Capitolo 2

Strutture

2.1 Strutture e tipi

Una struttura $\mathcal{A}$ è costituita da un insieme A, il dominio della struttura, e da una successione di relazioni su A, funzioni su A e individui di A detti costanti. Il concetto di struttura è molto duttile e consente di rappresentare in modo efficace diverse situazioni di carattere empirico e teorico. Ridurre una situazione a una struttura significa ricondurla nell'ambito dell'algebra. Il passaggio da una situazione "concreta" a una struttura "astratta" è un impoverimento, nel senso che molti dettagli, molti aspetti specifici vanno inevitabilmente perduti, tuttavia non si deve concepire il sacrificio dei particolari come un limite di questo modo di procedere, dato che buona parte dell'attività conoscitiva umana consiste precisamente nella produzione di astrazioni che isolano, in una certa realtà, ciò che si ritiene essenziale da ciò che si ritiene contingente, gli aspetti fondamentali da trasferire nella struttura, dagli aspetti che invece si ritengono inessenziali.

Esaminiamo alcuni esempi di strutture che saranno utili in seguito. Consideriamo la porzione di realtà costituita da tutti i sottoinsiemi di un dato insieme A. È possibile organizzare questi oggetti in una struttura isolando la relazione di inclusione fra insiemi come un aspetto fondamentale della realtà: otteniamo così la struttura costituita dall'insieme ordinato $(P(A), \subseteq)$. Nella stessa realtà insiemistica di base si possono invece considerare come fondamentali le operazioni insiemistiche di intersezione, unione e complemento e quegli insiemi molto particolari che sono $\emptyset$ e A: otteniamo così la struttura $(P(A), \cap, \cup, -, \emptyset, A)$, detta *algebra dell'insieme potenza*, che indicheremo con $\mathcal{B}(A)$. Scegliendo le relazioni, le funzioni e le costanti che fanno parte della struttura, dichiariamo ciò che riteniamo fondamentale nella realtà in esame e a diverse scelte degli elementi caratterizzanti corrispondono diverse strutture.

Una prima classificazione delle strutture si ottiene mediante la nozione di tipo, ossia isolando il linguaggio necessario per nominare le relazioni, le funzioni e le costanti presenti nella struttura: strutture dello stesso tipo sono descrivibili

col medesimo linguaggio. Più precisamente un *tipo* è una quadrupla

$$\tau = (\{R_i\}_{i\in I}, \{F_j\}_{j\in J}, \{c_k\}_{k\in K}, ar)$$

che soddisfa le condizioni seguenti. Le successioni $\{R_i\}_{i\in I}$, $\{F_j\}_{j\in J}$ e $\{c_k\}_{k\in K}$ non contengono ripetizioni. Indicheremo con Rel, Fun e Cos le immagini di queste funzioni. L'insieme Rel contiene i *simboli di relazione*, Fun i *simboli di funzione* e Cos i *simboli di costante*: supporremo che questi insiemi di simboli non abbiano elementi in comune. La funzione $ar : Rel \cup Fun \to \omega$ assegna ad ogni simbolo di relazione e di funzione un numero naturale detto *arietà* del simbolo e parleremo quindi di simboli funzionali e relazionali n-ari. I simboli di relazione 1-ari sono detti anche *simboli di predicato*. Se τ è un tipo, definiamo *struttura di tipo* τ una coppia $\mathcal{A} = (A, \mathcal{I})$, dove A è un insieme non vuoto, detto *dominio* della struttura, e $\mathcal{I}$ è una funzione, detta *interpretazione*, che assegna ad ogni simbolo di relazione una relazione su A, ad ogni simbolo di funzione una funzione su A e ad ogni simbolo di costante una costante di A, ossia un elemento di A, in modo che le arietà dei simboli di relazione e di funzione corrispondano a quelle delle relazioni e funzioni loro assegnate. In altri termini:

1. per ogni simbolo relazionale n-ario, $\mathcal{I}(R_i) \subseteq A^n$,
2. per ogni simbolo funzionale n-ario, $\mathcal{I}(F_j) : A^n \to A$,
3. per ogni simbolo di costante, $\mathcal{I}(c_k) \in A$.

La restrizione a strutture con dominio non vuoto è essenziale. Se ammettessimo strutture con dominio vuoto dovremmo modificare la logica classica, nella quale l'esistenza di almeno un oggetto è formalmente dimostrabile (si veda il paragrafo 4.6). In alcune trattazioni i simboli di costante sono eliminati a favore di simboli di funzioni 0-arie, dato che una funzione 0-aria su A consiste nella scelta di un individuo di A. Scriveremo $R_i^{\mathcal{A}}$ al posto di $\mathcal{I}(R_i)$ per semplicità e per sottolineare il legame con la struttura $\mathcal{A}$. Lo stesso dicasi per simboli di funzione e di costante. Adotteremo la notazione $(A, \{R_i^{\mathcal{A}}\}_{i\in I}, \{F_j^{\mathcal{A}}\}_{j\in J}, \{c_k^{\mathcal{A}}\}_{k\in K})$ per denotare la struttura $(\mathcal{A},\mathcal{I})$, senza indicare il tipo e la funzione arietà in modo esplicito. Quando relazioni, funzioni e costanti sono in numero finito, ci limiteremo ad elencarle, dopo il dominio, in un'unica successione. A volte scriveremo semplicemente R invece di $R^{\mathcal{A}}$, quando non ci sia pericolo di confondere il simbolo di relazione con la relazione stessa. Lo stesso dicasi per i simboli di funzione e di costante. Può accadere che il tipo di una struttura non contenga del tutto simboli, in questo caso la struttura $\mathcal{A}$ si riduce a un semplice insieme A. Se mancano i simboli di funzione e di costante, allora parliamo di *struttura relazionale*, se mancano quelli di relazione, parliamo di *struttura algebrica*.

Ogni tipo τ dà origine a infinite strutture di quel tipo, sia perché è possibile scegliere insiemi diversi come dominio dell'interpretazione, sia perché, una volta scelto un insieme come dominio, esiste una varietà di modi distinti di interpretarvi i simboli del tipo. Sul dominio ω possiamo considerare sia la struttura relazionale $\mathcal{A} = (\omega, \leq^{\mathcal{A}})$, dove $\leq^{\mathcal{A}}$ è la relazione di minore o uguale, sia la struttura relazionale $\mathcal{B} = (\omega, \leq^{\mathcal{B}})$, dove $\leq^{\mathcal{B}}$ è la relazione "x divide y". Avremo

dunque $2 \leq^{\mathcal{A}} 3$ e non $2 \leq^{\mathcal{B}} 3$. La scelta di adottare il simbolo $\leq$ invece di R è dettata solo dal fatto che $\leq$ suggerisce l'idea di un ordine parziale, ma solo $\leq^{\mathcal{A}}$ è la "vera" relazione di minore o uguale. Sempre su ω possiamo definire sia la struttura algebrica $\mathcal{A} = (\omega, S^{\mathcal{A}}, 0^{\mathcal{A}})$, dove $S^{\mathcal{A}}$ è la funzione successore e $0^{\mathcal{A}}$ il numero zero, sia la struttura algebrica $\mathcal{B} = (\omega, S^{\mathcal{B}}, 0^{\mathcal{B}})$, dove $S^{\mathcal{B}}$ è la funzione elevamento al quadrato e $0^{\mathcal{B}}$ il numero 2. Avremo dunque $S^{\mathcal{A}}(0^{\mathcal{A}}) = 1$ e $S^{\mathcal{B}}(0^{\mathcal{B}}) = 4$. In linea di principio l'interpretazione di un simbolo del tipo non è soggetta ad alcun vincolo, tranne il rispetto delle arietà, quindi non bisogna lasciarsi fuorviare dall'aspetto di simboli come $+$, $\leq$ e 0, che possono ricevere interpretazioni che nulla hanno da spartire con somma, minore o uguale e zero.

La distinzione tra R e $R^{\mathcal{A}}$, tra un simbolo e la sua interpretazione, è particolarmente utile quando il discorso verte su strutture differenti in cui lo stesso simbolo riceve interpretazioni diverse, altrimenti la distinzione puntigliosa tra i simboli e le loro interpretazioni appesantisce eccessivamente il discorso. Ci sarà quindi consentito adottare la notazione $(P(A), \cap, \cup, -, \emptyset, A)$ per quella che formalmente è una struttura di tipo $\tau = (\emptyset, \{F_i\}_{i\in 3}, \{c_k\}_{k\in 2}, ar)$ dove $ar(F_0) = ar(F_1) = 2$ e $ar(F_2) = 1$. Il lettore dovrebbe essere in grado, ogni volta che in seguito verrà presentata una struttura in modo informale, di ricostruirne la presentazione rigorosa e di individuarne il tipo.

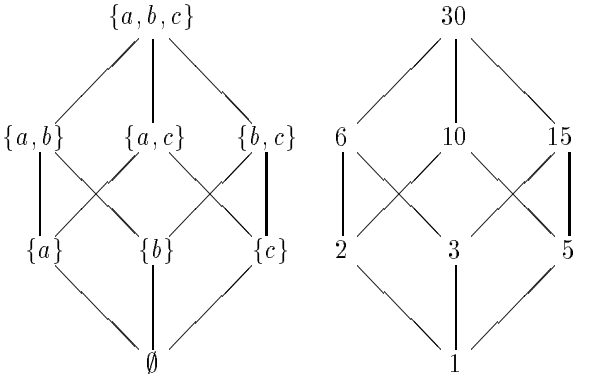
Per convincersi della duttilità del concetto di struttura può essere utile cercare di analizzare in termini di strutture varie realtà concrete della nostra esperienza, individuando prima gli elementi dell'insieme coinvolto, quindi le funzioni e le relazioni che li legano. E' sorprendente quanto di ogni specifica situazione possa essere travasato in una struttura: più la nostra analisi sarà dettagliata, maggiore sarà il numero delle costanti, delle funzioni e delle relazioni coinvolte nella rappresentazione.

2.2 Iso e monomorfismi

Gli individui che appartengono al dominio di una struttura non sono tanto caratterizzati da una loro sostanza, quanto dai rapporti che li legano agli altri individui: un individuo è ciò che è solo in virtù delle relazioni che lo legano agli altri. Quindi se una struttura è ottenuta da un'altra semplicemente sostituendo gli individui del dominio della prima con altri, e tuttavia mantenendo inalterato il loro comportamento rispetto a relazioni e funzioni, non la si dovrà considerare come qualcosa di essenzialmente diverso dalla prima. Sulla base di questa osservazione possiamo concepire l'essenza di una struttura come ciò che è invariante rispetto a questo tipo di sostituzione, ossia la forma generale dei rapporti in cui entrano tali individui in virtù delle funzioni e delle relazioni della struttura. La sostanza degli individui che la compongono diviene un fatto accidentale, un aspetto del tutto marginale della realtà. Questo punto di vista dà origine a un nuovo tipo di sostanza e porta in primo piano il linguaggio, mediante il quale vengono rappresentati i rapporti tra gli individui della struttura, come strumento di individuazione della natura profonda degli oggetti.

Per chiarire questo punto di vista consideriamo la struttura $\mathcal{A} = (A, \subseteq)$ dove

$A = P(\{a,b,c\})$ e $\subseteq$ è la relazione di inclusione, e la struttura $\mathcal{B} = (B, |)$ dove $B = \{1,2,3,5,6,10,15,30\}$ e $|$ la relazione "divide". Adottando la rappresentazione introdotta nel paragrafo 1.4 per gli insiemi parziali, le due strutture possono essere raffigurate nel modo seguente:



Definiamo ora una biiezione $\varphi : \mathcal{A} \to \mathcal{B}$ che associ ad ogni punto di A il punto omologo di B. È evidente allora che, per ogni $x, y \in A$, $x \subseteq y$ sse $\varphi(x)|\varphi(y)$: due insiemi sono inclusi l'uno nell'altro sse il numero che è immagine del primo divide il numero che è immagine del secondo. Comunque si scelga un oggetto in A, le sue relazioni con gli oggetti di A si rispecchiano esattamente nelle relazioni che la sua immagine in B intrattiene con le immagini in B degli altri oggetti di A. Che cosa distingue le due strutture? Solo la natura degli oggetti del dominio, ma non la forma dei rapporti che gli oggetti intrattengono fra di loro. Si osservi che nel passaggio da $\mathcal{A}$ a $\mathcal{B}$ sono conservati anche i rapporti negativi, oltre a quelli positivi: il fatto che$\{b\} \not\subseteq \{a,c\}$ si riflette in $3 \nmid 10$.

Consideriamo un altro esempio in cui le strutture in gioco contengono funzioni e costanti : sia $\mathcal{C} = (P(A), \cap, \cup, \emptyset, A)$ dove $A = \{a,b\}$ e $\cap$ e $\cup$ sono le usuali operazioni di intersezione e unione, e sia $\mathcal{D} = (B, MCD, mcm, 1, 6)$ dove $B = \{1,2,3,6\}$ e MCD e mcm sono rispettivamente le operazioni di "massimo comun divisore" e "minimo comune multiplo". (Si noti che le due strutture hanno lo stesso tipo dato che sono costituite entrambe da due funzioni binarie e da due costanti.) Definiamo ora una biiezione $\psi : P(A) \to B$ ponendo $\psi(\emptyset) = 1$, $\psi(\{a\}) = 2$, $\psi(\{b\}) = 3$, $\psi(\{a,b\}) = 6$. Le due tabelle seguenti rappresentano le funzioni $\cap$ e MCD:

$\cap$	$\{a,b\}$	$\{a\}$	$\{b\}$	$\emptyset$
$\{a,b\}$	$\{a,b\}$	$\{a\}$	$\{b\}$	$\emptyset$
$\{a\}$	$\{a\}$	$\{a\}$	$\emptyset$	$\emptyset$
$\{b\}$	$\{b\}$	$\emptyset$	$\{b\}$	$\emptyset$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$

MCD	6	3	2	1
6	6	3	2	1
3	3	3	1	1
2	2	1	2	1
1	1	1	1	1

Si noti che gli elementi della seconda tabella sono ottenuti dagli elementi omologhi della prima mediante l'applicazione di ψ. Lo stesso si verifica per le due tabelle seguenti, che rappresentano rispettivamente $\cup$ e mcm:

$\cup$	$\{a,b\}$	$\{a\}$	$\{b\}$	$\emptyset$
$\{a,b\}$	$\{a,b\}$	$\{a,b\}$	$\{a,b\}$	$\{a,b\}$
$\{a\}$	$\{a,b\}$	$\{a\}$	$\{a,b\}$	$\{a\}$
$\{b\}$	$\{a,b\}$	$\{a,b\}$	$\{b\}$	$\{b\}$
$\emptyset$	$\{a,b\}$	$\{a\}$	$\{b\}$	$\emptyset$

mcm	6	3	2	1
6	6	6	6	6
3	6	3	6	3
2	6	6	2	2
1	6	3	2	1

Ciò significa che se si sostituiscono gli insiemi coi numeri, secondo il criterio fornito da ψ, intersecare è come calcolare il massimo comun divisore, riunire è come calcolare il minimo comune multiplo. In altri termini, per ogni $x, y \in P(A)$

$$\psi(x \cap y) = MCD(\psi(x), \psi(y)) \quad \text{e} \quad \psi(x \cup y) = mcm(\psi(x), \psi(y)).$$

Il tipo di rapporto tra strutture illustrato dagli esempi precedenti si può vedere come un trasferimento di forma da una struttura all'altra, ossia come un morfismo. In questo paragrafo studieremo alcuni dei principali tipi di morfismi: si tratta di relazioni fra strutture la cui importanza trascende l'algebra, se si pensa a quante delle nostre modalità conoscitive siano catalogabili come metafore, come "riconoscere che qualcosa è, sotto certi aspetti, anche qualcosa d'altro", a quante conoscenze mirino a stabilire qualche tipo di "identità di struttura". Per prima cosa sottolineiamo che si parla di morfismi solo fra strutture del medesimo tipo, infatti le strutture di tipo τ, per quanto diversi possano essere i loro domini, sono accomunate dal fatto di contenere solo relazioni, funzioni e costanti descrivibili coi simboli di τ e ciò ci permette di individuare in esse le relazioni, le funzioni e le costanti *corrispondenti*, ossia denotate dal medesimo simbolo. Quindi, se $\mathcal{A}$ e $\mathcal{B}$ sono due strutture di tipo τ e R è un simbolo relazionale di τ, le relazioni $R^{\mathcal{A}}$ e $R^{\mathcal{B}}$ sono corrispondenti. In modo analogo parleremo di funzioni e di costanti corrispondenti. Gli oggetti corrispondenti, per quanto diversi fra loro, avranno la stessa arietà. Ogni morfismo da $\mathcal{A}$ verso $\mathcal{B}$ presenta le caratteristiche seguenti: a) esiste una funzione $\varphi : A \to B$ che crea un'immagine del dominio di $\mathcal{A}$ entro il dominio di $\mathcal{B}$, b) le immagini degli individui di A giocano i medesimi ruoli rispetto alle relazioni, alle funzioni e alle costanti corrispondenti. Ciò significa che, identificando $R^{\mathcal{A}}$ con $R^{\mathcal{B}}$, $F^{\mathcal{A}}$ con $F^{\mathcal{B}}$, $c^{\mathcal{A}}$ con $c^{\mathcal{B}}$ e $a \in A$ con $\varphi(a) \in B$, possiamo trasferire la forma di $\mathcal{A}$ entro $\mathcal{B}$. Veniamo ora alla definizione formale. Date $\mathcal{A}$ e $\mathcal{B}$ dello stesso tipo $\tau = (\{R_i\}_{i\in I}, \{F_j\}_{j\in J}, \{c_k\}_{k\in K})$, diremo che una biiezione $\varphi : A \to B$ è un *isomorfismo* se per ogni R_i, F_j e c_k del tipo τ, per ogni $a_0, \ldots, a_{n-1} \in A$:

i) $R_i^{\mathcal{A}}(a_0, \ldots, a_{n-1})$ sse $R_i^{\mathcal{B}}(\varphi(a_0), \ldots, \varphi(a_{n-1}))$,

ii) $\varphi(F_j^{\mathcal{A}}(a_0, \ldots, a_{n-1})) = F_j^{\mathcal{B}}(\varphi(a_0), \ldots, \varphi(a_{n-1}))$,

iii) $\varphi(c_k^{\mathcal{A}}) = c_k^{\mathcal{B}}$.

La struttura $\mathcal{A}$ è *isomorfa* a $\mathcal{B}$ se esiste un isomorfismo di $\mathcal{A}$ verso $\mathcal{B}$. Se $\mathcal{A}$ è isomorfa a $\mathcal{B}$, lo indichiamo scrivendo $\mathcal{A} \simeq \mathcal{B}$. E' facile verificare che la relazione di isomorfismo fra strutture di tipo τ è una relazione di equivalenza, ossia è riflessiva, simmetrica e transitiva, quindi l'insieme di tutte le strutture di tipo τ può essere ripartito in classi di equivalenza di strutture isomorfe tra loro.

Ai fini del nostro discorso strutture isomorfe sono considerate come la stessa struttura, quindi ogni volta che parleremo di $\mathcal{A}$ in realtà il discorso varrà per tutte le strutture della classe di equivalenza di $\mathcal{A}$ rispetto a $\simeq$. Il lettore dovrebbe ritornare agli esempi precedenti e verificare che φ e ψ sono effettivamente degli isomorfismi, rispettivamente, tra $\mathcal{A}$ e $\mathcal{B}$ e tra $\mathcal{C}$ e $\mathcal{D}$. Nel primo caso occorrerà verificare la i), mentre nel secondo caso occorrerà verificare la ii) e la iii). (Lo schema della ii) si riproduce in modo più evidente, se scriviamo $\cap(x,y)$ invece di $x \cap y$ e $\cup(x,y)$ invece di $x \cup y$.) L'esempio seguente dovrebbe chiarire come le costanti contribuiscano a costituire quella "forma" che deve essere conservata nei morfismi. Se $\mathcal{A} = (\omega, <, c^{\mathcal{A}})$ e $\mathcal{B} = (\omega - \{0\}, <, c^{\mathcal{B}})$, l'esistenza di un isomorfismo dipende dall'interpretazione della costante c. Se $c^{\mathcal{A}}$ e $c^{\mathcal{B}}$ sono il medesimo oggetto, per esempio il numero 1, non esiste isomorfismo tra $\mathcal{A}$ e $\mathcal{B}$. Se esistesse dovrebbe valere $\varphi(c^{\mathcal{A}}) = c^{\mathcal{B}}$. Come scegliere ora $\varphi(0)$? Comunque si ponga $\varphi(0) = n$, dovrà essere $n > 1$ e questo impedisce che la relazione $0 <^{\mathcal{A}} c^{\mathcal{A}}$ sia conservata da φ, dato che non potrà valere $\varphi(0) <^{\mathcal{B}} c^{\mathcal{B}}$. Per avere isomorfismo occorre che $c^{\mathcal{A}}$ e $c^{\mathcal{B}}$ giochino il medesimo ruolo rispetto alla relazione denotata da $<$, quindi se interpretiamo $c^{\mathcal{A}}$ come 1, cioè come secondo elemento di A, occorre che $c^{\mathcal{B}}$ sia 2, il secondo elemento di B. A questo punto la funzione $\varphi(n) = n + 1$ può connettere gli elementi di A a quelli di B in modo che le relazioni siano conservate.

