$

$A \to A \vee B \qquad B \to A \vee B$

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

Capitolo 5

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).

5.1 L'enunciato del teorema di completezza

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

Teorema 5.1 (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 ogni interpretazione; in altre parole, le regole del calcolo sono corrette. Il teorema di completezza, invece, afferma che le regole sono anche sufficienti a dimostrare ogni tautologia; cioè non abbiamo bisogno di aggiungere ulteriori regole.

5.2 Teorema di validità: dimostrazione.

In questa sezione dimostreremo il teorema di validità nella seguente forma:

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

con $A \in Frm$ e $\Gamma \subseteq Frm$. Da questa seconda forma del teorema si ottiene, ovviamente, la prima come caso particolare (quando $\Gamma = \emptyset$). In realtà le due forma sono equivalenti.

Dim: Per induzione (seconda forma; vedi appendice sui numeri naturali) sulla lunghezza n della dimostrazione di $\Gamma \vdash A$.

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

   $$A$$

   e quindi A deve essere fra le ipotesi, cioè $A \in \Gamma$. Di conseguenza, ogni volta che $val(\Gamma) = V$ anche $val(A) = V$ (per definizione di $val(\Gamma)$).

2. Adesso supponiamo che il teorema sia vero per tutte le prove di lunghezza minore di n e dimostriamolo per n. Distinguiamo vari casi a seconda dell'ultima regola usata nella derivazione. Sappiamo che possiamo limitarci alle regole sull'implicazione e a quella di riduzione all'assurdo.

   (a) Se l'ultima regola applicata è quella di $\rightarrow$-introduzione, allora A è del tipo $(B \rightarrow C)$ e la prova di $\Gamma \vdash A$ appare così:

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

   Per ipotesi induttiva, vale che $\Gamma, B \models C$; in altre parole, se $val(\Gamma)$ e $val(B)$ sono entrambe V allora anche $val(C) = V$. Noi vogliamo

provare che $\Gamma \models (B \to C)$; supponiamo, quindi, che $val(\Gamma)$ sia vera e distinguiamo due casi. Se B è falsa, allora $B \to C$ è vera. Se B è vera allora $val(\Gamma) = V = val(B)$ e quindi, per ipotesi induttiva, anche C deve essere vera; di conseguenza, anche in questo caso $B \to C$ è vera. Riassumendo, $B \to C$ risulta vera in ogni caso in cui $val(\Gamma) = V$.

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

$$\dfrac{\begin{array}{cc}\Gamma & \Gamma \\ \vdots & \vdots \\ B & B \to A\end{array}}{A}$$

per qualche B e C in Frm. L'ipotesi induttiva ci assicura che $\Gamma \models B$ e $\Gamma \models (B \to A)$. Quindi, se $val(\Gamma) = V$ allora $val(B) = V$ e $val(B \to A) = V$; pertanto A deve necessariamente essere vera (vedi tavola di verità dell'implicazione).

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

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

Per provare che $\Gamma \models A$, basta far vedere che è impossibile che $val(\Gamma) = V$ e $val(A) = F$. Infatti, se fosse $val(\Gamma) = V$ e $val(\neg A) = V$ allora, per ipotesi induttiva, seguirebbe che $val(\bot) = V$, che è impossibile.

c.v.d.

5.3 Teorema di completezza: dimostrazione.

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

Lemma 5.2 *Se* $\Gamma, B \vdash A$ *e* $\Gamma, \neg B \vdash A$ *sono entrambi dimostrabili allora anche* $\Gamma \vdash A$ *lo è.*

Dim:

$$\dfrac{\Gamma, [B]' \quad \Gamma, [\neg\, B]' \qquad\qquad \vdots}{A \qquad\quad A \qquad B \vee \neg\, B}\ ,$$

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. Ad esempio, $\widetilde{\bot}$ è sempre uguale a $\neg\, \bot$, cioè $\top$.

Lemma 5.3 *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. Se usiamo soltanto $\rightarrow$ come connettivo, allora A è del tipo $B \rightarrow C$. In questo caso 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 $P_A = P_B \cup P_C$. Per l'ipotesi induttiva, si ha $\widetilde{P_B} \vdash \widetilde{B}$ e $\widetilde{P_C} \vdash \widetilde{C}$. Possiamo distinguere tre casi a seconda dei valori di verità di B e C: B potrebbe essere falsa (e C qualsiasi); C potrebbe essere vera (e B qualsiasi); B potrebbe essere vera e C falsa. I tre alberi seguenti

$$\dfrac{\dfrac{\dfrac{\widetilde{P_B}}{\vdots}}{\dfrac{[B]' \quad \neg\, B}{\bot}}}{\dfrac{C}{B \rightarrow C}}\ , \qquad \dfrac{\dfrac{\widetilde{P_C}}{\vdots}}{\dfrac{C}{B \rightarrow C}} \qquad \dfrac{\dfrac{\widetilde{P_B}}{\vdots} \qquad\qquad \dfrac{\widetilde{P_C}}{\vdots}}{\dfrac{\dfrac{B \quad [B \rightarrow C]'}{C} \qquad \neg\, C}{\bot}}}{\neg\, (B \rightarrow C)}\ ,$$

dimostrano la tesi nei tre casi, rispettivamente (nota che A risulta vera nei primi due casi, falsa nel terzo).

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:

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

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

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

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

$$\vdots \qquad \vdots \qquad \vdots \qquad \vdots \qquad \vdots$$

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

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

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 varie ($= 2^{n-1}$) applicazioni del primo lemma ci ritroviamo con 2^{n-1} condizioni. Ripetendo il procedimento se ne ottengono 2^{n-2} e così via. Dopo aver ripetuto il procedimento per $n-1$ volte 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.

Come nel caso del teorema di validità, anche il teorema di completezza può essere dimostrato (vedi il caso predicativo) in una sua forma più generale, cioè con l'aggiunta di ipotesi Γ a sinistra. Pertanto, la forma più generale del teorema di validità e completezza per la logica proposizionale classica è la seguente.