Se nella definizione di isomorfismo richiediamo solo che φ sia iniettiva (e non necessariamente suriettiva), otteniamo il concetto di *monomorfismo*. Diremo che $\mathcal{A}$ è *immergibile* in $\mathcal{B}$ se esiste un monomorfismo di $\mathcal{A}$ verso $\mathcal{B}$. Se $\varphi : \mathcal{A} \to \mathcal{B}$ è un monomorfismo, possiamo utilizzare φ per creare una nuova struttura $\mathcal{C}$ di dominio $\varphi[A]$ nel modo seguente: per ogni $x_0, \ldots, x_{n-1} \in \varphi[A]$ definiamo

1. $R^{\mathcal{C}}(x_0, \ldots, x_{n-1})$ sse $R^{\mathcal{A}}(\varphi^{-1}(x_0), \ldots, \varphi^{-1}(x_{n-1}))$,
2. $F^{\mathcal{C}}(x_0, \ldots, x_{n-1}) = \varphi(F^{\mathcal{A}}(\varphi^{-1}(x_0), \ldots, \varphi^{-1}(x_{n-1})))$,
3. $c^{\mathcal{C}} = \varphi(c^{\mathcal{A}})$.

Talvolta indicheremo $\mathcal{C}$ con $\varphi[\mathcal{A}]$ per sottolineare che si tratta di una struttura indotta da φ. È immediato verificare che $\mathcal{C}$ è dello stesso tipo di $\mathcal{A}$ e $\mathcal{B}$, e che φ è un isomorfismo tra $\mathcal{A}$ e $\mathcal{C}$: quindi ogni monomorfismo $\varphi : \mathcal{A} \to \mathcal{B}$ permette di ritagliare in $\mathcal{B}$ una struttura isomorfa ad $\mathcal{A}$.

Date due strutture $\mathcal{B}$ e $\mathcal{C}$ del medesimo tipo, diremo che $\mathcal{C}$ è *sottostruttura* di $\mathcal{B}$, in simboli $\mathcal{C} \subseteq \mathcal{B}$, se $C \subseteq B$ e per ogni simbolo di relazione R, di funzione F e di costante c,

1. $R^{\mathcal{C}}$ è la restrizione a C^n di $R^{\mathcal{B}}$, ossia $R^{\mathcal{C}} = C^n \cap R^{\mathcal{B}}$,
2. $F^{\mathcal{C}}$ è la restrizione a C^n di $F^{\mathcal{B}}$, ossia $F^{\mathcal{C}} = F^{\mathcal{B}} \restriction C^n$,
3. $c^{\mathcal{C}} = c^{\mathcal{B}}$.

I due teoremi seguenti illustrano i rapporti tra monomorfismo, isomorfismo e sottostruttura e permettono di concepire il concetto di monomorfismo come generalizzazione di quello di sottostruttura.

Teorema 2.2.1 *La funzione $\varphi : \mathcal{A} \to \mathcal{B}$ è un monomorfismo sse esiste una struttura $\mathcal{C}$ tale che φ è un isomorfismo tra $\mathcal{A}$ e $\mathcal{C}$ e $\mathcal{C} \subseteq \mathcal{B}$.*

La prima implicazione si dimostra ponendo $\mathcal{C} = \varphi[\mathcal{A}]$, la struttura indotta da φ tramite le 1)-3) precedenti. Si verifica facilmente che $\mathcal{C}$ è sottostruttura di $\mathcal{B}$. Per la seconda, osserviamo che se $\varphi : \mathcal{A} \to \mathcal{C}$ è un isomorfismo e $\mathcal{C} \subseteq \mathcal{B}$, allora $C \subseteq B$ e φ è una funzione iniettiva da A verso B. Dimostriamo che è un monomorfismo. Abbiamo infatti $R^{\mathcal{A}}(a_0, \ldots, a_{n-1})$ se e solo se $R^{\mathcal{C}}(\varphi(a_0), \ldots, \varphi(a_{n-1}))$, perché φ è un isomorfismo, e $R^{\mathcal{C}}(\varphi(a_0), \ldots, \varphi(a_{n-1}))$ se e solo se $R^{\mathcal{B}}(\varphi(a_0), \ldots, \varphi(a_{n-1}))$, perché $R^{\mathcal{C}}$ è la restrizione di $R^{\mathcal{B}}$ a $\varphi[A]$. Per quanto riguarda le funzioni,

$$\begin{aligned} \varphi(F^{\mathcal{A}}(a_0, \ldots, a_{n-1})) &= F^{\mathcal{C}}(\varphi(a_0), \ldots, \varphi(a_{n-1})) \\ &= F^{\mathcal{B}}(\varphi(a_0), \ldots, \varphi(a_{n-1})), \end{aligned}$$

essendo φ un isomorfismo e $F^{\mathcal{C}}$ la restrizione di $F^{\mathcal{B}}$ a $\varphi[A]$. Per quanto riguarda le costanti, $\varphi(c^{\mathcal{A}}) = c^{\mathcal{C}} = c^{\mathcal{B}}$.

Corollario 2.2.2 *$\mathcal{A} \subseteq \mathcal{B}$ sse $i_A : \mathcal{A} \to \mathcal{B}$ è un monomorfismo.*

Per il teorema precedente, i_A è un monomorfismo sse esiste una struttura $\mathcal{C}$ tale che $i_A : \mathcal{A} \to \mathcal{C}$ è un isomorfismo e $\mathcal{C} \subseteq \mathcal{B}$. Ma poiché il monomorfismo è l'identità, $\mathcal{C}$ coincide con $\mathcal{A}$.

Non tutti i sottoinsiemi del dominio di una struttura $\mathcal{A}$ costituiscono il dominio di una sottostruttura di $\mathcal{A}$. Se $B \subseteq A$ pretende di essere il dominio di una sottostruttura di $\mathcal{A}$, allora B non deve essere vuoto e deve essere chiuso rispetto alle funzioni di $\mathcal{A}$. (Ricordiamo che un insieme $B \subseteq A$ è chiuso rispetto a una funzione n-aria f se per ogni n-pla $x_0, ..., x_{n-1}$ di elementi di B vale $f(x_0, ..., x_{n-1}) \in B$.) Solo così, infatti, possiamo definire $F^{\mathcal{B}}$ come la restrizione di $F^{\mathcal{A}}$ alle n-ple di B. Mancando la chiusura, la restrizione risulterebbe indefinita per qualche n-pla di elementi di B e non sarebbe quindi una funzione. Inoltre B deve contenere tutte le costanti di $\mathcal{A}$, perché solo così possiamo definire $c^{\mathcal{B}} = c^{\mathcal{A}}$. Se consideriamo le costanti come funzioni 0-arie, quest'ultima condizione si riduce alla chiusura.

Supponiamo, ad esempio, che $\mathcal{A}$ sia $(Z, +^{\mathcal{A}}, -^{\mathcal{A}})$ e che sia $\omega = X$. E' chiaro che X non può essere il dominio di una sottostruttura di $\mathcal{A}$ dato che non è chiuso rispetto a $-^{\mathcal{A}}$. E' vero che possiamo sempre definire una funzione 2-aria f simile alla sottrazione ponendo

$$f(m,n) = \begin{cases} -^{\mathcal{A}}(m,n) & \text{se} \quad n \leq m \\ 0 & \text{altrimenti.} \end{cases}$$

Ma allora la struttura $\mathcal{B} = (\omega, +^{\mathcal{B}}, -^{\mathcal{B}})$, dove $-^{\mathcal{B}}$ è f, non è sottostruttura di $\mathcal{A}$ perché $-^{\mathcal{B}}$ non coincide con la restrizione di $-^{\mathcal{A}}$alle coppie di elementi di ω. Ad esempio, $-^{\mathcal{A}}(1,2) = -1$ mentre $-^{\mathcal{B}}(1,2) = 0$. Se $\mathcal{A}$ è $(Z, +^{\mathcal{A}})$, allora ω, essendo chiuso rispetto alla somma, è il dominio di una sottostruttura. Problemi analoghi possono sorgere con le costanti. Se $\mathcal{A}$ è $(\omega, +^{\mathcal{A}}, 0^{\mathcal{A}})$ allora $\omega - \{0\}$ è

chiuso rispetto alle funzioni di $\mathcal{A}$, ma non ne contiene le costanti. Comunque si definisca una struttura $\mathcal{B} = (\omega - \{0\}, +^{\mathcal{B}}, 0^{\mathcal{B}})$, possiamo ottenere che $+^{\mathcal{B}}$ sia la restrizione di $+^{\mathcal{A}}$ a B, ma non possiamo avere $0^{\mathcal{B}} = 0^{\mathcal{A}}$. Le relazioni, invece, non pongono problemi di questo tipo: per ogni $B \subseteq A$ e ogni relazione n-aria $R^{\mathcal{A}}$ su A, è sempre possibile definire $R^{\mathcal{B}}$ come la restrizione di $R^{\mathcal{A}}$ a B^n, dato che $R^{\mathcal{A}} \cap B^n$ è sempre una relazione su B. (Anche $\emptyset$ è una relazione su B.)

Tuttavia, se $X \subseteq A$ non è il dominio di una sottostruttura di $\mathcal{A}$, è sempre possibile estenderlo quanto basta per renderlo tale. Innanzitutto osserviamo che, sotto opportune condizioni, possiamo introdurre il concetto di *intersezione di strutture*. Data una famiglia non vuota di strutture $\{\mathcal{A}_i\}_{i \in I}$, se le varie $\mathcal{A}_i$ sono tutte sottostrutture della stessa $\mathcal{A}$ di tipo τ e se $\bigcap\{A_i\} \neq \emptyset$, allora possiamo definire $\bigcap\{\mathcal{A}_i\}_{i \in I}$ come la struttura $\mathcal{B}$ di tipo τ tale che

1. $B = \bigcap\{A_i\}_{i \in I}$,
2. $R^B(b_0, ..., b_{n-1})$ sse $R^{\mathcal{A}}(b_0, ..., b_{n-1})$,
3. $F^B(b_0, ..., b_{n-1}) = F^{\mathcal{A}}(b_0, ..., b_{n-1})$,
4. $c^{\mathcal{B}} = c^{\mathcal{A}}$.

Verifichiamo che le condizioni precedenti definiscono effettivamente una struttura. Il primo punto stabilisce il dominio, che risulta essere non vuoto, il secondo stabilisce che le relazioni di $\mathcal{B}$ sono semplicemente la restrizione a B delle relazioni di $\mathcal{A}$. Il terzo punto è più delicato, perché occorre verificare che, per ogni $b_0, \ldots, b_{n-1} \in B$, il valore di $F^{\mathcal{A}}$ per tale argomento sia ancora in B. Poiché $b_0, \ldots, b_{n-1}$ appartengono a B, appartengono anche ad ogni $\mathcal{A}_i$ e quindi ogni $\mathcal{A}_i$ contiene il valore di $F^{\mathcal{A}_i}$ per l'argomento $b_0, \ldots, b_{n-1}$. D'altra parte ogni $\mathcal{A}_i$ è sottostruttura di $\mathcal{A}$ e quindi $F^{\mathcal{A}_i}(b_0, \ldots, b_{n-1})$ coincide sempre con $F^{\mathcal{A}}(b_0, \ldots, b_{n-1})$. Ne segue che quest'ultimo appartiene ad ogni A_i e quindi a B. Le stesse considerazioni valgono per il quarto punto. È chiaro allora che $\mathcal{B}$ è una struttura ed inoltre è sottostruttura di ogni $\mathcal{A}_i$, e quindi di $\mathcal{A}$.

Siamo ora in grado di definire, per ogni $B \subseteq A$, $B \neq \emptyset$, la *sottostruttura generata da* B in $\mathcal{A}$ come $\bigcap\{\mathcal{C} : \mathcal{C} \subseteq \mathcal{A}, B \subseteq C\}$. La definizione è corretta, dato che la famiglia di strutture in questione non è vuota, perché contiene almeno $\mathcal{A}$, e inoltre l'intersezione dei domini delle varie $\mathcal{C}$ non è vuota, poiché ognuno deve includere $B \neq \emptyset$. Dalla definizione risulta immediatamente che la sottostruttura generata da B in $\mathcal{A}$ è anche la minima sottostruttura di $\mathcal{A}$ che includa B ed è quindi ottenuta estendendo B quanto basta per ottenere un insieme chiuso rispetto alle funzioni di $\mathcal{A}$ e contenente le costanti di $\mathcal{A}$.

Ci sono due casi limite di sottostruttura generata da B in $\mathcal{A}$. Nel primo, il dominio della sottostruttura generata coincide con B: in questo caso B era il sostegno adatto per una sottostruttura di $\mathcal{A}$ senza che fosse necessario aggiungere nulla. Nel secondo, il dominio della sottostruttura generata è A: in questo caso si sono dovuti aggiungere tutti gli elementi di $A - B$ per ottenere una sottostruttura. In questo secondo caso diremo che B è un insieme di *generatori* per $\mathcal{A}$.

Consideriamo, ad esempio, la struttura $\mathcal{A} = (\omega, S^{\mathcal{A}})$. Per ogni $B \subseteq \omega$, la sottostruttura generata da B in $\mathcal{A}$ ha come dominio l'insieme dei numeri naturali maggiori o uguali al minimo di B. Se $\mathcal{A} = (\omega, S^{\mathcal{A}}, 0^{\mathcal{A}})$, per ogni $B \subseteq \omega$ la sottostruttura generata da B coincide con $\mathcal{A}$ poiché dovrà contenere lo zero ed essere chiusa rispetto alla funzione successore. Quindi una struttura può avere diversi insiemi di generatori: in quest'ultimo esempio ogni sottoinsieme del dominio è un insieme di generatori.

Esercizio 2.2.1 Si dimostri che ogni struttura $(A, \leq)$, dove $\leq$ è un ordine parziale, è isomorfa a una struttura $(B, \subseteq)$ dove $\subseteq$ è l'inclusione insiemistica. (Si associ ad $a \in A$ l'insieme $\{b : b \leq a\}$.)

Esercizio 2.2.2 Si determini se $\mathcal{A}$ è immergibile in $\mathcal{B}$, se $\mathcal{A} \simeq \mathcal{B}$, se $\mathcal{A} \subseteq \mathcal{B}$ in ognuno dei casi seguenti:

1. $\mathcal{A} = (\omega, \leq)$ e $\mathcal{B} = (Z, \leq)$,
2. $\mathcal{A} = (\omega, +, \cdot)$ e $\mathcal{B} = (Z, +, \cdot)$,
3. $\mathcal{A} = (\omega, +, \cdot)$ e $\mathcal{B} = (Z, \cdot, +)$,
4. $\mathcal{A} = (\omega, +, 0)$ e $\mathcal{B} = (\omega, \cdot, 1)$.

Esercizio 2.2.3 Si determini se $\mathcal{A}$ è immergibile in $\mathcal{B}$ quando

1. $\mathcal{A}$= $(\omega, \leq, \cdot, 1)$ e $\mathcal{B}$= $(\omega, \leq, +, 0)$.
2. $\mathcal{A}$ =$(\omega - \{0\}, \leq, \cdot, 1)$ e $\mathcal{B}$= $(\omega, \leq, +, 0)$.
3. $\mathcal{A}$ =$(\omega - \{0\}, \cdot, 1)$ e $\mathcal{B}$ =$(\omega, +, 0)$.

Esercizio 2.2.4 Sia $\mathcal{A} = (P(\{a, b\}, \cap, \cup)$ e $\mathcal{B} = (P(\{a, b, c\}, \cap, \cup)$. Si dimostri che $\mathcal{A} \subseteq \mathcal{B}$. Supponiamo che $\mathcal{A}'$ e $\mathcal{B}'$ siano ottenute aggiungendo alle strutture precedenti l'operazione di complemento: si dimostri che $\mathcal{A}' \not\subseteq \mathcal{B}'$.

Esercizio 2.2.5 Si dimostri che la relazione $\mathcal{A} \simeq \mathcal{B}$ è di equivalenza e che la relazione $\mathcal{A} \subseteq \mathcal{B}$ è un ordine parziale.

Esercizio 2.2.6 Definiamo $R(\mathcal{A}, \mathcal{B})$ sse $\mathcal{A}$ è immergibile in $\mathcal{B}$. Si dimostri che:

1. R è riflessiva e transitiva ma non antisimmetrica;
2. $R(\mathcal{A}, \mathcal{B})$ e $R(\mathcal{B}, \mathcal{A})$ non implica $\mathcal{A} \simeq \mathcal{B}$. (Si considerino Q e Q^+ con $\leq$.)

Esercizio 2.2.7 (Questo esercizio richiede alcuni risultati di aritmetica cardinale.) Sia A un insieme di cardinalità infinita α. Si determini il numero di strutture distinte di dominio A (vale a dire strutture ottenute con differenti interpretazioni dei simboli del tipo) nei casi seguenti:

1. $\tau = (\{c\})$ $[\alpha]$

2. $\tau = (\{c_k\}_{k\in K})$ $[\alpha^{|K|}]$

3. $\tau = (\{F_0\})$ $[2^{\alpha}]$

4. $\tau = (\{F_j\}_{j\in J})$ $[2^{\alpha+|J|}]$

5. $\tau = (\{R_0\})$ $[2^{\alpha}]$

6. $\tau = (\{R_i\}_{i\in I})$ $[2^{\alpha+|I|}]$

Esercizio 2.2.8 Sia $|\tau| = \sup\{|I|, |J|, |K|\}$. Se α è il cardinale di A ed è infinito, si dimostri che esistono al più $2^{\sup\{\alpha,|\tau|\}}$ strutture non isomorfe di tipo τ e dominio A.

2.3 Omomorfismi

Il concetto di omomorfismo si ottiene da quello di monomorfismo lasciando cadere la richiesta di iniettività della funzione. Quindi l'uguaglianza $\varphi(x) = \varphi(y)$ è compatibile sia con $x = y$ sia con $x \neq y$, mentre $x = y$ implica necessariamente $\varphi(x) = \varphi(y)$. Questo comportamento della relazione di identità, per cui a punti identici devono corrispondere immagini identiche mentre immagini identiche possono provenire da punti distinti, è esteso a tutte le relazioni della struttura e si esprime nella prima condizione della definizione seguente che è un indebolimento della corrispondente condizione nella definizione di monomorfismo. Date due strutture $\mathcal{A}$ e $\mathcal{B}$ dello stesso tipo, diremo che una funzione $\varphi : A \to B$ è un *omomorfismo* se per ogni R_i, F_j e c_k del tipo τ, per ogni $a_0, \ldots, a_{n-1} \in A$:

i) se $R_i^{\mathcal{A}}(a_0, \ldots, a_{n-1})$ allora $R_i^{\mathcal{B}}(\varphi(a_0), \ldots, \varphi(a_{n-1}))$,

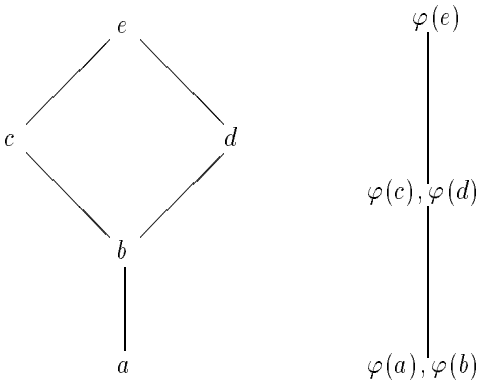
ii) $\varphi(F_j^{\mathcal{A}}(a_0, \ldots, a_{n-1})) = F_j^{\mathcal{B}}(\varphi(a_0), \ldots, \varphi(a_{n-1}))$,

iii) $\varphi(c_k^{\mathcal{A}}) = c_k^{\mathcal{B}}$.

Diremo che φ è un *omomorfismo forte* se è possibile sostituire la i) con la condizione seguente che coincide con la condizione corrispondente nella definizione di monomorfismo:

i') $R_i^{\mathcal{A}}(a_0, \ldots, a_{n-1})$ sse $R_i^{\mathcal{B}}(\varphi(a_0), \ldots, \varphi(a_{n-1}))$.

Se $\mathcal{A}$ e $\mathcal{B}$ sono strutture algebriche, ossia sono prive di relazioni, la distinzione tra omomorfismo e omomorfismo forte non ha più luogo e diremo semplicemente che φ è un omomorfismo se verifica le condizioni ii) e iii). Se $\mathcal{A}$ e $\mathcal{B}$ sono ordini parziali, un omomorfismo di $\mathcal{A}$ verso $\mathcal{B}$ è una funzione $\varphi : A \to B$ tale che $x \leq^{\mathcal{A}} y$ implica $\varphi(x) \leq^{\mathcal{B}} \varphi(y)$. Nella figura seguente φ è un esempio di omomorfismo tra ordini parziali, ma non è un omomorfismo forte:



Come esempio di omomorfismo tra strutture algebriche consideriamo le due strutture $\mathcal{A} = (P(A), \cap, \cup, A, \emptyset)$ e $\mathcal{B} = (P(B), \cap, \cup, B, \emptyset)$ dove $B \subseteq A$ e la funzione $\varphi : P(A) \to P(B)$ definita ponendo $\varphi(X) = X \cap B$ per ogni $X \subseteq A$. Verifichiamo che φ conserva le operazioni e le costanti:

$$\begin{aligned}
\varphi(X \cap Y) &= (X \cap Y) \cap B = (X \cap B) \cap (Y \cap B) = \varphi(X) \cap \varphi(Y), \\
\varphi(X \cup Y) &= (X \cup Y) \cap B = (X \cap B) \cup (Y \cap B) = \varphi(X) \cup \varphi(Y), \\
\varphi(A) &= A \cap B = B, \\
\varphi(\emptyset) &= \emptyset \cap B = \emptyset.
\end{aligned}$$

Mentre iso e monomorfismi forniscono immagini che sono copie esatte del dominio, l'immagine fornita dall'omomorfismo, proprio perché fornita da una semplice funzione, è costituita da oggetti che possono essere visti come rappresentanti di classi di equivalenza di individui del dominio. Nel paragrafo dedicato alle relazioni di equivalenza abbiamo visto che ad ogni relazione di equivalenza $\sim$ su A è associato un insieme quoziente $A/\sim$ i cui elementi sono esattamente le classi di equivalenza degli elementi di A. Se immaginiamo che A sia l'insieme degli esseri umani e $\sim$ la relazione "x è nato nello stesso anno di y", allora gli elementi di $A/\sim$ sono le classi di tutti gli esseri umani nati nel medesimo anno. Il passaggio da A a $A/\sim$ è del tipo molti-uno: molti individui vengono radunati sotto un unico aspetto e da essi si astrae un nuovo tipo di individuo, la classe di equivalenza. Supponiamo ora che A sia il dominio di una struttura $\mathcal{A}$. Ci si può chiedere se i rapporti che valgono fra gli elementi di A, stabiliti dalle funzioni e dalle relazioni di $\mathcal{A}$, sono estendibili a rapporti tra le classi di equivalenza in modo che la struttura $\mathcal{A}$ induca una struttura dello stesso tipo su $A/\sim$. Ad esempio, se A è l'insieme degli esseri umani e tra gli elementi di A è stabilita la relazione "x è più vecchio di y", è possibile estendere questa relazione a una relazione R tra classi di equivalenza definita ponendo $[x]R[y]$ sse x è più vecchio di y? La cosa è sensata, dato che se x è più vecchio di y, allora anche tutti gli elementi di $[x]$ sono più vecchi degli elementi di $[y]$, quindi il comportamento degli elementi delle classi di equivalenza è omogeneo rispetto alla relazione R. D'altra parte non è sempre lecito questo passaggio alle classi di equivalenza. Consideriamo la relazione "x ama y". Non è detto che, se x ama y, anche tutti

gli esseri umani nati nello stesso anno di x amino tutti gli esseri umani nati nello stesso anno di y, quindi questa relazione non è estendibile a $A/\sim$. Analogo discorso si può fare per le funzioni. Cerchiamo ora di fissare le caratteristiche di una relazione e di una funzione estendibile alle classi di equivalenza. Diremo che una relazione binaria $\sim$ è una *congruenza* su $\mathcal{A}$ se è una relazione di equivalenza su A e inoltre, per ogni funzione $F^{\mathcal{A}}$ e ogni relazione $R^{\mathcal{A}}$, se $a_i \sim b_i$ per ogni $i < n$, allora

1. $F^{\mathcal{A}}(a_0, \ldots, a_{n-1}) \sim F^{\mathcal{A}}(b_0, \ldots, b_{n-1})$,
2. $R^{\mathcal{A}}(a_0, \ldots, a_{n-1})$ implica $R^{\mathcal{A}}(b_0, \ldots, b_{n-1})$.

Si osservi che, essendo $\sim$ simmetrica, nella 2) possiamo sostituire "implica" con "sse". Ogni congruenza $\sim$ su $\mathcal{A}$ induce una struttura su $A/\sim$ nel modo seguente. Definiamo *struttura quoziente* di $\mathcal{A}$ modulo $\sim$ la struttura $\mathcal{B}$ dello stesso tipo di $\mathcal{A}$ avente dominio $B = A/\sim$ e tale che, per ogni simbolo di costante c, di funzione F, di relazione R,

1. $c^{\mathcal{B}} = [c^{\mathcal{A}}]$,
2. $F^{\mathcal{B}}([a_0], \ldots, [a_{n-1}]) = [F^{\mathcal{A}}(a_0, \ldots, a - n - 1)]$,
3. $R^{\mathcal{B}}([a_0], \ldots, [a_{n-1}])$ sse $R^{\mathcal{A}}(a_0, \ldots, a_{n-1})$.

È immediato verificare che le funzioni e le relazioni di $\mathcal{B}$ risultano ben definite sulle classi di equivalenza proprio perché $\sim$ è una congruenza. Solitamente si indica $\mathcal{B}$ con $\mathcal{A}/\sim$.

La caratteristica fondamentale della congruenza, vale a dire l'essere compatibile con le relazioni e le funzioni di $\mathcal{A}$, rende possibile un trasferimento di struttura da $\mathcal{A}$ verso la struttura quoziente $\mathcal{A}/\sim$. Per ogni congruenza $\sim$ su $\mathcal{A}$ definiamo una funzione $\varphi_\sim : A \to A/\sim$ ponendo $\varphi_\sim(a) = [a]$.

Teorema 2.3.1 *Se $\sim$ è una congruenza su $\mathcal{A}$, allora $\varphi_\sim$ è un omomorfismo forte suriettivo da $\mathcal{A}$ verso $\mathcal{A}/\sim$.*

Semplifichiamo la notazione ponendo $\mathcal{A}/\sim = \mathcal{B}$. Per quanto riguarda le relazioni,

$$\begin{array}{rll} R^{\mathcal{A}}(a_0, \ldots, a_{n-1}) & \text{sse} & R^{\mathcal{B}}([a_0], \ldots, [a_{n-1}]) \\ & \text{sse} & R^{\mathcal{B}}(\varphi_\sim(a_0), \ldots, \varphi_\sim(a_{n-1})). \end{array}$$

Per quanto riguarda le funzioni,

$$\begin{array}{rcl} \varphi(F^{\mathcal{A}}(a_0, \ldots, a_{n-1})) & = & [F^{\mathcal{A}}(a_0, \ldots, a_{n-1})] \\ & = & F^{\mathcal{B}}([a_0], \ldots, [a_{n-1}]) \\ & = & F^{\mathcal{B}}(\varphi_\sim(a_0), \ldots, \varphi_\sim(a_{n-1})). \end{array}$$

Per quanto riguarda le costanti, $\varphi_\sim(c^{\mathcal{A}}) = [c^{\mathcal{A}}] = c^{\mathcal{B}}$.

Abbiamo visto che il risultato di una congruenza, cioè il passaggio a una struttura quoziente, è sempre ottenibile come immagime omomorfa della struttura di partenza, poiché $\mathcal{A}/\sim$ coincide con $\varphi_\sim[\mathcal{A}]$. Mostriamo ora che ogni immagine omomorfa è ottenibile quozientando la struttura di partenza con un'opportuna congruenza. Ad ogni funzione $\varphi : A \to B$ è associata una relazione binaria $\sim_\varphi$ su A definita ponendo $x \sim_\varphi y$ sse $\varphi(x) = \varphi(y)$.

Teorema 2.3.2 *Se $\varphi : \mathcal{A} \to \mathcal{B}$ è un omomorfismo forte, allora $\sim_\varphi$ è una congruenza su $\mathcal{A}$.*

Dato che $=$ è una relazione di equivalenza, anche $\sim_\varphi$ lo è. Supponiamo che $a_i \sim_\varphi b_i$ per ogni $i < n$, e quindi che $\varphi(a_i) = \varphi(b_i)$. Poiché φ è un omomorfismo, per ogni simbolo funzionale F

$$\begin{aligned} \varphi(F^{\mathcal{A}}(a_0, \ldots, a_{n-1})) &= F^{\mathcal{B}}(\varphi(a_0), \ldots, \varphi(a_{n-1})) \\ &= F^{\mathcal{B}}(\varphi(b_0), \ldots, \varphi(b_{n-1})) \\ &= \varphi(F^{\mathcal{A}}(b_0, \ldots, b_{n-1})). \end{aligned}$$

Quindi $F^{\mathcal{A}}(a_0, \ldots, a_{n-1}) \sim_\varphi F^{\mathcal{A}}(b_0, \ldots, b_{n-1})$. Poiché φ è un omomorfismo forte, per ogni simbolo relazionale R abbiamo

$$\begin{aligned} R^{\mathcal{A}}(a_0, \ldots, a_{n-1}) &\text{ implica } R^{\mathcal{B}}(\varphi(a_0), \ldots, \varphi(a_{n-1})) \\ &\text{implica } R^{\mathcal{B}}(\varphi(b_0), \ldots, \varphi(b_{n-1})) \\ &\text{implica } R^{\mathcal{A}}(b_0, \ldots, b_{n-1}). \end{aligned}$$

Si osservi che l'ultimo passaggio richiede che φ sia forte.

Teorema 2.3.3 *Se $\varphi : \mathcal{A} \to \mathcal{B}$ è un omomorfismo forte suriettivo, esiste un isomorfismo tra $\mathcal{A}/\sim_\varphi$ e $\mathcal{B}$.*

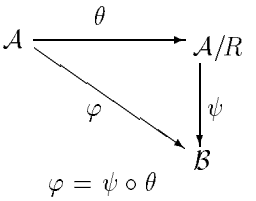
Per il teorema precedente $\sim_\varphi$ è una congruenza su $\mathcal{A}$ e quindi possiamo considerare la struttura quoziente $\mathcal{A}/\sim_\varphi$. Come abbiamo visto nel teorema 1.4.3, la funzione $\psi : A/\sim_\varphi \to B$ definita ponendo $\psi([a]) = \varphi(a)$ è una biiezione. Dimostriamo che è anche un isomorfismo. Per brevità poniamo $\mathcal{C} = \mathcal{A}/\sim_\varphi$, abbiamo allora

$$\begin{aligned} \psi(F^{\mathcal{C}}([a_0], \ldots, [a_{n-1}])) &= \psi([F^{\mathcal{A}}(a_0, \ldots, a_{n-1})]) \\ &= \varphi(F^{\mathcal{A}}(a_0, \ldots, a_{n-1})) \\ &= F^{\mathcal{B}}(\varphi(a_0), \ldots, \varphi(a_{n-1})) \\ &= F^{\mathcal{B}}(\psi[a_0], \ldots, \psi[a_{n-1}]) \end{aligned}$$

Per quanto riguarda le relazioni abbiamo

$$\begin{aligned} R^{\mathcal{C}}([a_0], \ldots, [a_n]) &\text{ sse } R^{\mathcal{A}}(a_0, \ldots, a_{n-1}) \\ &\text{sse } R^{\mathcal{B}}(\varphi(a_0), \ldots, \varphi(a_{n-1})) \\ &\text{sse } R^{\mathcal{B}}(\psi[a_0], \ldots, \psi[a_{n-1}]). \end{aligned}$$

La situazione è illustrata dalla figura seguente, dove θ indica la funzione da $\mathcal{A}$ verso $\mathcal{A}/\sim_\varphi$ che associa ad ogni $a \in A$ la sua classe $[a]$ modulo $\sim_\varphi$.



Congruenze e omomorfismi forti sono due aspetti diversi di una medesima realtà. La congruenza effettua una costruzione col materiale fornito dalla struttura di partenza, organizzandolo in classi di equivalenza in modo tale che si conservino funzioni e relazioni della struttura, mentre l'omomorfismo produce un'immagine "esterna" alla struttura data, ma i teoremi precedenti garantiscono l'equivalenza tra queste due operazioni che riproducono, nelle sue linee fondamentali, la procedura di astrazione. Procedere per astrazione conduce alla formazione di nuovi enti, le classi di individui identificabili rispetto alle caratteristiche da cui si astrae, ma l'astrazione si rivela particolarmente feconda dal punto di vista conoscitivo quando la classificazione riproduce alcuni aspetti strutturali rilevanti della realtà da cui eravamo partiti, cioè quando funzioni e relazioni vigenti tra le classi rispecchiano un'analoga strutturazione dei dati iniziali. E questo è, a piacere, omomorfismo o congruenza.

Esercizio 2.3.1 Si dimostri che, nel caso degli ordini, un omomorfismo forte è addirittura un monomorfismo.

2.4 Reticoli e algebre di Boole

In questo paragrafo presenteremo due classi di strutture particolarmente importanti nello studio della logica: i reticoli e le algebre di Boole. Gli assiomi che le individuano sono ispirati dalle proprietà che caratterizzano le operazioni insiemistiche fondamentali e la genesi di tali assiomi fornisce un esempio di come si costituiscano le moderne teorie assiomatiche. Se consideriamo i sottoinsiemi di W come oggetti di studio, possiamo dapprima considerare fondamentali le operazioni di unione e intersezione e quindi organizzare $P(W)$ nella struttura $\mathcal{R}(W) = (P(W), \cap, \cup)$ di tipo $(\wedge, \vee)$, dove $\wedge$, $\vee$ sono simboli funzionali binari. Il tipo permette una prima rozza classificazione delle strutture: scegliendo il tipo dichiariamo con quale linguaggio intendiamo studiare la realtà, quali rapporti fra gli oggetti siamo disposti a considerare come fondamentali. Esistono tuttavia infinite strutture di tipo $(\wedge, \vee)$ che nulla hanno a che vedere con gli insiemi, ad esempio $(Z, +, \cdot)$. Se vogliamo caratterizzare meglio il nostro oggetto di studio, possiamo isolare alcune proprietà fondamentali delle funzioni di $\mathcal{R}(W)$. Si ottiene così il seguente insieme L di assiomi:

i) $x \wedge y = y \wedge x$ e $x \vee y = y \vee x$ (commutatività),

ii) $(x \wedge y) \wedge z = x \wedge (y \wedge z)$ e $(x \vee y) \vee z = x \vee (y \vee z)$ (associatività),

iii) $(x \wedge y) \vee y = y$ e $(x \vee y) \wedge y = y$ (assorbimento),

Se $\mathcal{A}$ è una struttura di tipo τ, diremo che tali assiomi sono veri in $\mathcal{A}$ se, interpretando $\wedge$ come $\wedge^{\mathcal{A}}$ e $\vee$ come $\vee^{\mathcal{A}}$, otteniamo equazioni soddisfatte da ogni possibile sostituzione delle variabili x, y, z con oggetti di A. Se tutti gli assiomi di L sono veri in $\mathcal{A}$, diremo che $\mathcal{A}$ è un modello degli assiomi L, ossia che $\mathcal{A}$ è un *reticolo*. Si verifica facilmente che $\mathcal{R}(W)$ è un reticolo: basta rimpiazzare $\wedge$ con $\cap$ e $\vee$ con $\cup$. Quando $W = 1$ otteniamo un reticolo particolarmente importante, che indichiamo con 2, poiché il suo dominio è $P(1)$, ossia $P(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\} = \{0, 1\} = 2$. Non tutti i reticoli hanno domini costituiti da insiemi strutturati dalle usuali operazioni insiemistiche: basta considerare l'algebra $\mathcal{A}$ in cui $A = \{x : x \text{ divide } 30\}$, $\wedge^{\mathcal{A}} = MCD$, $\vee^{\mathcal{A}} = mcm$. Lasciamo al lettore il compito di verificare che $\mathcal{Z}$ non è un modello dell'insieme di assiomi L.

Per ogni proposizione α riguardante i reticoli, definiamo α^* come la proposizione ottenuta sostituendo in α i simboli $\wedge$ con $\vee$ e $\vee$ con $\wedge$. Diremo che α^* è la *duale* di α. Si verifica facilmente che se α è un assioma di L anche α^* lo è. Ciò significa che se $\mathcal{A} = (A, \wedge^{\mathcal{A}}, \vee^{\mathcal{A}})$ è un reticolo, anche la struttura $\mathcal{A}^* = (A, \vee^{\mathcal{A}}, \wedge^{\mathcal{A}})$ lo è. Possiamo allora giustificare il seguente *principio di dualità*: ogni volta che abbiamo dimostrato che la proposizione α è vera in ogni reticolo, sappiamo che anche α^* è vera in ogni reticolo. (Basta osservare che per ipotesi α à vera in ogni reticolo e quindi anche in $\mathcal{A}^*$, ma allora α^* è vera in $\mathcal{A}^{**} = \mathcal{A}$.) Tale principio dimezza l'impegno dimostrativo: tutte le volte che abbiamo dimostrato un teorema α, vale anche il teorema duale α^*.

È possibile esprimere la relazione $X \subseteq Y$ senza fare riferimento agli elementi di X e di Y: infatti, se definiamo una relazione XRY sse $X \cap Y = X$, si dimostra facilmente che R coincide con $\subseteq$. Se ora ci collochiamo in un reticolo qualsiasi, che cosa possiamo dire in generale di una relazione $\leq$ definita ponendo $x \leq y$ sse $x \wedge y = x$? Il significato di $\leq$ è legato a quello di $\wedge$ che a sua volta dipende solamente dagli assiomi di reticolo, ma tali assiomi sono sufficienti a dimostrare che $\leq$ è un ordine.

Teorema 2.4.1 *In ogni reticolo valgono le equazioni seguenti:*

1. $x \wedge x = x$ *e* $x \vee x = x$ *(idempotenza),*

2. $x \wedge y = x$ *sse* $x \vee y = y$.

1. Usando gli assiomi i) e iii): $x \wedge x = x \wedge (x \vee (y \wedge x)) = x$. L'altra equazione si ottiene per dualità.

2. Usando l'assioma iii), se $x \wedge y = x$ allora $x \vee y = (x \wedge y) \vee y = y$. Usando gli assiomi i) e iii), se $x \vee y = y$ allora $x \wedge y = x \wedge (x \vee y) = (y \vee x) \wedge x = x$.

Teorema 2.4.2 *La relazione* $x \leq y$ *sse* $x \wedge y = x$ *è un ordine.*

Per il punto 1) del teorema precedente $\leq$ è riflessiva. Per l'assioma i) è antisimmetrica: infatti da $x \leq y$ e $y \leq x$ segue $x \wedge y = x$ e $y \wedge x = y$, ma per la commutatività $x \wedge y = y \wedge x$. Per l'assioma ii) è transitiva. Infatti da $x \leq y$ e $y \leq z$ otteniamo $x \wedge y = x$ e $y \wedge z = y$. Sostituendo e usando l'associatività otteniamo $x \leq z$, dato che $x = x \wedge y = x \wedge (y \wedge z) = (x \wedge y) \wedge z = x \wedge z$.

Teorema 2.4.3 *Le operazioni $\wedge$ e $\vee$ sono monotone rispetto a $\leq$, vale a dire se $x \leq y$ allora $x \wedge z \leq y \wedge z$ e $x \vee z \leq y \vee z$.*

Se $x \leq y$ allora $x \wedge y = x$ e quindi $(x \wedge y) \wedge z = x \wedge z$. Utilizzando commutatività, associatività e idempotenza abbiamo allora $(x \wedge z) \wedge (y \wedge z) = (x \wedge y) \wedge z = x \wedge z$, da cui $x \wedge z \leq y \wedge z$. In modo analogo si procede con $\vee$.