Teorema 5.4 *Siano $\mathcal{L}$ un linguaggio proposizionale, $A \in Frm_{\mathcal{L}}$ e $\Gamma \subseteq Frm_{\mathcal{L}}$. Allora $\Gamma \vdash A$ se e solo se $\Gamma \models A$.*

Dim: (solo per il caso in cui Γ è finito; per il caso di Γ arbitrario, vedi la dimostrazione del teorema di completezza nel caso predicativo)

Sia $\Gamma = \{B_1, \ldots, B_n\}$; allora: $\Gamma \vdash A$ se e solo se $(B_1 \wedge \ldots \wedge B_n) \vdash A$ se e solo se (teorema di deduzione) $\vdash (B_1 \wedge \ldots \wedge B_n) \rightarrow A$ se e solo se (teorema di completezza, caso $\Gamma = \emptyset$) $\models (B_1 \wedge \ldots \wedge B_n) \rightarrow A$, cioè $(B_1 \wedge \ldots \wedge B_n) \rightarrow A$ è una tautologia. Ci si convince facilmente che $(B_1 \wedge \ldots \wedge B_n) \rightarrow A$ è una tautologia se e solo se $B_1, \ldots, B_n \models A$, cioè $\Gamma \models A$. c.v.d.

Come corollario del teorema di completezza si ottiene che le due nozioni di equivalenza semantica e di equivalenza sintattica, in effetti, coincidono.

Corollario 5.5 *Siano $A, B \in Frm_{\mathcal{L}}$. Allora:*

$$A \equiv_{sem} B \quad \textit{se e solo se} \quad A \equiv_{sint} B \ .$$

Dim: $A \equiv_{sem} B$ se solo se $A \models B$ e $B \models A$ se e solo se $A \vdash B$ e $B \vdash A$ se e solo se $A \equiv_{sint} B$. c.v.d.

Parte II

La logica dei predicati

Capitolo 6

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 così:

$$(\forall x \in \mathbb{R})(x \neq 0 \to (\exists y \in \mathbb{R})(x \cdot y = 1))$$

mentre la frase "ogni sottoinsieme non vuoto dei reali che sia limitato superiormente ammette estremo superiore" ha bisogno della logica del secondo ordine; infatti, la sua formalizzazione è del tipo $(\forall U \subseteq \mathbb{R})(\ldots)$ ed ha bisogno, quindi, di usare sia l'insieme $\mathbb{R}$ che il suo insieme delle parti.

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 di regole.

Per cominciare, analizziamo il seguente esempio: "il quadrato di un numero reale non nullo è sempre positivo". Di solito esso viene scritto simbolicamente così: $(\forall x \in \mathbb{R})(x \neq 0 \to x^2 > 0)$. 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 (cioè con due argomenti), ma ha un ruolo particolare, come vedremo; infine, x^2 è una funzione (unaria, cioè di una sola variabile). In generale, quindi, possiamo dare la seguente definizione.

Definizione 6.1 *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 $P, Q, \ldots$ ognuno con la sua molteplicità (o* arietà*);*
- *i connettivi $\wedge$, $\vee$, $\rightarrow$, $\neg$, $\bot$ e $\top$;*
- *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*. Ad esempio, la scrittura $)x \rightarrow f(a))P(x, y) \neg$ non è un'espressione ben formata.

Le espressioni ben formate si possono dividere in due classi: quelle che descrivono degli elementi del dominio (termini) e quelle che esprimono delle frasi (formule). Ad esempio, nell'insieme dei numeri reali, l'espressione $x^2 + \sqrt{2}$ è un termine perché rappresenta un numero (incognito), mentre $x = x^2 + \sqrt{2}$ è una formula.

Definizione 6.2 *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:*

  - $\bot, \top \in Frm$;
  - *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* $(A \wedge B), (A \vee B), (A \to B), (\neg A) \in Frm$;
  - *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, l'=, i connettivi, i quantificatori, ecc.), 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 $(\exists y(x \cdot y = e))$ è una formula.

A sua volta, l'insieme dei termini (e, come vedremo dopo, anche quello delle formule) si divide in due categorie: i termini *aperti*, che sono quelli che contengono variabili, e i termini *chiusi*, che non ne contengono. Continuando l'esempio del linguaggio dei gruppi, il termine $(x \cdot e)^{-1} \cdot y$ è aperto (quindi individua un elemento incognito), mentre $(e \cdot e)^{-1} \cdot e$ individua un elemento ben preciso.

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

[1] A volte, per semplificare, considereremo anche $\bot$ e $\top$ fra le formule atomiche.

6.1 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 $\int f(1)\ \mathrm{d}1$ 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:

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

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 (con alcuni accorgimenti) 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: $\int f(t)\ \mathrm{d}t$. Bisogna fare attenzione, però, ad alcuni accorgimenti. Nell'esempio $F(x) = \int_0^x f(t)\ \mathrm{d}t$, possiamo cambiare il nome alla variabile libera; ad esempio, possiamo chiamarla z e ottenere la frase $F(x) = \int_0^x f(z)\ \mathrm{d}z$ che è equivalente a quella di partenza. Di solito, però, si preferisce evitare di sostituire a t la stessa variabile x perché la formula che si otterrebbe potrebbe cambiare significato. Ad esempio, la frase $(\exists y \in \mathbb{Q})(x \cdot y = 2)$, che contiene x come variabile libera, è certamente equivalente a $(\exists z \in \mathbb{Q})(x \cdot z = 2)$, ma ha un significato diverso rispetto a $(\exists x \in \mathbb{Q})(x \cdot x = 2)$. Infatti, le prime due contengono una variabile libera e quindi il loro valore di verità dipende dal valore assegnato a tale variabile. La terza formula, invece, non contiene variabili libere e quindi il suo valore di verità è fissato (in questo caso è falsa); quindi ha un significato diverso dalle prime due.

Riassumendo, quando si cambia nome ad una variabile, bisogna stare attenti a non far cambiare il significato della frase. Una buona regola pratica

è quella di non usare mai lo stesso nome per due variabili diverse. Ad esempio, se si incontra la formula $A(x) \vee \exists x B(x) \vee \forall x C(x)$ è meglio riscriverla come $A(x) \vee \exists y B(y) \vee \forall z C(z)$ (ovviamente, abbiamo cambiato nome alle variabili legate, ma non alla variabile che compare in A che è libera).

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 7

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*. Quindi 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, cioè delle variabili libere. 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 qualsiasi $x \in \mathbb{R}$, 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 7.1 *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 *(il* dominio *dell'interpretazione);*
- *una funzione* $\sigma : Var \longrightarrow D$ *(*assegnazione per le 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. Di conseguenza, si può scrivere $\sigma(a)$ al posto di a_D e $\sigma(f(x, y))$ al posto di $f_D(\sigma(x), \sigma(y))$.