Quindi a ogni reticolo possiamo associare un insieme ordinato avente lo stesso dominio e strutturato da una relazione d'ordine $x \leq y$ che può essere definita indifferentemente da $x \wedge y = x$ o da $x \vee y = y$. Torniamo ora alla realtà insiemistica da cui siamo partiti per ricavarne altre significative proprietà di $\cap$ e di $\cup$. Osserviamo che vale la distributività di $\cap$ su $\cup$ e da essa ricaviamo l'assioma

iv) $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ (*distributività di $\wedge$ su $\vee$*).

Diremo che una struttura $\mathcal{A}$ è un *reticolo distributivo* se in essa valgono gli assiomi i)-iv). Il teorema seguente mostra che non è necessario assumere anche la distributività duale.

Teorema 2.4.4 *In ogni reticolo, se vale iv) allora vale anche iv)* e viceversa.*

Utilizzando iv), iii) e i) otteniamo

$$\begin{aligned}(x \vee y) \wedge (x \vee z) &= ((x \vee y) \wedge x) \vee ((x \vee y) \wedge z) \\ &= x \vee (z \wedge (x \vee y)) \\ &= x \vee (z \wedge x) \vee (z \wedge y) \\ &= x \vee (z \wedge y).\end{aligned}$$

Assumendo iv)* si ottiene iv) con una dimostrazione duale.

Tutti gli esempi di reticolo introdotti finora sono distributivi, ma vedremo in seguito che non tutti i reticoli lo sono. La distributività è comunque una proprietà che caratterizza fortemente la realtà insiemistica che ha ispirato i nostri assiomi, è infatti possibile dimostrare il seguente teorema di rappresentazione: ogni reticolo distributivo è isomorfo a una sottostruttura di $\mathcal{R}(W)$, per un'opportuna scelta di W (si veda, ad esempio, [Davey-Priestley 90, teorema 10.3]).

Un altro aspetto importante di $P(W)$ che possiamo tradurre negli assiomi è la presenza di un insieme massimo e di un insieme minimo rispetto a $\subseteq$, rispettivamente W e $\emptyset$. Per ogni $X \in P(W)$ vale $X \subseteq W$ e $\emptyset \subseteq X$ e tali proprietà di W e di $\emptyset$ si esprimono in termini di $\cup$ e di $\cap$ mediante le equazioni $X \cup W = W$ e $X \cap \emptyset = \emptyset$. Se espandiamo il tipo dei reticoli con l'aggiunta di due simboli di costante 1 e 0, possiamo riprodurle nei due assiomi seguenti:

M) $x \vee 1 = 1$,

m) $x \wedge 0 = 0$.

Chiameremo *reticolo limitato* ogni reticolo in cui valgano anche gli assiomi M) e m). Si vede immediatamente che in ogni reticolo limitato $\mathcal{A}$ gli elementi $0^{\mathcal{A}}$ e $1^{\mathcal{A}}$ sono rispettivamente il minimo e il massimo rispetto alla relazione $\leq$ associata al reticolo. Tutti gli esempi di reticoli che abbiamo mostrato possono essere espansi a reticoli limitati, con l'introduzione di due costanti definite in modo da rendere veri gli assiomi di massimo e minimo, ma vedremo in seguito che non tutti i reticoli sono limitati. Nel caso dei reticoli limitati, la duale α^* di una proposizione α si ottiene scambiando $\wedge$ con $\vee$, $\vee$ con $\wedge$, 0 con 1 e 1 con 0.

L'ultimo aspetto di $P(W)$ che vogliamo rispecchiare negli assiomi è l'esistenza del complemento. Se pensiamo $P(W)$ strutturato come l'algebra dell'insieme potenza $\mathcal{B}(W)$, vediamo che per ogni $X \in P(W)$ esiste un elemento di $P(W)$, indicato con $-X$, tale che $X \cap -X = \emptyset$ e $X \cup -X = W$. Se espandiamo il tipo dei reticoli limitati con l'aggiunta di un simbolo funzionale unario $\neg$, possiamo tradurre le equazioni precedenti nei seguenti assiomi:

v) $x \wedge \neg x = 0$ e $x \vee \neg x = 1$.

Indichiamo con BA l'insieme degli assiomi i)-v) e chiamiamo *algebra di Boole* una struttura $\mathcal{A}$ che sia modello degli assiomi BA. Quindi un'algebra di Boole è un reticolo distributivo in cui vale l'assioma v). Si verifica facilmente che $\mathcal{B}(W)$ è un'algebra di Boole: basta interpretare $\wedge$ su $\cap$, $\vee$ su $\cup$, $\neg$ su $-$, 0 su $\emptyset$, 1 su W. Quando $W = \{\emptyset\}$ otteniamo un'algebra di Boole particolarmente importante, che indichiamo ancora con 2, come il reticolo di due elementi. Il reticolo (A, MCD, mcm), dove $A = \{x \in \omega : x \text{ divide } 30\}$, si può espandere a un'algebra di Boole definendo $\neg^{\mathcal{A}}(x) = 30/x$, $0^{\mathcal{A}} = 1$, $1^{\mathcal{A}} = 30$. Anche per le algebre di Boole vale un teorema di rappresentazione analogo a quello dei reticoli distributivi : ogni algebra di Boole è isomorfa a una sottostruttura di $\mathcal{B}(W)$, per un'opportuna scelta di W (si veda, ad esempio, [Davey-Priestley 90, teorema 10.4]). Il primo punto del teorema seguente mostra che ogni algebra di Boole è un reticolo limitato, poiché 0 e 1 soddisfano le condizioni poste dagli assiomi m) e M). D'ora in poi daremo le dimostrazioni in forma abbreviata, senza segnalare tutti gli assiomi o i teoremi precedenti utilizzati.

Teorema 2.4.5 *Le proposizioni seguenti valgono in ogni algebra di Boole:*

1. $x \wedge 0 = 0$ *e* $x \vee 1 = 1$, *ossia* $0 \leq x$ *e* $x \leq 1$,
2. $x \wedge 1 = x$ *e* $x \vee 0 = x$,
3. $x = \neg y$ *sse* $x \vee y = 1$ *e* $x \wedge y = 0$,
4. $x = \neg\neg x$,
5. $\neg(x \wedge y) = \neg x \vee \neg y$ *e* $\neg(x \vee y) = \neg x \wedge \neg y$ *(leggi di De Morgan)*,
6. $x \wedge y \leq z$ *sse* $x \leq \neg y \vee z$,
7. $x \leq y$ *sse* $\neg x \vee y = 1$.

1. Usando gli assiomi v), ii) e l'idempotenza (teorema 2.4.1): $x \wedge 0 = x \wedge (x \wedge \neg x) = (x \wedge x) \wedge \neg x = x \wedge \neg x = 0$. L'altra equazione si ottiene per dualità.

2. Usando gli assiomi v), i) e iii): $x \wedge 1 = x \wedge (x \vee \neg x) = (\neg x \vee x) \wedge x = x$. L'altra equazione si ottiene per dualità.

3. Se $x = \neg y$ allora $x \vee y = \neg y \vee y = 1$, utilizzando i) e v); $x \wedge y = 1$ si ottiene per dualità. Assumiamo ora $x \vee y = 1$ e $x \wedge y = 0$. Utilizzando gli assiomi v), iv), i) e il punto 2):

$$\begin{aligned} x &= x \wedge 1 \\ &= x \wedge (y \vee \neg y) \\ &= (x \wedge y) \vee (x \wedge \neg y) \\ &= 0 \vee (x \wedge \neg y) \\ &= (y \wedge \neg y) \vee (x \wedge \neg y) \\ &= (\neg y \wedge y) \vee (\neg y \wedge x) \\ &= \neg y \wedge (y \vee x) \\ &= \neg y \wedge 1 \\ &= \neg y. \end{aligned}$$

4. Per il punto precedente, basta verificare che $x \vee \neg x = 1$ e $x \wedge \neg x = 0$, il che segue da v).

5. Basta dimostrare la prima equazione, perché la seconda si ottiene per dualità. Per dimostrare che $\neg x \vee \neg y = \neg(x \wedge y)$ è sufficiente dimostrare, per il punto 3), che $(\neg x \vee \neg y) \vee (x \wedge y) = 1$ e $(\neg x \vee \neg y) \wedge (x \wedge y) = 0$. La prima è giustificata da

$$\begin{aligned} (\neg x \vee \neg y) \vee (x \wedge y) &= (\neg x \vee \neg y \vee x) \wedge (\neg x \vee \neg y \vee y) \\ &= 1 \wedge 1 \\ &= 1 \end{aligned}$$

e la seconda è giustificata da

$$\begin{aligned} (\neg x \vee \neg y) \wedge (x \wedge y) &= (\neg x \wedge x \wedge y) \wedge (\neg y \vee x \wedge y) \\ &= 0 \wedge 0 \\ &= 0. \end{aligned}$$

6. Se $x \wedge y \leq z$ allora $(x \wedge y) \vee \neg y \leq z \vee \neg y$ per il teorema 2.4.3. Ma

$$x \leq x \vee \neg y = (x \vee \neg y) \wedge (y \vee \neg y) = (x \wedge y) \vee \neg y$$

per la distributività, l'assioma v) e il punto 2) e quindi $x \leq \neg y \vee z$. Se $x \leq \neg y \vee z$ allora $x \wedge y \leq (\neg y \vee z) \wedge y$ per il teorema 2.4.3. Ma

$$(\neg y \vee z) \wedge y \leq (\neg y \wedge y) \vee (z \wedge y) = z \wedge y \leq y$$

per la distributività, l'assioma v) e il punto 2).

7. Per il punto 2) l'asserzione $x \leq y$ equivale a $1 \wedge x \leq y$, che equivale a $1 \leq \neg x \vee y$ per il punto 6), che infine equivale a $1 = \neg x \vee y$ per il punto 1).

Consideriamo ora $P(W)$ sotto un altro punto di vista, isolando come fondamentale la relazione di inclusione $\subseteq$ tra insiemi: la struttura che si ottiene è l'insieme ordinato $(P(W), \subseteq)$. Ora il tipo contiene solo il simbolo relazionale binario $\leq$ e nel linguaggio associato al tipo possiamo formulare gli assiomi che caratterizzano la relazione di inclusione come ordine parziale:

$\mathbf{a}_1$) $x \leq x$ (riflessività),

$\mathbf{a}_2$) se $x \leq y$ e $y \leq x$ allora $x = y$ (antisimmetria),

$\mathbf{a}_3$) se $x \leq y$ e $y \leq z$ allora $x \leq z$ (transitività).

Indichiamo con OP l'insieme degli assiomi a_1)-a_3). Tali assiomi fanno sì che in ogni modello $\mathcal{A}$ di OP la relazione $\leq^{\mathcal{A}}$ sia un ordine e quindi $\mathcal{A}$ sia un insieme ordinato. Anche per gli insiemi ordinati vale un *principio di dualità* analogo a quello dei reticoli, definendo la duale α^* di una proposizione α come la proposizione ottenuta da α sostituendo $\leq$ con $\geq$. Per giustificare questo principio basta osservare che ogni insieme ordinato $\mathcal{A} = (A, \leq)$ si trasforma in un altro insieme ordinato $\mathcal{A}^* = (A, \geq)$ tale che α vale in $\mathcal{A}$ sse α^* vale in $\mathcal{A}^*$. Se adottiamo la rappresentazione grafica degli insiemi ordinati del paragrafo 1.4, la rappresentazione di $\mathcal{A}^*$ si ottiene capovolgendo quella di $\mathcal{A}$.

Gli assiomi OP non colgono però un aspetto importante di $P(W)$: la possibilità di formare intersezioni e unioni. Il fatto che ora il linguaggio non disponga di simboli funzionali binari per rappresentare $\cap$ e $\cup$ non significa che non si possano esprimere, nei termini di $\subseteq$, le proprietà che caratterizzano $X \cap Y$ e $X \cup Y$. Iniziamo da $\cap$ e osserviamo che $X \cap Y \subseteq X$ e $X \cap Y \subseteq Y$. Inoltre, tra gli insiemi Z che sono simultaneamente inclusi in X e in Y, l'intersezione $X \cap Y$ è il massimo. Per quanto riguarda $\cup$ valgono le proprietà duali: $X \subseteq X \cup Y$ e $Y \subseteq X \cup Y$ e inoltre, tra gli insiemi Z che includono simultaneamente X e Y, l'unione $X \cup Y$ è il minimo. Da questa analisi possiamo ricavare gli assiomi seguenti:

$\mathbf{a}_4$) per ogni x, y esiste uno z tale che: $z \leq x$ e $z \leq y$ e per ogni w, se $w \leq x$ e $w \leq y$ allora $w \leq z$;

$\mathbf{a}_5$) per ogni x, y esiste uno z tale che: $x \leq z$ e $y \leq z$ e per ogni w, se $x \leq w$ e $y \leq w$ allora $z \leq w$.

Un insieme ordinato in cui valgano gli assiomi a_4) e a_5) è detto *reticolo*, per ragioni che risulteranno chiare dal teorema seguente. Supponiamo che $\mathcal{A}$ sia un insieme ordinato. Se $X \subseteq A$, diremo che un elemento a di A è un *confine superiore* di X se, per ogni $x \in X$, vale $x \leq a$. Sia X^+ l'insieme dei confini superiori di X: se X^+ ha un minimo, tale elemento è detto *minimo confine superiore*, o *supremum*, di X ed è denotato da $\sup X$. Dualmente, definiamo *confine inferiore* di X un elemento a di A tale che, per ogni $x \in X$, valga $a \leq x$.

Indichiamo con X^- l'insieme dei confini inferiori di X: se X^- ha un massimo, tale elemento è detto *massimo confine inferiore*, o *infimum*, di X ed è denotato da $\inf X$. Poiché il massimo e il minimo di un insieme, se esistono, sono unici, ne segue che $\inf X$ e $\sup X$, se esistono, sono unici. Quindi in una struttura che renda veri gli assiomi a_1)-a_5) possiamo usare $\inf\{x, y\}$ e $\sup\{x, y\}$ come funzioni binarie: gli assiomi a_4) e a_5) garantiscono l'esistenza del valore, l'antisimmetria l'unicità.

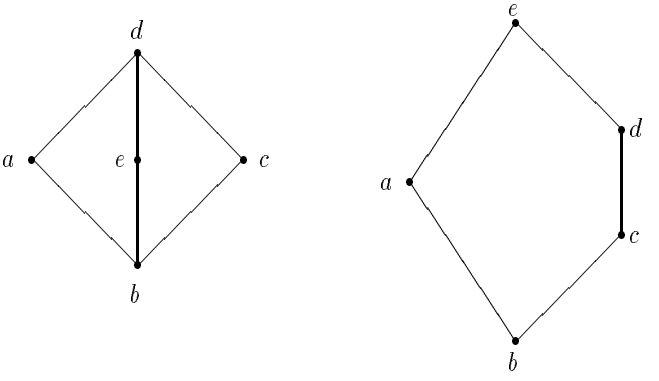
Teorema 2.4.6 *Se $\mathcal{A} = (A, \leq)$ è modello degli assiomi a_1)-a_5) allora possiamo espandere il suo tipo con l'aggiunta di due simboli funzionali binari $\wedge$ e $\vee$ in modo tale che, interpretando $\wedge$ su $\inf\{x, y\}$ e $\vee$ su $\sup\{x, y\}$, la struttura $(A, \wedge^{\mathcal{A}}, \vee^{\mathcal{A}})$ soddisfi gli assiomi L.*

La commutatività di $\wedge$ ossia $\inf\{x, y\} = \inf\{y, x\}$ dipende dal fatto che $\{x, y\} = \{y, x\}$. La commutatività di $\vee$ si ottiene per dualità. Per dimostrare l'associatività di $\wedge$ ossia

$$\inf\{x, \inf\{y, z\}\} = \inf\{\inf\{x, y\}, z\}$$

osserviamo innanzitutto che $\inf\{x, \inf\{y, z\}\} = \inf\{x, y, z\}$: basta verificare che $\{x, \inf\{y, z\}\}^- = \{x, y, z\}^-$. Analogamente si dimostra che $\inf\{\inf\{x, y\}, z\} = \inf\{x, y, z\}$. L'associatività di $\vee$ si ottiene per dualità. Dimostriamo che l'assioma $(x \wedge y) \vee y = y$ è vero, ossia che $\sup\{\inf\{x, y\}, y\} = y$. Osserviamo che $\inf\{x, y\} \leq y$ e quindi y appartiene a $\{\inf\{x, y\}, y\}^+$. D'altra parte, per ogni $z \in \{\inf\{x, y\}, y\}^+$ vale $y \leq z$ e quindi y è il minimo tra i confini superiori di $\{\inf\{x, y\}, y\}$.

Useremo quindi il termine reticolo per indicare sia una struttura per $\{\wedge, \vee\}$ in cui valgano gli assiomi L, sia una struttura per $\{\leq\}$ in cui valgano gli assiomi a_1)-a_5), lasciando al contesto il compito di determinare quale delle due accezioni del termine stiamo usando.



Spesso conviene pensare un reticolo come un particolare insieme ordinato, perché in tal modo possiamo darne una rappresentazione grafica intuitiva. La figura precedente presenta due reticoli nei quali non vale l'assioma di distributività. Nel primo $e \wedge (a \vee c) \neq (e \wedge a) \vee (e \wedge c)$ nel secondo $d \wedge (a \vee c) \neq (d \wedge a) \vee (d \wedge c)$.

Esercizio 2.4.1 Si dimostri che ogni catena (insieme totalmente ordinato) è un reticolo. Si fornisca quindi un esempio di reticolo non limitato.

Esercizio 2.4.2 Se $\mathcal{A} = (A, \wedge, \vee)$ e $\mathcal{B} = (B, \wedge, \vee)$ sono due reticoli e $\varphi{:}\mathcal{A} \to \mathcal{B}$ è un omomorfismo, allora φ conserva anche la relazione d'ordine associata ai reticoli. Se $\mathcal{A} = (A, \leq)$ e $\mathcal{B} = (B, \leq)$ sono due reticoli e $\varphi{:}\mathcal{A} \to \mathcal{B}$ è un omomorfismo, allora φ in genere non conserva le operazioni inf e sup.

Esercizio 2.4.3 Espandiamo un reticolo con due costanti 0 e 1 che soddisfino i due assiomi seguenti: i) $x \wedge 1 = x$, ii) $x \vee 0 = x$. Si dimostri che il reticolo così ottenuto è limitato. Viceversa, si dimostri che in ogni reticolo limitato valgono i) e ii).

Esercizio 2.4.4 Sia 2 il reticolo $\mathcal{R}(1) = (\{0, 1\}, \cap, \cup)$. Si dimostri che tutti i reticoli con due elementi sono isomorfi a 2. Si dimostri un risultato analogo per le algebre di Boole.

Esercizio 2.4.5 Sia a un elemento fissato di A. Si dimostri che la funzione $f : P(A) \to 2$ definita ponendo, per ogni $X \subseteq A$,

$$f(X) = \begin{cases} 0 & se \quad a \notin X \\ 1 & se \quad a \in X \end{cases}$$

è un omomorfismo da $\mathcal{B}(A)$ verso 2, dove 2 è l'algebra di Boole con due elementi.

Esercizio 2.4.6 In ogni reticolo limitato A definiamo complemento di un elemento a un elemento a' tale che $a \wedge a' = 0$ e $a \vee a' = 1$. Diremo che un reticolo è complementato se è limitato e ogni elemento ha un complemento. Si dimostri che in un reticolo complementato e distributivo ogni elemento ha un unico complemento. Quindi in ogni reticolo complementato e distributivo si può espandere a un'algebra di Boole.

2.5 Definizioni induttive

Tutti gli oggetti del nostro discorso sono insiemi, quindi ogni volta che si definisce un oggetto si tratta della definizione di un insieme. Fino a questo punto le definizioni adottate sono state sempre del tipo seguente: dato un insieme A e una proprietà P, definiamo $\{x : P(x)\}$ come l'insieme degli elementi di A che godono di P. Diremo che l'insieme in questione è definito *esplicitamente* sulla base dell'insieme A dalla proprietà P. Ad esempio, l'insieme dei numeri pari può essere definito sulla base dell'insieme dei numeri naturali ω considerando la proprietà "esiste un $n \in \omega$ tale che $n + n = x$". Cerchiamo ora di immaginare l'insieme dei pari come il frutto di un processo generativo ne fornisca gli elementi in successione. Non è difficile immaginare una legge di generazione che operi all'interno di ω: si parte da 0 e quindi si applica la funzione $\psi(x) = x + 2$ ripetutamente ottenendo $\{0, \psi(0), \psi(\psi(0)), \ldots\}$. È immediato riconoscere che

abbiamo ottenuto l'insieme dei numeri pari, anche se non è altrettanto immediato giustificare questo tipo di definizione. Gli elementi dell'insieme possiedono una descrizione uniforme, ma siamo ben lontani dall'avere una definizione esplicita, cioè una proprietà goduta da tutti e soli gli elementi dell'insieme.