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 7.2 *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:

- $val(\bot) = F$ *e* $val(\top) = V$*;*
- *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* $val(B) = V$*;*
- $val(A \to B) = V$ *se e solo se* $val(A) = F$ *e/o* $val(B) = V$*;*

- *$val(\neg A) = V$ se e solo se $val(A) = F$;* [1]
- *$val(\forall x\ A(x)) = V$ se, presa comunque un'altra assegnazione 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'.*[3]

Per semplicità, con un pò di abuso di linguaggio, dato un elemento $d \in D$ diremo "$val(A(d)) = V$ in D" anziché il più corretto "$val(A(t)) = V$ in D, σ dove $\sigma(t) = d$".

Pertanto, le due condizioni sulla valutazione di $\forall$ e $\exists$ le possiamo leggere così:

- $val(\forall x\ A(x)) = V$ se $val(A(d)) = V$ per ogni $d \in D$;
- $val(\exists x\ A(x)) = V$ se esiste un $d \in D$ tale che $val(A(d)) = V$.

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 7.3 *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 7.4 *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 $val(A) = V$.

[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.

[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.

[3] Significa che esiste un elemento di D che sostituito al posto di x rende vera $A(x)$.

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

Ovviamente, il simbolo $\models A$ significa che A è sempre vera, cioè è universalmente valida. Nota, invece, che dire che A è soddisfacibile, equivale a dire che $\neg A$ non è universalmente valida; di conseguenza la soddisfacibilità di A si può esprimere con il simbolo $\not\models \neg A$ o, equivalentemente, con $A \not\models \bot$ (visto che $\neg A$ è equivalente a $A \to \bot$). Pertanto, il simbolo $\Gamma \not\models \bot$ equivale a dire che Γ è soddisfacibile.

Proposizione 7.5 *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 $val(\forall y A(y)) = V$ 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

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

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:

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

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 7.6 *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 $val(A(t)) = V$. □

Esempio 7.7 *Se $t \in Trm$, la formula $A(t) \rightarrow \exists x A(x)$ è valida.*

Soluzione. Simmetrica rispetto alla precedente. □

Proposizione 7.8 *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 7.9 *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 8

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.

8.1 Le regole per i quantificatori

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

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

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 y come termine t; 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:

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

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:

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

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 *finito*) 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].

Definizione 8.1 *Se $\Gamma \vdash \bot$ 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:

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

$(A, B \in Frm)$.

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 fra le ipotesi effettivamente utilizzate (Γ potrebbe essere infinito).

Teorema 8.2 (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; infatti se vale $K \vdash A$ per un certo $K \subseteq \Gamma$, a maggior ragione deve valere $\Gamma \vdash A$.

Per l'altro verso, basta considerare l'albero di una dimostrazione di $\Gamma \vdash A$ (che esiste per ipotesi) e prendere come K l'insieme delle formule che compaiono come foglie (non scaricate); K è, quindi, finito e contenuto in Γ.

c.v.d.

8.2 Esempi

Esempio 8.3 *Dimostrare che:* $\neg \forall x A(x) \vdash \exists x \neg A(x)$*, per ogni formula* A.

Soluzione.

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

Con z libero per x in $A(x)$. □

Esempio 8.4 *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.

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

Con z libero per x in A. □

Capitolo 9

Complementi

9.1 Forma normale prenessa

Definizione 9.1 *Una formula predicativa si dice in* forma normale prenessa *se è del tipo*

$$Q_1 x_1 \; Q_2 x_2 \; \cdots \; Q_n x_n \; A$$

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 (cioè da sinistra a destra!) 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.

9.2 Usare soltanto $\bot$, $\to$ e $\exists$.

Sappiamo che, nel caso proposizionale, ci si può limitare ad usare soltanto $\to$, $\bot$ e le loro tre regole. Nel caso predicativo, ovviamente, occorre aggiungere almeno un quantificatore e le sue regole. Ad esempio, possiamo scegliere di usare solo $\exists$ (e le sue due regole) e definire $\forall x A(x)$ come $\neg\ \exists x\ \neg\ A(x)$ o, meglio:

$$(\exists x(A(x) \to \bot)) \to \bot\ .$$

Dobbiamo, però, verificare che le regole sul $\forall$ sono derivabili, come si vede dalle seguenti dimostrazioni:

$$\dfrac{\dfrac{\dfrac{[A(t) \to \bot]^1}{\exists x(A(x) \to \bot)}\ \exists - i \qquad (\exists x(A(x) \to \bot)) \to \bot}{\dfrac{\bot}{A(t)}\ {}_1\ a}\ \to -e$$

$$\dfrac{\begin{array}{c}\Gamma \\ \vdots \\ A(z)\end{array} \qquad \dfrac{\dfrac{[A(z) \to \bot]^1}{\bot}\ \to -e \qquad \exists x(A(x) \to \bot)}{\dfrac{\bot}{(\exists x(A(x) \to \bot)) \to \bot}\ {}_2\ \to -i}\ {}_1\ \exists - e}{\text{ipotesi}}$$

(nota che il passaggio di $\exists - e$ è lecito perchè z non compare in Γ (e, ovviamente, neanche in $\bot$) perchè l'abbiamo come ipotesi nella regola di $\forall - i$ che vogliamo dimostrare).

9.3 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.

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

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

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

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

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. Quindi bisogna aggiungere qualche altra proprietà.

Quello appena fatto è un caso molto semplice di una proprietà generale dell'uguaglianza, detta *principio di Leibnitz*[1]: "se y è uguale ad x allora possiamo sostituire 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 di una nuova regola: siano t e t' due termini tali che $t = t'$ e sia A una formula in cui compare t; allora la formula che si ottiene sostituendo t' al posto di t è equivalente ad A. Vogliamo dire che se nella formula A compare t e sappiamo che $t' = t$ allora possiamo sostituire t' a t tutte le volte che compare t, ma anche, se preferiamo, solo in alcuni punti. Ad esempio, nella frase $(2^3) : (2^3) = 1$ possiamo sostituire 8 al posto di 2^3 sia entrambe le volte in cui compare sia una volta sola; in ogni caso otteniamo frasi vere: $8 : 8 = 1$, $8 : (2^3) = 1$ e $(2^3) : 8 = 1$.

Dobbiamo inventarci un simbolo per esprimere la sostituzione di t' a t non ovunque (che sarebbe il simbolo $A(t')$), ma solo in un punto particolare. Scegliamo il simbolo $A[t']$. In altre parole, quando scriviamo $A[t]$ non solo vogliamo dire che t compare in A, ma anche che stiamo pensando ad un punto particolare in cui compare.

Prendiamo quest'ultima regola e la proprietà riflessiva come regole ufficiali sull'uguaglianza:

$$\frac{}{t = t}\ riflessiva \qquad \frac{A[t] \quad t = t'}{A[t']}\ Leibnitz$$

con $t, t' \in Trm$, $A[t] \in Frm$ e t' libera per l'occorrenza di t in considerazione.

A questo punto, si può vedere che queste regole sono sufficienti per dimostrare anche la proprietà simmetrica e quella transitiva:

$$\frac{\overline{x = x}\ riflessiva \quad x = y}{y = x}\ Leibnitz$$

prendendo come $A[x]$ la formula $x = x$ relativamente alla prima occorrenza di x e

$$\frac{x = y \quad y = z}{x = z}\ Leibnitz$$

[1] ... o Leibniz?!

con $A[y] : x = y$ come prima ipotesi della regola.

Esempio 9.2 *Sia $\mathcal{L} = \{\ldots, f, \ldots =\}$ un linguaggio con uguaglianza contenete un simbolo di funzione unaria f. Dimostare che se $x = y$ allora anche $f(x) = f(y)$.*

Soluzione.

$$\dfrac{\dfrac{}{f(x) = f(x)}\ {\scriptstyle riflessiva} \qquad x = y}{f(x) = f(y)}\ {\scriptstyle Leibnitz}$$

dove l'ipotesi $A[x]$ della regola di Leibnitz in questo caso è $f(x) = f(x)$ rispetto alla seconda occorrenza di x. □

Ovviamente, le due regole sull'uguaglianza corrispondono, come tutte le regole, a due schemi di assiomi:

$$t = t \qquad \text{(un assioma per ogni } t \in Trm\text{)};$$

$$A[t] \wedge (t = t') \to A[t'] \qquad \text{(un assioma per ogni } A \in Frm \text{ e } t, t' \in Trm\text{)}.$$

9.3.1 Il quantificatore $\exists!$

Nella pratica matematica si è soliti usare formule del tipo $\exists! x P(x)$ col significato di: "esiste un unico x che soddisfa la proprietà P". Tali formule sono da considerarsi delle abbreviazioni di:

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

Capitolo 10

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 10.1 *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).

10.1 Il teorema di validita

Teorema 10.2 (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 cinque casi a seconda dell'ultima regole usata nella dimostrazione di $\Gamma \vdash A$ (ricordiamo che possiamo supporre di usare soltanto le regole di $\bot$, $\rightarrow$ ed $\exists$).

  $\rightarrow$-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.

  $$\dfrac{\begin{array}{cc} \Gamma & \Gamma \\ \vdots & \vdots \\ B & B \rightarrow A \end{array}}{A}$$

  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 $val(\bot) = V$, per l'ipotesi induttiva, che è assurdo.

  $\exists$-introduzione. In questo caso, si ha $A = \exists x B(x)$ e

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

  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 in D. 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:

$$\dfrac{\begin{array}{cc}\Gamma, [B(z)]' & \Gamma \\ \vdots & \vdots \\ A & \exists x B(x)\end{array}}{A},$$

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.

10.2 Il 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 10.3 *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 (cioè consistente) è anche soddisfacibile, cioè ha un modello. Ci serviranno alcuni risultati preliminari.

10.2.1 Insiemi consistenti massimali

Definizione 10.4 $\Gamma \subseteq Frm$ *si dice* consistente massimale *se:*

1. Γ *è consistente; cioè* $\Gamma \nvdash \bot$*;*
2. Γ *è massimale; cioè, se* $\Gamma' \supsetneq \Gamma$ *allora* Γ' *è contraddittorio (cioè* $\Gamma' \vdash \bot$*).*

Proposizione 10.5 *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.[1] Per dimostrare che è limitata superiormente (in F) basta esibirne un maggiorante (in F). Sia

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

[1] In realtà possiamo supporre che la catena sia non vuota, cioè che l'insieme degli indici I è non vuoto. Infatti, nel caso limite di una catena vuota (l'insieme vuoto è banalmente una catena) è facile trovarne un maggiorante: basta prendere Γ stesso.

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 $\overline{\Gamma} \vdash \bot$. Allora, per il teorema di finitezza deve esistere un $K \subseteq \overline{\Gamma}$, K finito, tale che $K \vdash \bot$. Ma se K è finito allora deve esistere un $n \in \mathbb{N}$ tale che $K \subseteq \Gamma_n$. Allora, da $K \vdash \bot$ seguirebbe $\Gamma_n \vdash \bot$ 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 $\Gamma' \supsetneq \Delta$ 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 10.6 *Sia $\Delta \subseteq Frm$ consistente massimale. Se $\Delta \vdash A$ allora $A \in \Delta$.*

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

In particolare, 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 $A \vdash B$; quindi $\Delta \vdash B$ e $B \in \Delta$.

Corollario 10.7 *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 $\Delta, A \vdash \bot$. In altre parole si ha $\Delta \vdash \neg A$ e quindi $\neg A \in \Delta$ per il lemma precedente. c.v.d.

Proposizione 10.8 *Se $\Delta \subseteq Frm$ è consistente massimale allora:*

1. $\neg A \in \Delta \iff A \notin \Delta$
2. $\bot \notin \Delta \iff \top \in \Delta$
3. $A \wedge B \in \Delta \iff A \in \Delta$ *e* $B \in \Delta$
4. $A \vee B \in \Delta \iff A \in \Delta$ *o* $B \in \Delta$
5. $A \to B \in \Delta \iff A \notin \Delta$ *o* $B \in \Delta$
6. $\forall x A(x) \in \Delta \implies A(t) \in \Delta$ *per ogni* $t \in Trm$
7. $\exists x A(x) \in \Delta \impliedby$ *esiste un* $t \in Trm$ *tale che* $A(t) \in \Delta$

Dim:

1. Conseguenza del corollario precedente.

2. Ovvio, perchè Δ è consistente e perché $\top$ è dimostrabile.

3. Visto che $A \wedge B \vdash A$, $A \wedge B \vdash B$ e $A, B \vdash A \wedge B$ basta applicare il lemma precedente.

4. 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).

5. 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.

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

7. 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.

Prima di procedere vogliamo fare alcuni esempi.