Sottolineiamo che quando si parla di "processo generativo" non si intende necessariamente che in virtù di questo processo si porti qualcosa all'esistenza. Esistono infatti due modi profondamente diversi di considerare le definizioni degli oggetti matematici: si può ritenere che esse creino gli oggetti che definiscono, che nell'atto della definizione si conferisca ad essi l'esistenza, oppure si può pensare che le definizioni si limitino a segnare i confini di un insieme di oggetti e che quindi abbiano un compito puramente descrittivo. Noi adottiamo questo secondo punto di vista e quindi assumiamo che sia gli oggetti che verranno a costituire un insieme, sia l'insieme stesso di questi oggetti, preesistano alla definizione e che quest'ultima sia solo un modo per individuare tale insieme e sottoporlo all'attenzione. Nell'esempio precedente i numeri pari già esistono come elementi dell'insieme ω. Se proprio vogliamo vedere qualcosa che si crea, questo è il "bordo" dell'insieme dei pari che viene ritagliato in ω, ma ciò non è strettamente necessario, dato che l'insieme dei pari esiste già come elemento di $\mathcal{P}(\omega)$, l'insieme potenza di ω che contiene tutti i sottoinsiemi di ω. Alle definizioni non attribuiamo dunque alcuna facoltà creatrice: tutto esiste fin dall'inizio ed è proprio nel momento iniziale, cioè negli assiomi della teoria degli insiemi, che si stabilisce che cosa debba esistere.

Vediamo ora di cogliere gli aspetti più generali di questo nuovo modo di definire insiemi. Innanzitutto supponiamo che ogni definizione di questo tipo sia formulata in riferimento a una data struttura $\mathcal{A}$: ciò significa che essa avrà il compito di definire un sottoinsieme del dominio A di $\mathcal{A}$ e che nel fare ciò potrà utilizzare solo funzioni e costanti della struttura $\mathcal{A}$. Vi sono inoltre due elementi della definizione precedente che possono essere generalizzati: possiamo ammettere come punto di partenza un sottoinsieme qualsiasi di A, senza necessariamente limitarci a quelli unitari, e possiamo ammettere che il processo generativo sia sostenuto dall'insieme $\mathcal{F}$ delle funzioni e delle costanti di $\mathcal{A}$, piuttosto che da un'unica funzione. Chiameremo allora *definizione induttiva* in $\mathcal{A}$ una coppia $(B, \mathcal{F})$ tale che $B \subseteq A$, $B \neq \emptyset$ e $\mathcal{F}$ è l'insieme delle funzioni e delle costanti di $\mathcal{A}$. Diremo che un insieme $X \subseteq A$ è $(B, \mathcal{F})$-*chiuso* se:

1. $B \subseteq X$,
2. $c^{\mathcal{A}} \in X$, per ogni $c^{\mathcal{A}} \in \mathcal{F}$,
3. $F^{\mathcal{A}}(x_0, \ldots, x_{n-1}) \in X$, per ogni $F^{\mathcal{A}} \in \mathcal{F}$ e $x_0, \ldots, x_{n-1} \in X$.

Diremo infine che l'insieme

$$I_{B,\mathcal{F}} = \bigcap \{X \subseteq A : X \text{ è } (B, \mathcal{F})\text{-chiuso}\}$$

è l'insieme *definito per induzione da* $(B, \mathcal{F})$ in $\mathcal{A}$. Gli insiemi $(B, \mathcal{F})$-chiusi coincidono con le sottostrutture di $\mathcal{A}$ che includono B e quindi $I_{B,\mathcal{F}}$ è il dominio

della sottostruttura generata da B in $\mathcal{A}$. Consideriamo, ad esempio, la struttura $\mathcal{A} = (\omega, F^{\mathcal{A}})$, dove $F^{\mathcal{A}}(n) = n + 2$, e poniamo $B = \{0\}$ e $\mathcal{F} = \{F^{\mathcal{A}}\}$: l'insieme $I_{B,\mathcal{F}}$ definito per induzione dalla coppia $(B, \mathcal{F})$ è l'insieme dei pari.

L'insieme $I_{B,\mathcal{F}}$, proprio perché è definito induttivamente da $(B, \mathcal{F})$ in $\mathcal{A}$, possiede una particolare struttura alla quale possiamo fare appello quando vogliamo dimostrare che ogni suo elemento gode di una particolare proprietà P. Il teorema seguente convalida un *principio di induzione* che garantisce la possibilità di dimostrare per induzione.

Teorema 2.5.1 *Per ogni definizione induttiva $(B, \mathcal{F})$ in $\mathcal{A}$ e per ogni proprietà $P \subseteq A$, per dimostrare che $I_{B,\mathcal{F}} \subseteq P$ basta dimostrare che P è $(B, \mathcal{F})$-chiuso.*

Poiché $I_{B,\mathcal{F}}$ è l'intersezione di tutti gli insiemi $(B, \mathcal{F})$-chiusi, è incluso in ogni insieme $(B, \mathcal{F})$-chiuso e quindi, in particolare, in P.

Se $\mathcal{A} = (\omega, \sigma)$ allora $A = I_{B,\mathcal{F}}$, con $B = \{0\}$ e $\mathcal{F} = \{\sigma\}$, e in questo caso il principio di induzione coincide con l'induzione sui naturali del paragrafo 1.5. Come primo esempio di dimostrazione per induzione, presentiamo un teorema che ci sarà utile nel paragrafo seguente.

Teorema 2.5.2 *Supponiamo che $\mathcal{A}$ sia generata da $B \subseteq A$. Se $\mathcal{D}$ è una struttura dello stesso tipo di $\mathcal{A}$ e h e h' sono due morfismi da $\mathcal{A}$ verso $\mathcal{D}$ che coincidono sui generatori, ossia tali che $h(b) = h'(b)$ per ogni $b \in B$, allora $h = h'$.*

Sia $K = \{x \in A : h(x) = h'(x)\}$. Se dimostriamo che $K = A$, allora per ogni $x \in A$ avremo $h(x) = h'(x)$ e quindi $h = h'$. Poiché per ipotesi $A = I_{B,\mathcal{F}}$, dove $\mathcal{F}$ è l'insieme delle funzioni e delle costanti di $\mathcal{A}$, possiamo procedere per induzione mostrando che K è $(B, \mathcal{F})$-chiuso. Verifichiamo che $B \subseteq K$: ciò deriva immediatamente dal fatto che h e h' coincidono per ipotesi sui generatori. Verifichiamo che $c^{\mathcal{A}} \in K$, per ogni costante di $\mathcal{A}$. Poiché h e h' sono morfismi

$$h(c^{\mathcal{A}}) = c^{\mathcal{D}} = h'(c^{\mathcal{A}}).$$

Supponiamo ora che $F^{\mathcal{A}}$ sia una funzione n-aria di $\mathcal{A}$ e mostriamo che, se ogni a_i appartiene a K, per $i < n$, allora $F^{\mathcal{A}}(a_0, \ldots, a_{n-1}) \in K$. A tale scopo basta verificare che, essendo h e h' morfismi,

$$\begin{aligned} h(F^{\mathcal{A}}(a_0, \ldots, a_{n-1})) &= F^{\mathcal{D}}(h(a_0), \ldots, h(a_{n-1})) \\ &= F^{\mathcal{D}}(h'(a_0), \ldots, h'(a_{n-1})) \\ &= h'(F^{\mathcal{A}}(a_0, \ldots, a_{n-1})). \end{aligned}$$

La seconda riga deriva dal fatto che $a_0, \ldots, a_{n-1} \in K$.

Il punto più delicato delle dimostrazioni per induzione è il passo induttivo, ossia la dimostrazione dell'implicazione "se $a_i \in P$, per ogni $i < n$, allora $F^{\mathcal{A}}(a_0, \ldots, a_{n-1}) \in P$" che garantisce l'estendibilità di P da B a tutto $I_{B,\mathcal{F}}$. Per dimostrare che $F^{\mathcal{A}}(a_0, \ldots, a_{n-1})$ appartiene a P può accadere che occorra assumere non solo che P sia goduta da ogni a_i, ma che P sia goduta anche da

tutti gli elementi di $I_{B,\mathcal{F}}$ che sono "più semplici" di $F^{\mathcal{A}}(a_0, \ldots, a_{n-1})$, rispetto a un criterio di semplicità prefissato. Dimostriamo che questo modo di procedere è lecito. Innanzitutto conveniamo di misurare la semplicità degli elementi di un insieme qualsiasi A mediante una funzione $\varphi : A \to \omega$. Vedremo in seguito che esistono diversi tipi di misure, per il momento chiameremo genericamente *livello* il numero naturale assegnato da φ agli elementi di A. Definiamo $A_i = \{x : \varphi(x) \leq i\}$ per ogni $i \in \omega$, l'insieme di tutti gli elementi di A aventi livello $\leq i$. Evidentemente gli insiemi A_i formano una catena.

Lemma 2.5.3 *Sia $\varphi : A \to \omega$ e $P \subseteq A$. Se $A_0 \subseteq P$ e, per ogni $i \in \omega$, $A_i \subseteq P$ implica $A_{i+1} \subseteq P$, allora $A = P$.*

Consideriamo l'insieme di numeri naturali $N = \{x : A_x \subseteq P\}$. Per induzione su ω possiamo concludere che $N = \omega$ e quindi, per ogni $i \in \omega$, $A_i \subseteq P$. Quindi $A \subseteq P$ dato che $A = \bigcup\{A_i\}_{i\in\omega}$. Poiché $P \subseteq A$ possiamo concludere $P = A$.

Diremo che un elemento $a \in A$ è *P,φ-completo* se, per ogni $x \in A$, $\varphi(x) < \varphi(a)$ implica $P(x)$. Diremo che una proprietà P è *φ-progressiva* se ogni elemento P,φ-completo gode di P. In altri termini, se P è φ-progressiva accade che quando un elemento x di A è tale che tutti gli elementi più semplici di x godono di P, anche x gode di P, dove maggiore semplicità significa livello minore. Possiamo allora convalidare il principio induttivo seguente.

Teorema 2.5.4 *Se $\varphi : A \to \omega$ e P è φ-progressiva, allora $A = P$.*

Dimostriamo che $A_0 \subseteq P$. Se $a \in A_0$ allora $\varphi(a) = 0$ e quindi $\varphi(x) < \varphi(a)$ è falsa per ogni $x \in A$. Allora è banalmente vero che $\varphi(x) < \varphi(a)$ implica $P(a)$. Ciò dimostra che a è P,φ-completo e poiché P è φ-progressiva $a \in P$. Mostriamo ora che, per ogni $i \in \omega$, $A_i \subseteq P$ implica $A_{i+1} \subseteq P$. Per il lemma precedente potremo allora concludere che $A = P$. Sia $A_i \subseteq P$ e sia $a \in A_{i+1}$. Poiché $A_i \subseteq A_{i+1}$ si danno due casi. Caso 1), $a \in A_i$ e allora per ipotesi induttiva $a \in P$. Caso 2), $a \in A_{i+1} - A_i$, allora $\varphi(a) = i + 1$. Per ogni $x \in A$, $\varphi(x) < \varphi(a)$ implica $x \in P$, perché $\varphi(x) < \varphi(a)$ implica $\varphi(x) \leq i$ e quindi $x \in A_i$. Allora a è P,φ-completo e poiché P è φ-progressiva per ipotesi, $a \in P$. Quindi in entrambi i casi $A_{i+1} \subseteq P$.

Esercizio 2.5.1 Supponiamo che $\mathcal{A}$ abbia dominio ω. Si verifichi che $I_{B,\mathcal{F}}$ è: $\omega - \{0\}$ quando $B = \{1\}$ e $\mathcal{F} = \{+\}$, ω quando $B = \{0\}$ e $\mathcal{F} = \{\sigma, +\}$, $\{0\}$ quando $B = \{0\}$ e $\mathcal{F} = \{+\}$. Se $\mathcal{F} = \{\cdot\}$, qual è il minimo B tale che $I_{B,\mathcal{F}} = \omega$?

2.6 Definizioni per recursione

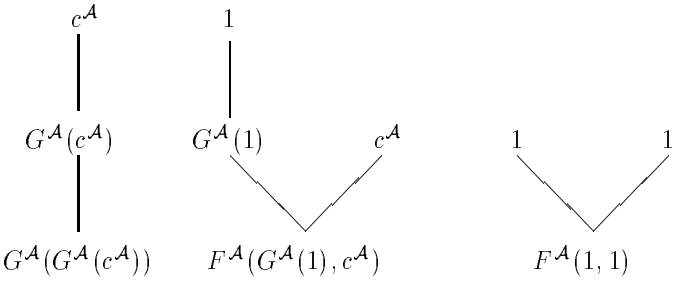
Se $\mathcal{A}$ è generata da B e la struttura $\mathcal{D}$ è dello stesso tipo di $\mathcal{A}$, potremmo cercare di definire una funzione $h : \mathcal{A} \to \mathcal{D}$ nel modo seguente. Fissiamo il comportamento di h sugli elementi di B, vale a dire supponiamo data una funzione $g : B \to D$ e poniamo $h(b) = g(b)$ per ogni $b \in B$. Quanto agli

$a \in A - B$, poniamo

$$h(a) = \begin{cases} c^{\mathcal{D}} & \text{se } a = c^{\mathcal{A}} \\ F^{\mathcal{D}}(h(a_0) \dots h(a_{n-1})) & \text{se } a = F^{\mathcal{A}}(a_0, \dots, a_{n-1}). \end{cases}$$

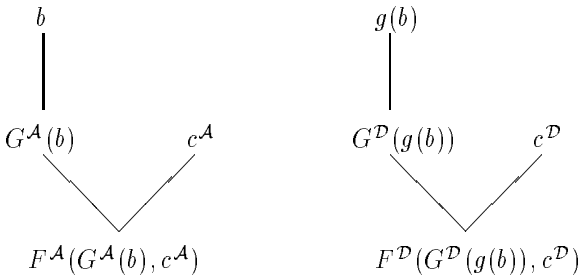
Diremo allora che h è definita *per recursione*. Che cosa garantisce che abbiamo veramente definito una funzione da A verso D, ossia che ad ogni elemento di A abbiamo associato un unico valore? Se $a = c^{\mathcal{A}}$ e $a \in B$ abbiamo $c^{\mathcal{D}} = h(a) = g(a)$, e nulla garantisce che $c^{\mathcal{D}}$ sia uguale a $g(a)$. Inoltre $h(F^{\mathcal{A}}(a_0, \dots, a_{n-1}))$ sembra definito in modo circolare nei termini dei vari $h(a_i)$: chi ci assicura che abbiamo definito qualcosa? Il teorema di recursione che dimostreremo in questo paragrafo mostra che è possibile definire per recursione, quando $\mathcal{A}$ soddisfa particolari condizioni, ma prima di presentare la dimostrazione del teorema conviene riesaminare le definizioni induttive.

Sia $\mathcal{A}$ una struttura, $B \subseteq A$ e $\mathcal{F}$ l'insieme delle funzioni e delle costanti di $\mathcal{A}$. (Non è necessario supporre che $I_{B,\mathcal{F}}$ coincida con A.) Nel paragrafo precedente abbiamo sottolineato che le definizioni induttive non creano gli oggetti che definiscono, è vero tuttavia che gli elementi di $I_{B,\mathcal{F}}$ sono ottenuti da B con un processo di generazione nel quale intervengono le funzioni e le costanti di $\mathcal{F}$. Il processo di generazione di un $a \in I_{B,\mathcal{F}}$ può essere rappresentato mediante un albero etichettato $\varphi : \tau \to A$, ossia una funzione φ che assegna ad ogni nodo dell'albero τ un oggetto di A come etichetta. Richiederemo che il vertice di τ sia etichettato da a e che i nodi terminali siano etichettati dagli elementi di B e dalle costanti di $\mathcal{F}$ che intervengono nel processo. Se $\nu \in \tau$ non è un nodo terminale e se $\nu_0, \dots, \nu_{n-1}$ sono i suoi successori, allora ν riceverà come etichetta $F^{\mathcal{A}}(a_0, \dots, a_{n-1})$, dove a_i è l'etichetta di ν_i per $i < n$. Un albero etichettato di questo genere è detto $(B, \mathcal{F})$-*costruzione* di a, o semplicemente costruzione, se è chiaro dal contesto qual è la coppia $(B, \mathcal{F})$ a cui si fa riferimento. Supponiamo, ad esempio, che sia $\mathcal{A} = (\omega, G^{\mathcal{A}}, F^{\mathcal{A}}, c^{\mathcal{A}})$, dove $G^{\mathcal{A}}$ è il successore, $F^{\mathcal{A}}$ la somma, $c^{\mathcal{A}}$ lo zero, e poniamo $B = \{1\}$. Possiamo visualizzare alcune costruzioni nel modo seguente:



Nella figura precedente sono mostrate tre costruzioni di 2: è evidente, quindi, che un elemento può avere costruzioni differenti. Tuttavia, se ci limitiamo a considerare strutture $\mathcal{A}$ in cui ogni elemento del dominio ha un'unica costruzione, allora possiamo sfruttare questa caratteristica di $\mathcal{A}$ per definire $h : \mathcal{A} \to \mathcal{D}$

per recursione. Dato $a \in A$ consideriamo l'unica costruzione che lo genera e la trasformiamo modificandone sistematicamente le etichette nel modo seguente: i) sostituendo nei nodi terminali b con $g(b)$ e le costanti di $\mathcal{A}$ con quelle di $\mathcal{D}$, ii) utilizzando negli altri nodi le funzioni di $\mathcal{D}$ corrispondenti a quelle di $\mathcal{A}$. La figura seguente illustra questa trasformazione:



Definiamo $h(a)$ come l'elemento nel vertice della costruzione trasformata. Nel caso della figura precedente,

$$h(F^{\mathcal{A}}(G^{\mathcal{A}}(b), c^{\mathcal{A}})) = F^{\mathcal{D}}(G^{\mathcal{D}}(g(b)), c^{\mathcal{D}}).$$

È evidente che una h così definita è un morfismo, mentre il fatto che sia una funzione dipende essenzialmente dall'unicità della costruzione degli elementi della struttura $\mathcal{A}$.

Il processo mediante il quale si trasforma una $(B, \mathcal{F})$- costruzione in una $(g[B], \mathcal{H})$-costruzione, dove $\mathcal{H}$ è l'insieme di funzioni e costanti di $\mathcal{D}$, è alla base della dimostrazione del teorema di recursione. La condizione che ogni elemento di $\mathcal{A}$ abbia un'unica costruzione è rimpiazzata dalla richiesta che $\mathcal{A}$ sia *generata liberamente* da B, ossia che $\mathcal{A}$ sia generata da B e che $(B, \mathcal{F})$ soddisfi le condizioni seguenti:

1. $c^{\mathcal{A}} \notin B$, per ogni $c^{\mathcal{A}} \in \mathcal{F}$,
2. $c^{\mathcal{A}} \neq e^{\mathcal{A}}$, per ogni $c^{\mathcal{A}}$, $e^{\mathcal{A}} \in \mathcal{F}$ tali che $c \neq e$,
3. $Im(F^{\mathcal{A}}) \cap B = \emptyset$, per ogni $F^{\mathcal{A}} \in \mathcal{F}$,
4. $Im(F^{\mathcal{A}}) \cap Im(G^{\mathcal{A}}) = \emptyset$, per ogni $F^{\mathcal{A}}$, $G^{\mathcal{A}} \in \mathcal{F}$ tali che $F \neq G$,
5. $c^{\mathcal{A}} \notin Im(F^{\mathcal{A}})$, per ogni $c^{\mathcal{A}}$, $F^{\mathcal{A}} \in \mathcal{F}$,
6. $F^{\mathcal{A}}$ è iniettiva, per ogni $F^{\mathcal{A}} \in \mathcal{F}$.

(È possibile dimostrare che se $\mathcal{A}$ è generata liberamente, ogni suo elemento possiede un'unica costruzione.)