Siano Γ gli assiomi della teoria dei gruppi (con l'uguaglianza) sul linguaggio $\mathcal{L} = \{e, \cdot, \ldots\}$. Ovviamente, l'insieme $\mathbb{Z}_2$ delle classi resto modulo 2 è un modello di Γ, rispetto all'operazione $+$ e all'elemento neutro 0 (classe zero). I termini chiusi di questo linguaggio (cioè e, $e \cdot e$, ecc.) corrispondono tutti, quando interpretati, alla classe 0. Quindi, non esiste un termine di $\mathcal{L}$ che rappresenta la classe 1. Di conseguenza, la formula $(\exists x)(x \neq e)$ è vera in $\mathbb{Z}_2$, ma non c'è nessun termine t del linguaggio tale che la formula $t \neq e$ sia vera.

Fissiamo un'assegnazione σ (ad esempio $\sigma(x) = 0$, per ogni x) e consideriamo adesso l'insieme $\Delta = \{A \in Frm_{\mathcal{L}} \ : \ A \text{ è vera in } \mathbb{Z}_2, \sigma\}$. Si può verificare facilmente che Δ è consistente massimale.[2] Per prima cosa, proviamo che Δ è consistente. Infatti, se per assurdo fosse $\Delta \vdash \bot$ allora, per il teorema di validità, si avrebbe $\Delta \models \bot$. Questo significa che non potrebbe esistere un modello di Δ, che non è vero perché $\mathbb{Z}_2$ lo è per definizione. In secondo luogo, per provare che Δ è massimale, si può ragionare così. Sia Δ' che contiene propriamente Δ; quindi esiste un B che appartiene a Δ', ma non a Δ. Di conseguenza, B è falso in $\mathbb{Z}_2$, mentre $\neg B$ è vero; cioè $\neg B \in \Delta$. Allora Δ' conterrebbe sia B che $\neg B$ e sarebbe, quindi, contraddittorio.

Concludendo, questo Δ sarebbe consistente massimale, ma non verificherebbe l'inverso dell'ultimo punto della proposizione precedente. Il motivo risiede nel fatto che il linguaggio $\mathcal{L}$ non permette di rappresentare classe 1; in questo caso, basterebbe aggiungere a $\mathcal{L}$ una nuova costante.

Un esempio di insieme consistente massimale in cui valgono anche le altre proprietà sui quantificatori si può ottenere ripetendo la costruzione dell'esempio precedente a partire, anziché da $\mathbb{Z}_2$, da un gruppo banale (cioè con un solo elemento).

[2] Questo è un fatto generale. Se D, σ è un modello di un certo insieme di assiomi Γ, allora l'insieme delle formule che sono vere in D, σ risulta essere consistente massimale.

10.2.2 Espansione di un linguaggio e assiomi di Henkin

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. Partiamo dal nostro linguaggio $L_0 = \mathcal{L}$ 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.[3] Chiamiamo L_1 il linguaggio che si ottiene aggiungendo ad L_0 tutte queste nuove costanti. 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}. Ad esempio, se c è una delle costanti che abbiamo aggiunto per formare L_1 (e quindi c non appartiene ad L_0), allora la formula $x = c$ appartiene a Frm_{L_1}, ma non a Frm_{L_0}. 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; $A(x)$ sarà scritta usando 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

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

viene chiamata l'*assioma di Henkin* relativo alla formula $A(x)$.[4] Indichiamo

[3] Se, per esempio, una formula A contiene due variabili libere, diciamo x e y, allora aggiungeremo due nuove costanti $c_{A,x}$ e $c_{A,y}$. Nota anche che se $A(x)$ e $B(x)$ sono due formule differenti, allora anche i simboli $c_{A,x}$ e $c_{B,x}$ saranno diversi.

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

con H l'insieme di tutti gli assiomi di Henkin. Ovviamente, possiamo immaginare H come l'unione infinita $H_0 \cup H_1 \cup \ldots \cup H_n \cup \ldots$, dove H_i è l'insieme degli assiomi di Henkin relativi alle costanti c aggiunte al passo i-esimo. In altre parole, in H_i ci stanno quegli assiomi di Henkin che possiamo scrivere nel linguaggio L_i, ma non prima.

Lemma 10.9 *Sia $\mathcal{L}$ un linguaggio, $\overline{\mathcal{L}}$ la sua espansione di Henkin e H l'insieme degli assiomi di Henkin relativi ad $\overline{\mathcal{L}}$. Allora, se $\Gamma \subseteq Frm_{\mathcal{L}}$ è consistente, anche $\Gamma \cup H \subseteq Frm_{\overline{\mathcal{L}}}$ è consistente.*

Dim: Infatti, se per assurdo fosse $\Gamma, H \vdash \bot$ allora, per il teorema di finitezza, esisterebbe un insieme finito K di assiomi di Henkin tale che $\Gamma, K \vdash \bot$. Procediamo per induzione sulla cardinalità n di K. Vogliamo provare che si arriverebbe a un assurdo.

Se $n = 0$ si avrebbe $\Gamma \vdash \bot$ che è assurdo perchè Γ è consistente.

Se $n > 0$, supponiamo che

$$K = \{(\exists x A_1(x) \to A(c_{A_1,x})), \ldots, (\exists x A_n(x) \to A(c_{A_n,x}))\}$$

con ogni $\exists x A_i(x) \to A(c_{A_i,x})$ appartenente ad un certo H_{m_i}, $i = 1, \ldots, n$. A meno di riordinare gli elementi di K, possiamo supporre che $m_i \leq m_j$ ogni volta che $i < j$. In altre parole, se $i < j$ allora la costante $c_{A_j,x}$ non può comparire nell'assioma $\exists x A_i(x) \to A(c_{A_i,x})$; infatti, anche nel caso limite in cui $m_i = m_j$, le costanti $c_{A_j,x}$ e $c_{A_i,x}$ sono diverse, perché relative a formule differenti.

Supponiamo adesso che il teorema sia vero per n. Supponiamo che K abbia cardinalità $n+1$ e che $K = K' \cup \{\exists x A_{n+1}(x) \to A(c_{A_{n+1},x})\}$ (con K' di cardinalità n). Per ipotesi induttiva, $\Gamma \cup K'$ è consistente; poniamo $\Gamma' = \Gamma \cup K'$ e, per semplicità, scriviamo semplicemente A al posto di A_{n+1} e c al posto di $c_{A_{n+1},x}$. Da $\Gamma', \exists x A(x) \to A(c) \vdash \bot$ segue $\Gamma' \vdash\neg\ (\exists x A(x) \to A(c))$ e quindi $\Gamma' \vdash \exists x A(x) \wedge\neg\ A(c)$. In altre parole, si avrebbe sia $\Gamma' \vdash \exists x A(x)$ che $\Gamma' \vdash\neg\ A(c)$. Ma c, cioè $c_{A_{n+1},x}$, non compare in Γ'; infatti c non può comparire in Γ in quanto Γ è scritto nel linguaggio $\mathcal{L}$, che non contiene c fra i suoi simboli; inoltre $c_{A_{n+1},x}$ non può neanche appartenere a K' perché, per ipotesi, la costante $c_{A_{n+1},x}$ è stata aggiunta dopo quelle che compaiono in K'. Quindi c, nella prova di $\Gamma' \vdash\neg\ A(c)$, si comporta come se fosse una variabile che non compare in Γ'. In altre parole è possibile provare, per $\forall$-introduzione, che $\Gamma' \vdash \forall x\ \neg\ A(x)$; 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 $\Gamma' \vdash \bot$ che è assurdo.

c.v.d.

Lemma 10.10 *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 (cioè se $H \subseteq \Delta$), 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: Supponiamo che $\exists x A(x) \in \Delta$; ma Δ contiene anche l'assioma di Henkin $\exists x A(x) \rightarrow A(c_{A,x})$ 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.

10.2.3 La prova del teorema di completezza

Adesso siamo pronti a dimostrare il teorema di completezza.

Teorema 10.11 (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 $t_1 \ldots t_n$ associa $f(t_1, \ldots, t_n) \in Trm = D$. Inoltre consideriamo l'identità come assegnazione σ (cioè $\sigma(x) = x$ per ogni x), che si può fare, ovviamente, perché ogni variabile, in quanto termine del linguaggio, è anche

un elemento del nostro dominio. 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:

$$val(P(t_1, \ldots, t_n)) = V \qquad \stackrel{def.}{\iff} \qquad P(t_1, \ldots, t_n) \in \Delta \ .$$

Sia adesso A una formula qualsiasi; vogliamo provare che:

$$val(A) = V \qquad \iff \qquad A \in \Delta \ .$$

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).

10.3 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 10.12 (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, $\Gamma \vdash \perp$ 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 10.13 *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

Logiche non classiche

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.

A.1 Logica intuizionistica

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 *togliere* la regola di riduzione all'assurdo.

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:

- $\neg\neg A \vdash A$;
- $\vdash A \vee \neg A$;
- $A \to B \vdash \neg A \vee B$;
- $\neg (A \wedge B) \vdash (\neg A) \vee (\neg B)$;
- $\neg \forall x A(x) \vdash \exists x \neg A(x)$.

Per la semantica della logica intuizionistica vedi l'appendice sulle algebre di Heyting.

A.2 Logiche modali

Vanno sotto il nome di *logiche modali* una varietà di sistemi logici accomunati dall'intento di descrivere le frasi e i ragionamenti che coinvolgono i concetti di possibile e necessario. Di solito, data una certa frase A, vengono usati i simboli (detti "modalità") $\Box A$ e $\Diamond A$ per abbreviare le frasi "A è necessaria" e "A è possibile", rispettivamente. Ovviamente, a seconda di cosa si intende per necessario e possibile, risulta naturale dare certi assiomi piuttosto che altri. Senza scendere troppo nei particolari, la maggior parte dele logiche modali moderne sono tutte estensioni di un particolare sistema chiamato K, in onore del logico Saul Kripke. La logica K è definita aggiungendo alle regole della logica proposizionale classica le seguenti due, dette N (regola di necessitazione) e K, rispettivamente:

$$\frac{\begin{array}{c}\emptyset\\ \vdots\\ A\end{array}}{\Box A}\ N \qquad\qquad \frac{\Box A \quad \Box(A \to B)}{\Box B}\ K\ .$$

Di solito $\Diamond A$ viene definito come $\neg\,\Box\,\neg\,A$. La seguente proposizione ha come corollario che le modalità rispettano l'equivalenza fra formule.

Proposizione A.1 *Per ogni A e B, se $A \vdash B$ allora $\Box A \vdash \Box B$ e $\Diamond A \vdash \Diamond B$.*

Dim: Per quanto riguarda la prima parte, basta considerare l'albero:

$$\dfrac{\Box A \quad \dfrac{\dfrac{\begin{array}{c}[A]^1\\ \vdots\ ipotesi\\ B\end{array}}{A \to B}\ {\scriptstyle 1}\ \to -i}{\Box(A \to B)}\ N}{\Box B}\ K\ .$$

Infine, si noti che da $A \vdash B$ segue $\neg\ B \vdash \neg\ A$ (contronominale) e quindi $\Box\,\neg\,B \vdash \Box\,\neg\,A$ per la prima parte. Passando alla contronominale si ottiene $\neg\,\Box\,\neg\,A \vdash \neg\,\Box\,\neg\,B$ che, per definizione, non è altro che $\Diamond A \vdash \Diamond B$. c.v.d.

Esempio A.2 *Dimostrare che nella logica modale K valgono:*

$$\Box(A \wedge B) \equiv (\Box A) \wedge (\Box B) \quad e \quad \Diamond(A \vee B) \equiv (\Diamond A) \vee (\Diamond B)\ .$$

Soluzione. Visto che $A \wedge B \vdash A$ allora, per la proposizione precedente, anche $\Box(A \wedge B) \vdash \Box A$; similmente $\Box(A \wedge B) \vdash \Box B$. Di conseguenza $\Box(A \wedge B) \vdash (\Box A) \wedge (\Box B)$ per $\wedge$-introduzione. Viceversa:

$$\dfrac{\dfrac{(\Box A) \wedge (\Box B)}{\Box B} \qquad \dfrac{\dfrac{(\Box A) \wedge (\Box B)}{\Box A} \qquad \dfrac{\begin{matrix}\emptyset \\ \vdots \\ A \to (B \to A \wedge B)\end{matrix}}{\Box(A \to (B \to A \wedge B))}\ N}{\Box(B \to A \wedge B)}}{\Box(A \wedge B)}\ .$$

Inoltre $\Diamond(A \vee B) \equiv$ (per definizione) $\neg \Box \neg (A \vee B) \equiv$ (De Morgan) $\neg \Box(\neg A \wedge \neg B) \equiv$ (per quanto appena visto) $\neg ((\Box \neg A) \wedge (\Box \neg B)) \equiv$ (De Morgan) $\neg (\Box \neg A) \vee \neg (\Box \neg B)$ $\equiv$ (per definizione) $(\Diamond A) \vee (\Diamond B)$. $\Box$

Nella logica K non è dimostrabile né $(\Box A) \to A$, né $(\Box A) \to (\Box\Box A)$. Per poterle dimostrare bisogna aggiungere nuovi assiomi, rispettivamente:

$$\dfrac{\Box A}{A}\ T \qquad\qquad \dfrac{\Box A}{\Box\Box A}\ 4$$

La logica che si ottiene aggiungendo la regola T e la regola 4 viene indicata con il simbolo $S4$. Quindi la logica $S4$ ha come regole tutte quelle della logica proposizionale classica più le regole N, K, T e 4.