Teorema 2.6.1 *Se $\mathcal{A}$ è generata liberamente da $B \subseteq A$ allora, per ogni struttura $\mathcal{D}$ dello stesso tipo di $\mathcal{A}$ e ogni $g : B \to D$, esiste un'unico morfismo $h : \mathcal{A} \to \mathcal{D}$ che estende g.*

La funzione h che definiremo è un insieme di coppie ordinate incluso in $A \otimes D$. Poiché h sarà definita per induzione, penseremo $A \otimes D$ come il dominio di una struttura $\mathcal{C} = \mathcal{A} \otimes \mathcal{D}$, detta prodotto cartesiamo di $\mathcal{A}$ per $\mathcal{B}$ e definita nel modo seguente. La struttura $\mathcal{C}$ ha lo stesso tipo τ di $\mathcal{A}$ e $\mathcal{D}$ e inoltre $c^{\mathcal{C}} =< c^{\mathcal{A}}, c^{\mathcal{D}} >$ per ogni simbolo di costante c e

$$F^{\mathcal{C}}(< x_0, y_0 >, \ldots, < x_{n-1}, y_{n-1} >) =< F^{\mathcal{A}}\overline{x}, F^{\mathcal{D}}\overline{y} >$$

per ogni simbolo di funzione F, dove $\overline{x} \in A^n$ e $\overline{y} \in D^n$. Consideriamo allora la definizione induttiva $(g, \mathcal{F}^*)$ in $\mathcal{C}$, dove $\mathcal{F}^*$ è costituito da tutte le funzioni e le costanti di $\mathcal{C}$ e poniamo $h = I_{g,\mathcal{F}^*}$. La dimostrazione del fatto che h soddisfa le condizioni del teorema si articola in quattro punti.

1. Dimostriamo che h è una funzione. Sia K l'insieme degli elementi di A sui quali h, se è defnita, è univoca:

$$K = \{x \in A : \ < x, y >, < x, z > \in h \text{ implica } y = z\}.$$

Dimostreremo che K è $B, \mathcal{F}$-chiuso e quindi $K = A$. Poiché per ogni $< x, y >$ e $< x, z >$ in h vale sempre $x \in A$, ne segue che $y = z$, quindi h è una funzione. Passiamo ora alla dimostrazione di $B, \mathcal{F}$-chiusura per K.

Dimostriamo che $B \subseteq K$. Dobbiamo verificare che se $< b, y >$ e $< b, z >$ sono in h allora $y = z$. Se $< b, y >$ è in h si danno i tre casi seguenti: i) $< b, y > \in g$ e allora $y = g(b)$; ii) $< b, y >=< c^{\mathcal{A}}, c^{\mathcal{D}} >$, per qualche simbolo di costante c, ma allora $b = c^{\mathcal{A}}$, il che è impossibile per il punto 1) della definizione di struttura generata liberamente; iii) $< b, y >=< F^{\mathcal{A}}\overline{x}, F^{\mathcal{D}}\overline{y} >$, per qualche simbolo di funzione F e per $\overline{x} \in A^n$, $\overline{y} \in D^n$, ma allora $b = F^{\mathcal{A}}\overline{x}$, il che è impossibile per il punto 3) della definizione. Analogamente se $< b, z >$ è in h possiamo dimostrare che $z = g(b)$. Ma allora $y = g(b) = z$.

Dimostriamo che $c^{\mathcal{A}} \in K$, per ogni simbolo di costante c. Dobbiamo verificare che se $< c^{\mathcal{A}}, y >$ e $< c^{\mathcal{A}}, z >$ sono in h allora $y = z$. Se $< c^{\mathcal{A}}, y >$ è in h si danno i tre casi seguenti: i) $< c^{\mathcal{A}}, y > \in g$ e allora $< c^{\mathcal{A}}, y >=< b, g(b) >$ e quindi $c^{\mathcal{A}} = b$, per qualche $b \in B$, ma ciò è impossibile per il punto 1) della definizione; ii) $< c^{\mathcal{A}}, y >=< e^{\mathcal{A}}, e^{\mathcal{D}} >$, per qualche simbolo di costante e, e quindi $c^{\mathcal{A}} = e^{\mathcal{A}}$ e $y = e^{\mathcal{D}}$, ma allora $c = e$ per il punto 2) della definizione e quindi $y = e^{\mathcal{D}} = c^{\mathcal{D}}$; iii) $< c^{\mathcal{A}}, y >=< F^{\mathcal{A}}\overline{x}, F^{\mathcal{D}}\overline{y} >$, per qualche simbolo di funzione F e per $\overline{x} \in A^n$, $\overline{y} \in D^n$, ma allora $c^{\mathcal{A}} = F^{\mathcal{A}}\overline{x}$, il che è impossibile per il punto 5) della definizione. Quindi se $< c^{\mathcal{A}}, y >$ è in h deve essere $y = c^{\mathcal{D}}$. Analogamente se $< c^{\mathcal{A}}, z >$ è in h deve essere $z = c^{\mathcal{D}}$. Quindi dalla nostra ipotesi segue $y = c^{\mathcal{D}} = z$.

Dimostriamo che se $\overline{a} \in K^n$ allora $F^{\mathcal{A}}\overline{a} \in K$. Dobbiamo verificare che se $< F^{\mathcal{A}}\overline{a}, y >$ e $< F^{\mathcal{A}}\overline{a}, z >$ sono in h allora $y = z$. Se $< F^{\mathcal{A}}\overline{a}, y >$ è in h si danno i tre casi seguenti: i) $< F^{\mathcal{A}}\overline{a}, y >=< b, g(b) >$, per qualche $b \in B$, ma allora $F^{\mathcal{A}}\overline{a} = b$ e ciò è impossibile per il punto 3) della definizione; ii) $< F^{\mathcal{A}}\overline{a}, y >=< e^{\mathcal{A}}, e^{\mathcal{D}} >$, per qualche simbolo di costante e, ma allora $F^{\mathcal{A}}\overline{a} = e^{\mathcal{A}}$ e $y = e^{\mathcal{D}}$, ma ciò è impossibile per il punto 5) della definizione; iii) $< F^{\mathcal{A}}\overline{a}, y >=< G^{\mathcal{A}}\overline{q}, G^{\mathcal{D}}\overline{r} >$, dove $\overline{q} \in A^m$ e $\overline{r} \in D^m$ e dove $< q_i, r_i >$

appartiene a h. Allora

$$F^{\mathcal{A}}(a_0, ..., a_{n-1}) = G^{\mathcal{A}}(q_0, \ldots, q_{m-1})$$

da cui segue per il punto 4) della definizione sia $F = G$ sia $n = m$. Quindi

$$F^{\mathcal{A}}(a_0, ..., a_{n-1}) = F^{\mathcal{A}}(q_0, \ldots, q_{n-1})$$

da cui segue $a_i = q_i$ per il punto 6) della definizione. Allora anche $< a_i, r_i >$ appartiene a h. Poiché $F = G$ e $n = m$, abbiamo

$$y = G^{\mathcal{D}}(r_0, \ldots, r_{m-1}) = F^{\mathcal{D}}(r_0, \ldots, r_{n-1})$$

e poiché $h(a_i) = r_i$, vale $F^{\mathcal{D}}(r_0, \ldots, r_{n-1}) = F^{\mathcal{D}}(h(a_0), \ldots, h(a_{n-1}))$. Abbiamo allora $y = F^{\mathcal{D}}(h(a_0), \ldots, h(a_{n-1}))$. Se $< F^{\mathcal{A}}(\overline{a}), z >$ è in h otteniamo analogamente $z = F^{\mathcal{D}}(h(a_0), \ldots, h(a_{n-1}))$ e quindi $y = z$.

2. Dimostriamo che $Dom(h) = A$ e $\mathrm{Im}(h) \subseteq D$. È evidente che $\mathrm{Im}(h)$ è inclusa in D. Dimostriamo che A è il dominio di h. A tale scopo basta dimostrare che $Dom(h)$ è $(B, \mathcal{F})$-chiuso. Vale $B \subseteq Dom(h)$, dato che $g \subseteq h$ e $B = Dom(g)$. Vale $c^{\mathcal{A}} \in Dom(h)$, dato che $< c^{\mathcal{A}}, c^{\mathcal{D}} > \in h$ per ogni simbolo di costante c. Supponiamo ora che $a_0, \ldots, a_{n-1} \in Dom(h)$ e dimostriamo che $F^{\mathcal{A}}(\overline{a}) \in Dom(h)$. Per ipotesi esistono $d_0, \ldots, d_{n-1} \in D$ tali che ogni $< a_i, d_i >$ appartiene a h e quindi anche $< F^{\mathcal{A}}(\overline{a}), F^{\mathcal{A}}(\overline{d}) >$ appartiene a h, poiché h è $(g, \mathcal{F}^*)$-chiuso. Ma allora $F^{\mathcal{A}}(\overline{a})$ appartiene a $Dom(h)$.

3. Dimostriamo h è un omomorfismo. Vale ovviamente $h(c^{\mathcal{A}}) = c^{\mathcal{D}}$. Supponiamo ora che $a_0, \ldots, a_{n-1} \in A$, poiché $Dom(h) = A$ esistono $d_0, \ldots, d_{n-1} \in D$ tali che $h(a_i) = d_i$. Poiché h è un insieme $(g, \mathcal{F}^*)$-chiuso deve contenere anche $< F^{\mathcal{A}}(\overline{a}), F^{\mathcal{D}}(\overline{d}) >$ e quindi

$$h(F^{\mathcal{A}}(a_0, \ldots, a_{n-1})) = F^{\mathcal{D}}(d_0, \ldots, d_{n-1}) = F^{\mathcal{D}}(h(a_0) \ldots h(a_{n-1})).$$

4. Infine si dimostra facilmente, utilizzando il teorema 2.5.2, che h è l'unico omomorfismo da $\mathcal{A}$ verso $\mathcal{D}$ che estende g.

Gli esempi più semplici di definizioni per recursione si ottengono utilizzando la struttura $\mathcal{A} = (\omega, \sigma^{\mathcal{A}})$, dove $\sigma^{\mathcal{A}} = \sigma$. È evidente che $\mathcal{A}$ è generata liberamente da $B = \{0\}$. Se consideriamo la struttura $\mathcal{D} = (\omega, \sigma^{\mathcal{D}})$, dove $\sigma^{\mathcal{D}} = \psi$, allora il teorema 2.6.1 garantisce che per ogni funzione $g : \{0\} \to \omega$ esiste un'unica funzione $\varphi : \omega \to \omega$ tale che

$$\varphi(0) = g(0) \quad \text{e} \quad \varphi(\sigma(n)) = \psi(\varphi(n)).$$

Diremo allora che φ è definita per iterazione a partire da ψ e da g.

Il teorema 2.6.1 permette di giustificare anche definizioni più complesse dell'iterazione, nelle quali il valore $\varphi(n+1)$ dipende non solo dal valore precedente $\varphi(n)$, ma anche dal livello della recursione, ossia da n. Diremo che una funzione $\varphi : \omega \to \omega$ è definita per recursione primitiva da k e $\psi : {}^2\omega \to \omega$ se

$$\varphi(0) = k \quad \text{e} \quad \varphi(\sigma(n)) = \psi(\varphi(n), n).$$

Mentre nell'iterazione abbiamo $\varphi(n+1) = \psi(\ldots\psi(0)\ldots)$, dove la funzione ψ viene applicata $n+1$-volte, nella recursione primitiva abbiamo la chiamata in successione di diverse funzioni, tutte ottenibili come parametrizzazioni di ψ. Se parametrizziamo la seconda variabile di ψ con differenti numeri naturali, otteniamo la successione di funzioni

$$\psi_0(x) = \psi(x,0), \ldots, \psi_n(x) = \psi(x,n), \ldots$$

e possiamo scrivere $\varphi(n+1) = \psi_n(\ldots\psi_0(0)\ldots)$. Non si tratta quindi di un'iterazione, ma l'uniformità che sussiste nel passaggio dal calcolo del valore per n al calcolo del valore per $n+1$ è sufficiente per poter afferrare la procedura come un unico processo, detto recursione primitiva. Il teorema seguente giustifica una forma più generale di recursione primitiva che ci sarà utile in seguito.

Teorema 2.6.2 *Per ogni $c \in C$ e $\psi : C\times\omega \to C$, esiste una funzione $\varphi : \omega \to C$ tale che*

$$\varphi(0) = c \quad e \quad \varphi(\sigma(n)) = \psi(\varphi(n), n).$$

Diremo che φ è definita per recursione primitiva da c e ψ.

Consideriamo una struttura $\mathcal{A} = (\omega, \sigma^{\mathcal{A}})$, dove $\sigma^{\mathcal{A}} = \sigma$, e una struttura $\mathcal{D} = (C\times\omega, \sigma^{\mathcal{D}})$ dove, per ogni $x \in C$ e ogni $n \in \omega$, $\sigma^{\mathcal{D}}(x,n) = (\psi(x,n), \sigma(n))$. Per il teorema 2.6.1 esiste una funzione $\eta : \omega \to D$ tale che

$$\eta(0) = (c,0) \quad \text{e} \quad \eta(\sigma^{\mathcal{A}}(n)) = \sigma^{\mathcal{D}}(\eta(n)).$$

Osserviamo che $\eta(n) = (i_0^2(\eta(n)), i_1^2(\eta(n)))$, dove i_0^2 e i_1^2 sono le funzioni che danno rispettivamente il primo e il secondo elemento di una 2-pla. Dimostriamo per induzione su ω il seguente lemma:

$$i_1^2(\eta(n)) = n.$$

Vale infatti $i_1^2(\eta(0)) = i_1^2(k,0) = 0$. Supponiamo che l'asserto valga per n, abbiamo allora, ricordando che $\sigma^{\mathcal{A}} = \sigma$,

$$\begin{aligned} i_1^2(\eta(\sigma(n)) &= i_1^2(\sigma^{\mathcal{D}}(\eta(n)) \\ &= i_1^2(\sigma^{\mathcal{D}}(i_0^2(\eta(n)), i_1^2(\eta(n))) \\ &= i_1^2(\psi(i_0^2(\eta(n)), i_1^2(\eta(n))), \sigma(i_1^2(\eta(n)))) \\ &= \sigma(i_1^2(\eta(n))) \\ &= \sigma(n). \end{aligned}$$

A questo punto possiamo definire $\varphi = i_0^2 \circ \eta$. Verifichiamo che φ soddisfa le condizioni poste dal teorema. Innanzitutto

$$\varphi(0) = i_0^2(\eta(0)) = i_0^2(c,0) = c.$$

Inoltre abbiamo

$$\begin{aligned}
\varphi(\sigma(n)) &= i_0^2(\eta(\sigma(n))) \\
&= i_0^2(\sigma^{\mathcal{D}}(\eta(n))) \\
&= i_0^2(\sigma^{\mathcal{D}}(i_0^2(\eta(n)), i_1^2(\eta(n)))) \\
&= i_0^2(\psi(i_0^2(\eta(n)), i_1^2(\eta(n))), \sigma(i_1^2(\eta(n)))) \\
&= \psi(i_0^2(\eta(n)), i_1^2(\eta(n))) \\
&= \psi(i_0^2(\eta(n)), n) \\
&= \psi(\varphi(n), n),
\end{aligned}$$

dove la penultima equazione si ottiene per il lemma e l'ultima per la definizione di φ.

Corollario 2.6.3 *Per ogni $\theta : C \to C$ e $\psi : C \times \omega \times C \to C$, esiste una funzione $\varphi : \omega \times C \to C$ tale che, per ogni $c \in C$,*

$$\varphi(0, c) = \theta(c) \quad e \quad \varphi(\sigma(n), c) = \psi(\varphi(n, c), n, c).$$

Diremo che φ è definita per recursione primitiva da θ e ψ.

Fissiamo un elemento qualsiasi $c \in C$ e con esso parametrizziamo l'ultimo argomento di ψ ottenendo una funzione $\psi_c : C \times \omega \to C$ tale che, per ogni $x \in C$ e ogni $n \in \omega$, $\psi_c(x, n) = \psi(x, n, c)$. Se siamo in grado di definire una funzione $\varphi_c : \omega \to C$ tale che

$$\varphi_c(0) = \theta(c) \quad \text{e} \quad \varphi_c(\sigma(n)) = \psi_c(\varphi_c(n), n),$$

allora possiamo dimostrare, per induzione su ω, che $\varphi_c(n) = \varphi(n, c)$ e quindi possiamo usare quest'ultima equazione per definire, al variare di $c \in C$, la φ richiesta dal teorema. Ma l'esistenza di φ_c si ottiene immediatamente dal teorema precedente.

Siamo ora in grado di giustificare la seguente definizione ricorsiva della funzione somma:

$$+(0, m) = m \quad \text{e} \quad +(\sigma(n), m) = \sigma(+(n, m)).$$

È sufficiente identificare la θ del corollario con l'identità i_0^1 e la ψ con $\sigma \circ i_0^3$. Lasciamo al lettore come esercizio la giustificazione della definizione della funzione prodotto,

$$\cdot(0, m) = 0 \quad \text{e} \quad \cdot(\sigma(n), m) = +(\cdot(n, m), m)$$

assumendo data la funzione somma, e della funzione fattoriale

$$!(0) = 1 \quad \text{e} \quad !(\sigma(n) = \cdot(!(n), \sigma(n))$$

assumendo data la funzione prodotto.

Esercizio 2.6.1 Si dimostri che se $\mathcal{A}$ è generata liberamente, allora ogni elemento ha un'unica costruzione.

2.7 Il lemma di Zorn

Gli insiemi parzialmente ordinati sono strutture molto diffuse ed è spesso importante stabilire se un dato insieme parzialmente ordinato contenga (almeno) un elemento massimale. Il lemma di Zorn stablisce una condizione molto generale perché un insieme parzialmente ordinato non vuoto $\mathcal{A} = (A, \leq)$ contenga elementi massimali: è sufficiente che, per ogni catena $K \subseteq A$, valga $\sup K \in A$. La condizione si può anche indebolire a: A contiene un confine superiore, non necessariamente $\sup K$, per ogni catena K. (Si veda l'esercizio 2.7.1.) Il lemma di Zorn è un esempio di matematica non costruttiva, poiché stabilisce l'esistenza di un oggetto, l'elemento massimale, senza che dalla dimostrazione si possano ricavare informazioni per identificarlo. In effetti il lemma di Zorn è dimostrato sulla base dell'assioma di scelta della teoria degli insiemi (a cui risulta addirittura equivalente): tale assioma stabilisce che, per ogni insieme A, esiste una *funzione di scelta* $\varphi : \mathcal{P}(A) - \{\emptyset\} \to A$ che sceglie un elemento da ogni sottoinsieme non vuoto di A, ossia tale che, per ogni $X \subseteq A$ non vuoto, $\varphi(X) \in X$. L'assioma di scelta fu al centro di molte discussioni nei primi decenni del XX secolo, quando diversi matematici ne sottolinearono il carattere altamente non costruttivo: quando X era infinito, si poteva asserire l'esistenza di una funzione di scelta senza fornire un criterio per compiere le scelte? In seguito l'assioma fu accettato da gran parte dei matematici, anche perché si dimostrò insostituibile nella dimostrazione di alcuni importanti risultati tra cui citiamo soltanto, oltre al lemma di Zorn, il teorema del buon ordinamento: ogni insieme può essere bene ordinato.

Diremo che una funzione $f : A \to A$ ha un *punto fisso* se esiste un $a \in A$ tale che $f(a) = a$ ed è *progressiva* se, per ogni $a \in A$, $a \leq f(a)$. Definiamo *cpo* (da *complete partially ordered set*) una struttura $\mathcal{A} = (A, \leq, 0)$ costituita da un insieme parzialmente ordinato dotato di minimo 0 e tale che, per ogni catena $K \subseteq A$, $\sup K \in A$. (Ricordiamo che una catena è un insieme totalmente ordinato.) Otterremo il lemma di Zorn come corollario del seguente teorema riguardante l'esistenza di punti fissi per funzioni progressive definite su cpo.

Teorema 2.7.1 *Se $\mathcal{A}$ è un cpo e $f : A \to A$ è progressiva, allora f ha un punto fisso.*

Diremo che un insieme $X \subseteq A$ è f-chiuso se

i) $0 \in X$,

ii) $f[X] \subseteq X$,

iii) per ogni catena $K \subseteq X$, $\sup K \in X$.