Appendice B

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.

B.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 $x \in \mathbb{N}$.

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

Dati questi assiomi, è possibile definire le usuali operazioni di addizione e moltiplicazione e poi dimostrarne le note proprietà. Prima si definisce l'addizione per ricorsione:

1. $x + 0 = x$
2. $x + s(y) = s(x + y)$

per ogni x e y. Ad esempio $1 + 1 = 1 + s(0) = s(1 + 0) = s(1) = 2$; oppure $0 + 2 = 0 + s(1) = s(0 + 1) = s(0 + s(0)) = s(s(0 + 0)) = s(s(0)) = s(1) = 2$. Una volta definita l'addizione, si può definire la moltiplicazione:

1. $x \cdot 0 = 0$
2. $x \cdot s(y) = (x \cdot y) + x$

per ogni x e y. Infine si può porre: $x \leq y$ se e solo se esiste $z \in \mathbb{N}$ tale che $y = x + z$.

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 B.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 B.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.

B.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):

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

Inoltre, si può vedere che è necessario aggiungere esplicitamente i simboli $+$ e $\cdot$ per l'addizione e la moltiplicazione insieme agli assiomi

- $\forall x(x + 0 = x)$, $\forall x \forall y(x + s(y) = s(x + y))$;

- $\forall x(x \cdot 0 = 0)$, $\forall x \forall y(x \cdot s(y) = x \cdot y + x)$.

Invece, non occorre dare assiomi per $\leq$ perché si puo definire:

$$x \leq y \quad \stackrel{def}{\iff} \quad (\exists z)(x + z = y) \ .$$

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:

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

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 B.3 (primo teorema di incompletezza di Gödel) *Sia $\mathcal{L} = \{=, 0, s, +, \cdot, x_1, \ldots, x_n, \ldots\}$ 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 un numero finito di nuovi schemi di assiomi, a patto che il sistema di assiomi che si ottiene sia coerente.[1] Quindi, anche se si aggiunge agli assiomi la formula G di cui parla il teorema, dovrà

[1]Nota che se si parte da un sistema di assiomi contraddittorio, cioè tale che si possa derivare il falso, allora il teorema non vale; infatti, visto che dal falso segue tutto, non ci può essere una formula non dimostrabile. In altre parole, se da certi assiomi si può derivare il falso, allora si può derivare ogni formula (sia vera che falsa).

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 (che non sono altro che alberi finiti). 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, sappiamo che il fattoriale di un numero n (cioè $n! = n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1$) può essere definito ricorsivamente (quindi c'è un algoritmo) dalle seguenti condizioni:

$$\begin{aligned} 0! &\stackrel{def}{=} 1 \\ (n+1)! &\stackrel{def}{=} (n+1) \cdot (n!) \qquad \text{per } n \geq 0 \ . \end{aligned}$$

Di conseguenza, si può dimostrare che esiste una formula, diciamo $Fatt(x, y)$, che rappresenta il fattoriale, nel seguente senso: se sostituiamo ad x il termine corrispondente ad un certo numero n (cioè $s(\ldots s(0))$ con s ripetuto n volte; per comodità tale termine lo indicheremo pure con n) e a y il termine corrispondente a $n!$ allora $Fatt(n, n!)$ è dimostrabile (a partire da $\mathcal{P}$; cioè $\mathcal{P} \vdash Fatt(x, y)$); inoltre è dimostrabile anche la formula

$$\exists! y Fatt(x, y) \quad \equiv \quad \exists y \big(Fatt(x, y) \wedge (\forall z)(Fatt(x, z) \rightarrow z = y) \big)$$

che dice che esiste uno e un solo y tale che $Fatt(x, y)$. Sotto queste condizioni, è usanza denotare con $fatt(x)$ l'unico y tale che $Fatt(x, y)$.[2]

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

[2]Nota che $fatt(x)$ è solo un'abbreviazione; ogni volta che vogliamo considerare una frase in cui compare $fatt(x)$, tipo $P(fatt(x))$, in realtà dobbiamo scrivere $\exists y(Fatt(x, y) \wedge P(y))$, oppure $\forall y(Fatt(x, y) \rightarrow P(y))$.

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 (come nel caso del fattoriale) 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 (ovviamente a patto che la teoria sia coerente).

La situazione quasi paradossale è, quindi, questa: se un sistema di assiomi è incoerente allora da esso si può dimostrare tutto, anche che il sistema è coerente (cosa, quest'ultima, che è ovviamente falsa); al contrario, se un sistema è coerente, allora non è possibile dimostrare la sua coerenza a partire dai suoi soli assiomi (quindi la frase che dice che il sistema è coerente risulta vera, ma non dimostrabile).[3]

[3]Il secondo teorema di incompletezza di Gödel può essere parafrasato così: se una persona è veramente coerente, allora non può affermare di essere coerente; al contrario

L'idea del teorema è di definire formalmente la consistenza di una teoria tramite la formula

$$Cons \quad \equiv \quad \neg\, Dim(\bot)$$

(in realtà, al posto della formula $\bot$ dobbiamo mettere il suo numero di Gödel) e dimostrare, poi, che $Cons$ è equivalente alla formula G del primo teorema di incompletezza.

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!

---

una persona incoerente non ha nessuna difficoltà ad affermare di essere coerente (una persona incoerente può affermare tutto e il contrario di tutto)!

Appendice C

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 C.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 $\sim$).

C.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 $\forall x(x \in A \rightarrow x \leq z)$;
- z è un *minorante* di A se $(\forall x \in A)(z \leq x)$, cioè $\forall x(x \in A \rightarrow z \leq x)$;
- 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:

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

(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.

C.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 (cioè il numero di tratti del ramo più lungo).

C.2 Algebre di Boole

Definizione C.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 C.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 (riflessiva, anti-simmetrica e transitiva; vedi pagina 81), ponendo:

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

oppure $x + y = y$.

Proposizione C.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 $\subseteq$. In realtà, si può dimostrare che ogni algebra di Boole con un numero finito di elementi è isomorfa (cioè può essere identificata) all'algebra di Boole $\mathcal{P}(A)$, per qualche A. Di conseguenza il numero di elementi di un'algebra di Boole finita è sempre una potenza di 2; per esempio, non esistono algebre di Boole con 3 elementi.

Lemma C.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 C.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. □

Un altro esempio notevole di algebra di Boole si può ottenere a partire dalle formule delle logica proposizionale classica. Poniamo $X = Frm$ e leggiamo l'uguaglianza di elementi di X come se fosse l'equivalenza fra formule. Inoltre, identifichiamo $+$ con $\vee$, $\cdot$ con $\wedge$, 0 con $\bot$, 1 con $\top$ e $^-$ con $\neg$. Di conseguenza si avrà che $\leq$ viene a coincidere con $\vdash$. Questo chiarisce meglio la differenza fra $\rightarrow$ e $\vdash$: $A \rightarrow B$ corrisponde a $\overline{a} + b$, quindi è una certa operazione in un'algebra di Boole; invece, $A \vdash B$ corrisponde ad una relazione.

Si potrebbe dimostrare che una certa formula (o espressione) nel linguaggio delle algebre di Boole è sempre vera su ogni algebra di Boole se e solo se è vera quando è letta relativamente all'algebra di Frm. Per esempio, visto che l'espressione $a + \overline{a} = 1$ vale in tutte le algebre di Boole (per ogni a) allora la formula $A \vee \neg A$ è una tautologia e viceversa. Questo risultato viene chiamato *teorema di completezza della logica proposizionale classica rispetto alle algebre di Boole*. Tale teorema è utile per trovare dei controesempi: per dimostrare che un certo fatto logico non vale è sufficiente esibire un'algebra di Boole in cui non vale.

C.3 Algebre di Heyting

Definizione C.7 *Un'*algebra di Heyting *è una struttura* $(X, +, \cdot, 0, 1, \rightarrow, \leq)$ *dove* X *è un insieme,* $+$, $\cdot$ *e* $\rightarrow$ *sono operazioni binarie,* 0 *e* 1 *sono due costanti e* $\leq$ *è una relazione binaria tali che:*

- $\leq$ *è una relazione di ordine parziale, cioè soddisfa le proprietà riflessiva, anti-simmetrica e transitiva;*
- $+$ *e* $\cdot$ *sono operazioni idempotenti, commutative e associative;*
- $+$ *e* $\cdot$ *soddisfano le leggi di assorbimento* $x + (x \cdot y) = x$ *e* $x \cdot (x + y) = x$*;*
- *valgono le proprietà distributive di* $\cdot$ *rispetto a* $+$ *e di* $+$ *rispetto a* $\cdot$*;*
- 0 *è l'elemento neutro rispetto a* $+$ *e* 1 *è l'elemento neutro rispetto a* $\cdot$*;*
- $(x \cdot y \leq z) \longleftrightarrow (x \leq y \rightarrow z)$ *per ogni* x, y *e* z*.*

Ovviamente, ogni algebra di Boole è automaticamente un'algebra di Heyting (basta porre $a \rightarrow b = \overline{a} + b$). Però, non tutte le algebre di Heyting sono

anche algebre di Boole. Ad esempio, esiste un'algebra di Heyting con 3 elementi. Infatti, sia $X = \{0, a, 1\}$ con $0 \leq a \leq 1$ e le operazioni definite dalle seguenti tavole:

$+$	0	a	1
0	0	a	1
a	a	a	1
1	1	1	1

$\cdot$	0	a	1
0	0	0	0
a	0	a	a
1	0	a	1

$\rightarrow$	0	a	1
0	1	1	1
a	0	1	1
1	0	a	1

Si può verificare facilmente che in ogni algebra di Heyting $x + y$ 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 Heyting è fornito dall'insieme degli aperti di uno spazio topologico X prendendo $+ = \cup$, $\cdot = \cap$, $0 = \emptyset$, $1 = X$ e $A \rightarrow B$ l'interno dell'unione fra B e il complementare di A. Ad esempio, l'algebra di Heyting con 3 elementi, può essere immaginata così: si pensi a 0 come $\emptyset$, a 1 come l'insieme $\mathbb{R}$ dei numeri reali e ad a come l'insieme $(-\infty, 0) \cup (0, +\infty)$, che non è altro che tutta la retta reale escluso il punto 0.

Un altro esempio notevole di algebra di Heyting si può ottenere a partire dalle formule delle logica proposizionale intuizionistica. Poniamo $X = Frm$ e leggiamo l'uguaglianza di elementi di X come se fosse l'equivalenza fra formule. Inoltre, identifichiamo $\leq$ con $\vdash$, $+$ con $\vee$, $\cdot$ con $\wedge$, 0 con $\bot$, 1 con $\top$ e $\rightarrow$ con $\rightarrow$.

Si potrebbe dimostrare che una certa formula (o espressione) nel linguaggio delle algebre di Heyting è sempre vera su ogni algebra di Heyting se e solo se è vera quando è letta relativamente all'algebra di Frm nella logica proposizionale intuizionistica. Per esempio, visto che l'espressione $A \vee (A \rightarrow \bot) \equiv \top$ non vale in logica intuizionistica, allora ci deve essere un certo elemento x in qualche algebra di Heyting per cui $x + (x \rightarrow 0) \neq 1$ (ad esempio, si consideri l'elemento a nell'algebra di Heyting con 3 elementi). Questo risultato viene chiamato *teorema di completezza della logica proposizionale intuizionistica rispetto alle algebre di Heyting*. Tale teorema è utile per trovare dei controesempi: per dimostrare che un certo fatto logico non vale intuizionisticamente è sufficiente esibire un'algebra di Heyting in cui non vale.

C.4 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 C.8 (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 C.9 *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 C.10 *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. □

C.5 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 C.11 *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 C.12 (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

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

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 C.13 *La classe di tutti gli insiemi non è un insieme.*

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

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

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 C.14 *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 C.15 *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. □

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

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

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.]