In altri termini, X è f-chiuso se è un sotto-cpo di $\mathcal{A}$ chiuso rispetto a f. In analogia a quanto abbiamo visto a proposito delle definizioni induttive, diremo che l'insieme

$$Z = \bigcap \{X \subseteq A : X \text{ è } f\text{-chiuso}\}$$

è definito induttivamente da f in $\mathcal{A}$. È facile verificare che Z stesso è f-chiuso e quindi è il minimo f-chiuso incluso in A. Ogni volta che vorremo dimostrare che una data proprietà $P \subseteq A$ è goduta da ogni elemento di Z, basterà dimostrare che P è f-chiuso, perché in tal caso vale $Z \subseteq P$. Se la proprietà sarà tale che $P \subseteq Z$, avremo allora $Z = P$. In particolare dimostreremo che Z è una catena. Supponiamo per il momento di averlo dimostrato: poiché Z soddisfa la condizione iii) ed è una catena, $\sup Z \in Z$, poiché Z soddisfa la condizione ii), $f(\sup Z) \in Z$ e per la definizione di minimo confine superiore $f(\sup Z) \leq \sup Z$. D'altra parte f è progressiva, quindi $\sup Z \leq f(\sup Z)$. In conclusione, $\sup Z$ è un punto fisso di f.

Resta da dimostrare che Z è una catena ossia che, per ogni x, $y \in Z$, vale $x \leq y$ o $y \leq x$. Poiché f è progressiva, basterà dimostrare che $f(x) \leq y$ o $y \leq x$. Per ogni elemento $x \in Z$ definiamo l'insieme

$$C_x = \{y \in Z : x \leq y \text{ o } y \leq x\}$$

degli elementi confrontabili con x e l'insieme

$$Z_x = \{y \in Z : f(x) \leq y \text{ o } y \leq x\}.$$

Poiché f è progressiva, $Z_x \subseteq C_x$. Dimostreremo che $Z_x = Z$, per ogni $x \in Z$, e quindi $Z \subseteq C_x$. Da ciò si ottiene immediatamente che ogni elemento di Z è confrontabile con x, per ogni $x \in Z$, e quindi Z risulta essere una catena. Definiamo allora

$$C = \{x \in Z : \text{per ogni } y \in Z,\ y < x \text{ implica } f(y) \leq x\}$$

e dimostriamo in un primo tempo che $Z_x = Z$ quando $x \in C$. In seguito dimostreremo che $C = Z$.

Assumiamo quindi $x \in C$. Per dimostrare che $Z_x = Z$ basterà dimostrare che Z_x è f-chiuso. i) Vale $0 \in Z_x$, infatti $f(x) \leq 0$ o $0 \leq x$. ii) Assumiamo $y \in Z_x$ ossia $f(x) \leq y$ o $y \leq x$, e dimostriamo che $f(y) \in Z_x$, ossia $f(x) \leq f(y)$ o $f(y) \leq x$. Caso a): $f(x) \leq y$. Allora $f(x) \leq f(y)$, poiché f è progressiva. Caso b): $y = x$. Allora $f(x) \leq f(y)$. Caso c): $y < x$. In questo caso sfruttiamo l'ipotesi $x \in C$, da cui scende $f(y) \leq x$. iii) Sia K una catena tale che $K \subseteq Z_x$, allora per ogni $k \in K$ vale $f(x) \leq k$ o $k \leq x$. Dobbiamo dimostrare che $\sup K \in Z_x$, ossia $f(x) \leq \sup k$ o $\sup K \leq x$. Caso a): per ogni $k \in K$ vale $k \leq x$, allora $\sup K \leq x$. Caso b): esiste $k \in K$ tale che $f(x) \leq k$, allora $f(x) \leq \sup K$.

Resta dunque da dimostrare che $C = Z$ e ancora una volta, sfruttando il fatto che Z è definito induttivamente da f, basterà dimostrare che C è f-chiuso. i) Vale $0 \in C$ dato che, per ogni $y \in Z$, è banalmente vero che $y < 0$ implica $f(y) \leq 0$. ($y < 0$ è sempre falsa.) ii) Supponiamo $w \in C$, ossia che per ogni $y \in Z$, $y < w$ implichi $f(y) \leq w$. Dobbiamo dimostrare che $f(w) \in C$, ossia che, per ogni $y \in Z$, $y < f(w)$ implica $f(y) \leq f(w)$. Assumiamo dunque $y < f(w)$. Per quanto abbiamo dimostrato in precedenza, sappiamo che se $w \in C$, allora $Z_w = Z$, ossia per ogni $y \in Z$, $f(w) \leq y$ o $y \leq w$. La nostra ipotesi $y < f(w)$

è incompatibile con $f(w) \leq y$ (poiché ne verrebbe $y < y$), quindi deve valere l'altra alternativa: $y \leq w$. Caso a): $y = w$, allora $f(y) \leq f(w)$. Caso b): $y < w$. Poiché per ipotesi $w \in C$, abbiamo $f(y) \leq f(w)$. iii) Sia K una catena tale che $K \subseteq C$. Dobbiamo dimostrare che $\sup K \in C$, ossia per ogni $y \in Z$, $y < \sup K$ implica $f(y) \leq \sup K$. Fissiamo dunque $y \in Z$ tale che $y < \sup K$. Per quanto abbiamo dimostrato in precedenza sappiamo che se $x \in C$ allora $Z_x = Z$. Poiché ogni elemento di K è in C, per ogni $k \in K$ vale $Z_k = Z$ e quindi in particolare per y vale, per ogni $k \in K$, $f(k) \leq y$ o $y \leq k$. D'altra parte non può verificarsi $f(k) \leq y$ per ogni $k \in K$, altrimenti avremmo anche $k \leq y$ per ogni $k \in K$ e quindi $\sup K \leq y$, contro l'ipotesi $y < \sup K$. Deve quindi esistere un $k \in K$ tale che $y \leq k$. Caso a): $y = k$. Poiché $y < \sup K$, esisterà un $k' \in K$ tale che $k < k'$ (altrimenti, essendo K una catena, avremmo $\sup K = k = y$). Poiché $k' \in C$, da $y < k'$ ricaviamo $f(y) \leq k' \leq \sup K$. Caso b): $y < k$. Poiché $k \in C$ abbiamo $f(y) \leq k$ e quindi $f(y) \leq \sup K$.

Teorema 2.7.2 *Se $(A, \leq)$ è parzialmente ordinato non vuoto e per ogni catena $K \subseteq A$ vale $\sup K \in A$, allora ogni funzione progressiva $f : A \to A$ possiede un punto fisso.*

Fissiamo un elemento $a \in A$ e consideriamo $B = \{x \in A : a \leq x\}$. È immediato verificare che la struttura $(B, \leq, a)$, ottenuta restringendo a B la relazione d'ordine parziale definita su A, è un cpo. Definiamo ora una funzione $g : B \to B$ ponendo, per ogni $b \in B$, $g(b) = f(b)$. (Ciò è possibile perché f è progressiva e quindi $f(b) \in B$.) Evidentemente g è progressiva anch'essa e, per il teorema precedente, possiede un punto fisso in B che sarà anche punto fisso di f.

Corollario 2.7.3 (Zorn) *Se $(A, \leq)$ è parzialmente ordinato non vuoto e per ogni catena $K \subseteq A$ vale $\sup K \in A$, allora A contiene un elemento massimale.*

Se A non contiene un massimale, allora per l'assioma di scelta possiamo definire nel modo seguente una funzione $f : A \to A$ tale che, per ogni $a \in A$, $a < f(a)$. Per ogni $a \in A$ consideriamo l'insieme $X_a = \{x \in A : a < x\}$: se non ci sono massimali X_a è sempre diverso dal vuoto. Se φ è una funzione di scelta che associa ad ogni sottoinsieme di A non vuoto un suo elemento, possiamo definire $f(a) = \varphi(X_a)$, per ogni $a \in A$. Chiaramente vale $a < f(a)$, ma per il teorema precedente, essendo f progressiva, f deve avere un punto fisso, il che è assurdo.

Esercizio 2.7.1

1. Si dimostri che ogni insieme parzialmente ordinato $(A, \leq)$ contiene una catena massimale. (Si consideri l'insieme $(B, \subseteq)$ di tutte le catene in $(A, \leq)$ e si dimostri che per esso valgono le ipotesi del lemma di Zorn.)

2. Si dimostri la seguente versione del lemma di Zorn: se $(A, \leq)$ è un insieme parzialmente ordinato tale che, per ogni catena $K \subseteq A$, A contiene un

confine superiore di K, allora A contiene un elemento massimale. (Si consideri una catena massimale M in A, che esiste per il punto precedente, e si dimostri che ogni confine superiore di tale catena è un elemento massimale di A.)

Capitolo 3

Logica enunciativa

3.1 Linguaggio enunciativo

La logica può essere definita come la teoria dell'inferenza corretta. Un'inferenza è costituita da un insieme di enunciati detti premesse o assunzioni e da un enunciato detto conclusione. In un'inferenza corretta premesse e conclusione sono unite dal legame di conseguenza logica: in ogni circostanza in cui accettiamo le premesse, ci sentiamo costretti ad accettare inevitabilmente anche la conclusione. La logica non si limita a raccogliere e catalogare le inferenze che sono considerate corrette, ma fornisce soprattutto un'analisi del legame di conseguenza logica, poiché è l'esistenza di questo legame ciò che permette di riconoscere un'inferenza corretta. Per definire il concetto di conseguenza logica occorre stabilire la semantica del linguaggio, ossia bisogna definire in cosa consista il significato di un enunciato e come il significato venga attribuito agli enunciati. Sebbene il significato sia l'elemento decisivo e si possa ritenere accidentale la sua espressione linguistica, che può avvenire in modi diversi in linguaggi diversi o anche nello stesso linguaggio, inizieremo il nostro studio proprio dal linguaggio. Quale che sia il mondo dei significati, esso compare nell'inferenza inevitabilmente attraverso la mediazione del linguaggio: solo ciò che viene rappresentato nel linguaggio può essere rilevante per l'inferenza.

Immaginiamo di isolare cinque modi fondamentali di connettere enunciati del linguaggio naturale per formare enunciati più complessi: "non", "e", "o", "se ... allora", "se e solo se". Ciascuno di essi può essere considerato come un'operazione avente enunciati come argomenti e valori: operando con "non" su "Antonio ama Maria" otteniamo l'enunciato "Antonio non ama Maria", operando con "se ... allora" su "Antonio ama Maria" e su "Antonio ama Sara" otteniamo "Se Antonio ama Maria allora Antonio ama Sara", e così via. Naturalmente ci sono nella nostra lingua altri modi di connettere enunciati fra di loro, ma vedremo in seguito che quelli individuati sono più che sufficienti per il discorso logico. Poiché sappiamo come costruire enunciati complessi a partire da enunciati più semplici, siamo anche in grado di analizzare enunciati com-

plessi nei loro componenti. Questo processo di analisi si può spingere fino a un certo punto oltre il quale non può continuare, e precisamente fino a quando si incontra un enunciato che non è né una negazione, né una congiunzione, né una disgiunzione, né una implicazione, né una equivalenza: tali enunciati sono detti elementari. La logica enunciativa è caratterizzata dal fatto che il potere di risoluzione del suo linguaggio non va oltre gli enunciati elementari. Spetterà alla logica predicativa il compito di approfondire il livello dell'analisi valendosi di un linguaggio che estende quello enunciativo e mette in gioco anche la costituzione interna degli enunciati elementari. L'introduzione di questi due livelli di analisi logica, nell'ordine in cui vengono presentati, non rispecchia lo sviluppo storico della logica, che ha seguito invece l'ordine inverso, ma assolve semplicemente una funzione didattica. Iniziamo dalla logica enunciativa perché è più semplice della logica predicativa, pur presentando la stessa architettura complessiva: un linguaggio formale, una semantica, un calcolo logico e un teorema di completezza.

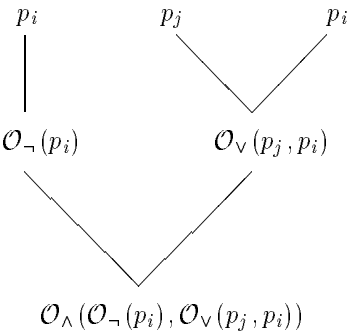
Il primo passo nella costruzione della logica enunciativa consiste nella definizione del linguaggio formale nel quale sarà possibile tradurre gli enunciati del linguaggio naturale. I modi di connettere enunciati che abbiamo isolato, "non", "e", "o", "se ... allora", "se e solo se" sono rappresentati nei linguaggi formali dai simboli $\neg$, $\wedge$, $\vee$, $\rightarrow$ e $\leftrightarrow$, detti *connettivi logici* e denominati rispettivamente negazione, congiunzione, disgiunzione, implicazione, equivalenza. Nel linguaggio formale che adotteremo ci limiteremo all'insieme di connettivi $C = \{\neg, \wedge, \vee\}$ e in seguito dimostreremo che ciò non comporta nessuna limitazione delle nostre facoltà espressive. Definiamo quindi *linguaggio enunciativo* l'insieme $\mathcal{L} = C \cup P$, dove $P = \{p_i : i \in \omega\}$ è un insieme di simboli detti *variabili enunciative*. Linguaggi enunciativi diversi possono essere ottenuti variando C e P. Talvolta ci si riferisce più correttamente a $\mathcal{L}$ come all'alfabeto del linguaggio, e si riserva il nome di linguaggio per l'insieme delle formule scritte con i simboli di $\mathcal{L}$, che intuitivamente corrispondono alle parole o agli enunciati dei linguaggi naturali: questo abuso di linguaggio è frequente quanto innocuo, dato che nei linguaggi formali l'insieme delle formule è univocamente determinato dall'alfabeto.

L'insieme delle formule di $\mathcal{L}$ è un insieme definito induttivamente, occorre quindi stabilire la struttura entro cui si realizza la definizione induttiva. Sia E l'insieme di tutte le successioni finite di elementi di $\mathcal{L}$: gli elementi di E sono detti *espressioni* di $\mathcal{L}$. In corripondenza dei connettivi $\neg$, $\wedge$ e $\vee$ definiamo su E tre funzioni $\mathcal{O}_\neg$, $\mathcal{O}_\wedge$ e $\mathcal{O}_\vee$ nel modo seguente:

$$\begin{aligned} \mathcal{O}_\neg(e) &= (\neg) * e, \\ \mathcal{O}_\wedge(e_0, e_1) &= (\wedge) * e_0 * e_1, \\ \mathcal{O}_\vee(e_0, e_1) &= (\vee) * e_0 * e_1. \end{aligned}$$

Consideriamo infine la struttura $\mathcal{E} = (E, \mathcal{O}_\wedge, \mathcal{O}_\vee, \mathcal{O}_\neg)$ e la definizione induttiva $(B, \mathcal{F})$, dove $B = P$ e $\mathcal{F} = \{\mathcal{O}_\wedge, \mathcal{O}_\vee, \mathcal{O}_\neg\}$. Gli elementi dell'insieme definito induttivamente $Fm_\mathcal{L}$ sono detti *formule* o *enunciati* di $\mathcal{L}$. Ometteremo l'indice $\mathcal{L}$ quando sia chiaro dal contesto. Per abbreviare scriveremo $s_0 s_1 \ldots s_n$ invece di $(s_0, s_1, \ldots, s_n)$. Saranno quindi formule espressioni come p_i, $\neg p_i$, $\wedge p_i p_j$. Ad

ogni formula è associata una costruzione che la genera, per esempio



è associata a $\wedge\neg p_i \vee p_j p_i$. Vedremo nel paragrafo seguente che le formule sono generate liberamente e quindi tale costruzione è unica. Espressioni come $\neg$, $p_i\neg$, $p_i \vee p_j$ non sono formule perché evidentemente non possono essere prodotte da alcuna costruzione. È chiaro che a ogni nodo di una costruzione è associata una formula: ciascuna di tali formule è detta *sottoformula* della formula associata alla radice.

È tipico di questo linguaggio premettere il connettivo binario invece di interporlo, ottenendo espressioni come $\vee p_i p_j$ invece di $p_i \vee p_j$. Questo modo di procedere, per quanto sembri innaturale, permette di avere un linguaggio senza parentesi. Infatti, mentre la notazione $p_0 \wedge p_1 \vee p_2$ è ambigua, e solo con le parentesi possiamo specificare se intendiamo parlare di $(p_0 \wedge p_1) \vee p_2$ o di $p_0 \wedge (p_1 \vee p_2)$, la notazione fornita dal nostro linguaggio consente di indicare la prima con $\vee \wedge p_0 p_1 p_2$ e la seconda con $\wedge p_0 \vee p_1 p_2$. L'ordine in cui vanno effettuate le operazioni è espresso dalla disposizione dei simboli, senza far uso delle parentesi. Lo scopo dell'eliminazione delle parentesi è quello di ottenere un linguaggio strutturalmente più semplice, anche se meno facilmente decifrabile. D'altra parte possiamo continuare a valerci dei servigi delle parentesi nella rappresentazione delle formule introducendo la seguente convenzione notazionale. Se consideriamo le lettere greche $\alpha, \beta, \gamma, \ldots$ come variabili metalinguistiche per formule, stabiliamo di rappresentare in generale la formula $\wedge\alpha\beta$ mediante la scrittura $(\alpha \wedge \beta)$ e la formula $\vee\alpha\beta$ mediante la scrittura $(\alpha \vee \beta)$.

Esistono linguaggi enunciativi basati su altri connettivi logici: i connettivi più comuni e naturali, oltre a quelli da noi adottati, sono $\rightarrow$ e $\leftrightarrow$, rispettivamente "se...allora...", e "...sse...". Se si vuole sviluppare un linguaggio enunciativo comprendente questi connettivi, basta introdurre tra le funzioni $\mathcal{F}$ della definizione induttiva delle formule anche le operazioni $\mathcal{O}_\rightarrow$ e $\mathcal{O}_\leftrightarrow$ definite in modo analogo alle precedenti. La scelta di limitarsi a $\neg$, $\wedge$, e $\vee$ ha una duplice giustificazione. In primo luogo è possibile dimostrare (si veda il teorema 3.4.8) che limitandoci a loro non ci siamo privati di nulla, nel senso che il nostro linguaggio enunciativo possiede già il massimo di espressività possibile. In secondo luogo, l'adozione di questi connettivi facilita l'individuazione del rapporto che esiste tra la semantica

del linguaggio enunciativo e le algebre di Boole. Un altro criterio frequentemente adottato è quello di minimizzare il numero dei connettivi, in modo da ridurre il numero dei casi da esaminare nelle dimostrazioni per induzione sulle formule: in questo caso la scelta più comune è quella di limitarsi a $\neg$, $\vee$ oppure a $\neg$, $\rightarrow$. D'altra parte, come nel caso delle parentesi, non vogliamo privarci dei servigi dei connettivi che abbiamo tralasciato, quindi li introduciamo con una convenzione notazionale, stabilendo di scrivere $(\alpha \rightarrow \beta)$ al posto di $(\neg\alpha \vee \beta)$ e $(\alpha \leftrightarrow \beta)$ al posto di $((\alpha \rightarrow \beta) \wedge (\beta \rightarrow \alpha))$. Il senso di questa convenzione risulterà chiaro quando stabiliremo il significato dei connettivi. Per ora ci limitiamo a considerare la scrittura $(p_0 \rightarrow p_1)$ come un'abbreviazione per $\neg p_0 \vee p_1$ che a sua volta rende più leggibile $\neg \vee p_0 p_1$. Solo quest'ultima è veramente una formula del nostro linguaggio.

Ora che abbiamo introdotto le parentesi per facilitare la lettura delle formule, fissiamo alcune convenzioni che permettono in alcuni casi di eliminarle, dato che un eccesso di parentesi disturba la lettura quanto la loro mancanza totale. Innanzitutto eliminiamo la coppia di parentesi più esterna convenendo di scrivere, ad esempio, $(\alpha \vee \beta) \wedge \gamma$ invece di $((\alpha \vee \beta) \wedge \gamma)$. Stabiliamo quindi un ordine di precedenza nell'applicazione dei connettivi, chiedendo che

1. $\neg$ si applichi prima di ogni altro connettivo,

2. $\wedge$ e $\vee$ si applichino prima di $\rightarrow$ e $\leftrightarrow$, senza però stabilire un ordine di precedenza fra $\wedge$ e $\vee$ e fra $\rightarrow$ e $\leftrightarrow$,

3. in una formula del tipo di $\alpha_0 \rightarrow \ldots \rightarrow \alpha_n$ le parentesi siano associate a destra e che una convenzione analoga valga per ogni altro connettivo binario.

Avremo quindi la possibilità di semplificare $(\neg\alpha) \vee (\beta \vee \gamma)$ in $\neg\alpha \vee \beta \vee \gamma$ (per le 1 e 3), mentre $\neg(\alpha \vee \beta) \vee \gamma$ non è ulteriormente semplificabile. Analogamente $(\alpha \wedge \beta) \rightarrow (\gamma \rightarrow \delta)$ si riduce a $\alpha \wedge \beta \rightarrow \gamma \rightarrow \delta$ (per le 2 e 3), mentre $((\alpha \wedge \beta) \rightarrow \gamma) \rightarrow \delta$ si riduce solo a $(\alpha \wedge \beta \rightarrow \gamma) \rightarrow \delta$ (per la 2) e la formula $((\alpha \rightarrow \beta) \rightarrow \gamma) \rightarrow \gamma$ non si riduce affatto. La formula $(\alpha \wedge \beta) \vee (\gamma \wedge \delta)$ non si riduce, perché tra $\wedge$ e $\vee$ non sono fissate regole di precedenza. Poiché eliminare le parentesi è una facoltà e non un obbligo, a volte non elimineremo tutte le parentesi eliminabili in base a queste convenzioni.

Siamo ora in grado di stabilire un rapporto tra il linguaggio naturale e il linguaggio enunciativo: ad ogni enunciato elementare del linguaggio naturale associamo una variabile p_i, a enunciati diversi variabili diverse, e alle operazioni "non", "e", "o", "se ... allora", "se e solo se" associamo ordinatamente i connettivi $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$. Ad esempio, l'enunciato complesso "Se Antonio non ama Maria, allora Antonio tradisce Sara o Antonio tradisce Maria", associando "Antonio ama Maria" a p_0, Antonio tradisce Sara" a p_1 e "Antonio tradisce Maria" a p_2, diventa $\neg p_0 \rightarrow (p_1 \vee p_2)$. A prima vista sembra di aver ottenuto solo una stenografia, una rappresentazione simbolica molto semplificata del linguaggio naturale. Si osservi, tuttavia, che nel passaggio dall'enunciato del linguaggio naturale "Se Antonio non ama Maria, allora Antonio tradisce Sara o Antonio

tradisce Maria" alla formula $\neg p_0 \rightarrow (p_1 \vee p_2)$ c'è una perdita di specificità: il primo parla di Antonio, di Maria, di amore e tradimento, la seconda fa lo stesso discorso del primo *solo* tenendo presente la corrispondenza tra enunciati elementari e variabili di P, corrispondenza che non risulta in alcun modo dalla formula. Sarebbe ingiusto dire che la formula non parla di nulla solo perché p_0, p_1 e p_2 sono variabili, e quindi non ha un significato determinato: la formula non fa nessuna asserzione puntuale, ma esibisce un tipo di rapporto di natura logica tra enunciati, è la *forma* da cui si possono ricavare infiniti enunciati del linguaggio naturale facendo variare in tutti i modi possibili la corrispondenza tra enunciati elementari e P.

La situazione risulta più chiara se partiamo dal linguaggio enunciativo. Fissata una corrispondenza tra variabili di P ed enunciati elementari del linguaggio naturale, vediamo che ogni formula si traduce in un enunciato del linguaggio naturale semplicemente cambiando p_i con l'enunciato elementare corrispondente e rimpiazzando i connettivi logici con "non", "e", "o", "se ... allora" e "se e solo se". Variando la corrispondenza otterremo infinite traduzioni di $\neg p_0 \rightarrow (p_1 \vee p_2)$ nel linguaggio naturale e nell'insieme di tutte le possibili traduzioni troveremo anche "Se Antonio non ama Maria, allora Antonio tradisce Sara o Antonio tradisce Maria": in generale si tratterà di enunciati del tipo di

se non ... allora ... o ... .

In conclusione possiamo dire che nel passaggio dal linguaggio naturale al linguaggio formale della logica enunciativa otteniamo una formula che costituisce la forma logica dell'enunciato del linguaggio naturale. Da questa forma logica possiamo riottenere l'enunciato di partenza tenendo presente la corrispondenza fissata all'inizio della traduzione tra enunciati elementari e P, ma facendo variare questa corrispondenza possiamo ottenere un'infinità di enunciati del linguaggio naturale che condividono la forma logica dell'enunciato di partenza.

Esercizio 3.1.1 Se p_0 denota l'enunciato "Bruno va al cinema", p_1 denota "la sera è fredda" e p_2 denota "I bar sono chiusi", si rappresentino con formule gli enunciati seguenti:

1. Se Bruno va al cinema allora o la sera è fredda o i bar sono chiusi

2. Se Bruno va al cinema e i bar non sono chiusi, allora la sera è fredda

3. O Bruno va al cinema e i bar sono chiusi, oppure la sera è fredda.

Esercizio 3.1.2 In ognuno dei seguenti enunciati si individuino gli enunciati elementari, assegnando a ciascuno una variabile p_i in modo che a enunciati elementari diversi corrispondano variabili diverse. Si traducano quindi gli enunciati in formule.

1. Anna è giovane e Bruno è vecchio

2. Bruno è vecchio ma è attivo

3. Anna e Bruno sono amici

4. Anna e Bruno non sono felici

5. Anna o Bruno vengono bocciati

6. Anna sostiene l'esame giovedì o venerdì

7. Anna va al cinema ammesso che piova e Bruno non sia a Torino

8. Anna va al cinema solo se piove

9. Quando Anna ha sete e non c'è the, ma solo allora, beve vodka

10. Questo esercizio non è né utile né divertente.

Esercizio 3.1.3 Si verifichi che le espressioni ai punti 2 e 4 sono formule esibendo la loro costruzione, si verifichi che quelle ai punti 1 e 3 non sono formule mostrando che non possiedono una costruzione.

1. $\wedge p_0 p_1 \vee p_0 p_1$,

2. $\vee \wedge p_0 p_1 \vee p_0 p_1$,

3. $\neg \vee p_0 p_1 p_2$,

4. $\neg \wedge \vee p_0 p_1 \neg p_2$.

3.2 Induzione e recursione sulle formule

Il fatto che l'insieme delle formule Fm sia definito induttivamente rende lecito dimostrare proprietà di formule per *induzione sulle formule*. Vale a dire, se Q è una proprietà di formule, per dimostrare che ogni formula gode di Q basta dimostrare che:

1. per ogni variabile p_i, vale $Q(p_i)$,

2. per ogni formula α, se $Q(\alpha)$ allora $Q(\neg\alpha)$,

3. per ogni coppia di formule α, β, se $Q(\alpha)$ e $Q(\beta)$ allora $Q(\alpha \wedge \beta)$ e $Q(\alpha \vee \beta)$.

La giustificazione di questo principio induttivo è data dal teorema 2.5.1, tenendo presente che $Fm = I_{B,\mathcal{F}}$ e che le clausole 1)-3) precedenti equivalgono ad asserire che Q è $B, \mathcal{F}$-chiusa.

Talvolta è necessario utilizzare altri principi induttivi, basati sull'assegnamento di una funzione $\varphi : Fm \to \omega$ che esprime una misura di complessità delle formule. Diremo che una formula α è Q, φ-completa se, per ogni formula β, $\varphi(\beta) < \varphi(\alpha)$ implica $Q(\beta)$. Diremo che la proprietà Q è φ-progressiva se, per ogni formula α, se α è Q, φ-completa allora $Q(\alpha)$, in altri termini, se vale $Q(\alpha)$ quando Q vale per tutte le formule di complessità minore di α. Dal teorema

2.5.4 si ricava il seguente principio induttivo: per dimostrare che ogni formula gode di Q basta dimostrare che Q è φ-progressiva. Le misure di complessità più utilizzate sono quelle in cui $\varphi(\alpha)$ rappresenta l'altezza della costruzione di α (vedremo tra breve che ogni formula ha un'unica costruzione), oppure $\varphi(\alpha)$ rappresenta la lunghezza di α, ossia il numero dei simboli che la compongono. Parleremo allora di *induzione sull'altezza* o di *induzione sulla lunghezza* di α.

Nel seguito ci accadrà spesso di definire per recursione funzioni dall'insieme delle formule verso altri insiemi. Ad esempio, la lunghezza di una formula è definita per recursione nel modo seguente:

1. $l(p_i) = 1$
2. $l(\neg\alpha) = l(\alpha) + 1$
3. $l(\alpha \wedge \beta) = l(\alpha \vee \beta) = l(\alpha) + l(\beta) + 1$.

Definire una funzione per recursione sulle formule significa applicare il teorema 2.6.1 che a sua volta può essere applicato solo se le formule costituiscono una struttura generata liberamente da P. Consideriamo la struttura $\mathcal{FM} = (Fm, \mathcal{O}_\wedge, \mathcal{O}_\vee, \mathcal{O}_\neg)$ detta *algebra delle formule* di $\mathcal{L}$. È chiaro che $\mathcal{FM}$ è generata da P, per dimostrare che è generata liberamente basta verificare che soddisfa le condizioni 1)-6) del paragrafo 2.6, che è quanto stabilisce il teorema seguente.

Teorema 3.2.1

1. $Im(\mathcal{O}_\neg) \cap P = \emptyset$, $Im(\mathcal{O}_\wedge) \cap P = \emptyset$ *e* $Im(\mathcal{O}_\vee) \cap P = \emptyset$,
2. $Im(\mathcal{O}_\neg) \cap Im(\mathcal{O}_\wedge) = \emptyset$, $Im(\mathcal{O}_\neg) \cap Im(\mathcal{O}_\vee) = \emptyset$, $Im(\mathcal{O}_\wedge) \cap Im(\mathcal{O}_\vee) = \emptyset$,
3. $\mathcal{O}_\neg$, $\mathcal{O}_\wedge$ *e* $\mathcal{O}_\vee$ *ristrette a* Fm, *sono iniettive.*

I primi due punti sono evidenti. Quanto al terzo punto, si vede facilmente che $\mathcal{O}_\neg$ è iniettiva, dato che $\neg\alpha = \neg\beta$ implica $\alpha = \beta$. L'iniettività di $\mathcal{O}_\wedge$ non è altrettanto semplice da dimostrare. (Quella di $\mathcal{O}_\vee$ si dimostra nello stesso modo.) Date le formule α, β, γ, δ, da $\wedge\alpha\beta = \wedge\gamma\delta$ si ricava solo $\alpha\beta = \gamma\delta$: come si può arrivare ad $\alpha = \gamma$ e $\beta = \delta$? Ora, se pensiamo ad $\alpha\beta$ e $\gamma\delta$ come a espressioni, successioni finite di simboli, da $\alpha\beta = \gamma\delta$ si ricava che $\alpha = \gamma$, oppure α è un segmento iniziale proprio di γ oppure γ è un segmento iniziale proprio di α. Se riusciamo a dimostrare che né α può essere segmento iniziale proprio di γ, né γ di α, allora deve essere necessariamente $\alpha = \gamma$. A questo punto da $\alpha\beta = \gamma\delta$ si può ricavare $\beta = \delta$ e l'iniettività della funzione $\mathcal{O}_\wedge$ è dimostrata. Resta allora da dimostrare il seguente lemma:

Per ogni formula di $\mathcal{L}$, *nessun suo segmento iniziale proprio è ancora una formula di* $\mathcal{L}$.

Definiamo una funzione K' che assegna ad ogni simbolo di $\mathcal{L}$ un numero intero in Z ponendo $K'(\neg) = 0$, $K'(\wedge) = K'(\vee) = -1$ e $K'(p_i) = 1$ per ogni

$i \in \omega$. Sulla base di K', definiamo una funzione $K : E \to Z$ come segue. Per ogni espressione $s_0, \ldots, s_{n-1}$, dove $s_i \in \mathcal{L}$ per ogni $i < n$, poniamo

$$K(s_0, \ldots, s_{n-1}) = K'(s_0) + \ldots + K'(s_{n-1}).$$

Si dimostra facilmente per induzione che, per ogni formula α, $K(\alpha) = 1$. Se $\alpha = p_i$, allora

$$K(p_i) = K'(p_i) = 1.$$

Se $\alpha = \neg\beta$, allora per ipotesi induttiva $K(\beta) = 1$ e quindi

$$K(\neg\beta) = K'(\neg) + K(\beta) = 1.$$

Se $\alpha = \wedge\beta\gamma$, allora per ipotesi induttiva $K(\beta) = K(\gamma) = 1$ e quindi

$$K(\wedge\beta\gamma) = K'(\wedge) + K(\beta) + K(\gamma) = 1.$$

Nello stesso modo si procede con $\alpha = \vee\beta\gamma$. A questo punto possiamo dimostrare che, per ogni formula α, se α' è un suo segmento iniziale proprio, $K(\alpha') < 1$. Procediamo anche qui per induzione. Se $\alpha = p_i$ l'asserto è vero a vuoto, perché non vi sono segmenti iniziali propri. Supponiamo che sia $\alpha = \neg\beta$. Allora $\alpha' = \neg$ oppure $\alpha' = \neg\beta'$, dove β' è un segmento iniziale proprio di β. Nel primo caso $K'(\alpha') = 0$ mentre nel secondo, poiché per ipotesi induttiva $K(\beta') < 1$, si ha $K(\alpha') = K'(\neg) + K(\beta') < 1$. Nello stesso modo si trattano i casi di $\wedge\beta\gamma$ e di $\vee\beta\gamma$. Abbiamo quindi dimostrato che ogni segmento iniziale proprio di una formula assume in K un valore minore di 1, mentre ogni formula assume valore 1, quindi nessun segmento iniziale di una formula può essere una formula.

3.3 Semantica enunciativa

Seguendo una distinzione dovuta originariamente a Gottlob Frege (1848-1925), chiamiamo senso o intensione di un enunciato il pensiero espresso e significato o estensione di un enunciato il suo valore di verità. I caratteri distintivi della logica classica, rintracciabili chiaramente già nell'opera di Frege, sono l'estensionalità e la bivalenza. L'estensionalità della logica stabilisce che nella valutazione della correttezza di un'inferenza, sia rilevante solo il significato degli enunciati, cioè il valore di verità. La bivalenza stabilisce che i possibili significati degli enunciati sono solo due, il vero e il falso. D'ora in poi identificheremo i due valori di verità della logica classica rispettivamente con 1 e 0, quindi l'insieme dei valori di verità sarà $\{0, 1\}$, ossia 2.

L'esclusione dalla semantica dell'intensione degli enunciati è un'assunzione di portata molto vasta e dal carattere evidentemente riduttivo. L'identificazione del significato col valore di verità comporta che due enunciati come "7 è maggiore di 5" e "Socrate è mortale" abbiano lo stesso significato, vale a dire denotino lo stesso oggetto: 1. Non ha alcuna importanza che il primo esprima un pensiero che riguarda i numeri e il secondo un pensiero riguardante certi esseri umani,

perché nell'analisi delle inferenze conta solo il significato e gli unici significati possibili sono 0 e 1. Vedremo in seguito che, pur rimanendo nell'ambito di una logica estensionale, è possibile recuperare la differenza tra i due enunciati utilizzando l'analisi logica più raffinata fornita dalla logica predicativa, ma al livello di analisi logica a cui ci muoviamo ora i significati dei due enunciati sono indistinguibili.

A queste due caratteristiche della logica occorre aggiungere un principio fondamentale, identificato sempre da Frege, che regola la semantica del linguaggio enunciativo: la composizionalità del significato. Tenendo presente che il compito degli enunciati è rappresentare nel linguaggio i significati, il principio di composizionalità stabilisce una modalità importante di questa rappresentazione: il significato di un enunciato composto mediante i connettivi è funzione del significato degli enunciati componenti. Questo ci conduce ad associare ad ogni connettivo una *funzione di verità*, ossia una funzione che assume argomenti e valori in 2. Iniziamo dalla funzione di verità associata alla negazione, cioè dalla funzione $f_\neg : 2 \to 2$ tale che

x	$f_\neg(x)$
0	1
1	0

È chiaro che non essendoci altri significati possibili per gli enunciati oltre a 0 e 1, la funzione $f_\neg$, che commuta 0 in 1 e 1 in 0, cattura il significato intuitivo della negazione e permette di calcolare il significato di $\neg\alpha$ noto quello di α.

La funzione di verità $f_\wedge : 2^2 \to 2$ associata alla congiunzione è definita nel modo seguente:

x	y	$f_\wedge(x,y)$
0	0	0
0	1	0
1	0	0
1	1	1

È intuitivo che una congiunzione $\alpha \wedge \beta$ significhi il vero solo quando entrambi i congiunti α e β significano il vero e quindi $f_\wedge$ calcola correttamente il significato di $\alpha \wedge \beta$ da quelli di α e β. Si osservi che l'ordine in cui vengono considerati gli enunciati da congiungere non influenza il risultato, quindi l'operazione $f_\wedge$ risulta essere commutativa.

La funzione di verità $f_\vee : 2^2 \to 2$ associata alla disgiunzione è definita nel modo seguente:

x	y	$f_\vee(x,y)$
0	0	0
0	1	1
1	0	1
1	1	1

Le definizione precedente comporta che una disgiunzione $\alpha \vee \beta$ significhi il vero se almeno uno dei due disgiunti α e β significa il vero e sulla base di questa concezione "inclusiva" della disgiunzione $f_\vee$ calcola in modo intuitivo il significato di $\alpha \vee \beta$, dati i significati di α e β. Naturalmente si potrebbe concepire la disgiunzione in modo tale che le due alternative debbano escludersi a vicenda, come richiede in latino l'uso di *aut*. Se si adotta la disgiunzione in questa accezione "esclusiva" occorre modificare la funzione di verità precedente, ponendo il valore 0 nell'ultima riga. Come vedremo in seguito, non è necessario adottare come primitiva la funzione di verità per la disgiunzione esclusiva, dato che può essere ottenuta dalle altre per composizione. Poiché l'ordine in cui vengono considerati gli enunciati da disgiungere non influenza il significato, anche nel caso della disgiunzione l'operazione $f_\vee$ risulta essere commutativa.

La funzione di verità $f_\to : 2^2 \to 2$ associata all'implicazione è definita nel modo seguente:

x	y	$f_\to(x,y)$
0	0	1
0	1	1
1	0	0
1	1	1

La funzione di verità $f_\to$ è definita in modo tale che $\alpha \to \beta$ risulti falsa quando l'antecedente α dell'implicazione è vero e il conseguente β falso, e vera in tutti i casi restanti. La nozione intuitiva di implicazione non è catturata pienamente da questa funzione di verità. Infatti sembra poco plausibile che un enunciato come "Se $1 = 2$ allora Parigi è in Francia" sia vero, anche se dobbiamo ammetterlo in conseguenza del fatto che $f_\to(0,1) = 1$. Una prima giustificazione della definizione di $f_\to$ si può ottenere esaminando tutte le definizioni possibili. Se si concede che il comportamento di $f_\to$ è corretto nei casi in cui l'antecedente è vero (gli ultimi due), le alternative possibili si riducono alle quattro seguenti:

$$\begin{array}{cccc} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{array}$$

Scegliendo la prima si ottiene $f_\wedge$. Scegliendo la seconda si ottiene una funzione $f(x,y) = y$ in cui il valore è sempre identico al secondo argomento. In tal modo asserire l'implicazione $\alpha \to \beta$ sarebbe equivalente ad asserire β, il che non rende certo il senso intuitivo dell'implicazione. Scegliendo la terza si ottiene la funzione $f_\leftrightarrow$ descritta in seguito. In questo caso asserire l'implicazione $\alpha \to \beta$ sarebbe come asserire l'equivalenza di α e β, e anche così non si renderebbe certo il senso intuitivo dell'implicazione per cui esiste un'asimmetria tra antecedente e conseguente. Non resta quindi che l'ultima colonna, quella di fatto adottata. Ciò non cancella il disagio provocato da implicazioni come "Se $1 = 2$ allora Parigi è in Francia", che dobbiamo considerare vere sebbene siano palesemente insensate, data la mancanza di un legame tra il pensiero espresso dall'antecedente e quello

espresso dal conseguente, tuttavia di questo non possiamo più lamentarci una volta che abbiamo accettato di escludere l'intensione e di ridurre il significato di un enunciato al valore di verità. Mettere in discussione questa riduzione significa mettere in discussione l'impostazione estensionale che abbiamo dato al discorso logico, e non solo la specifica tabella di calcolo della funzione $f_{\rightarrow}$.

La funzione di verità $f_{\leftrightarrow} : 2^2 \rightarrow 2$ associata all'equivalenza è definita nel modo seguente:

x	y	$f_{\leftrightarrow}(x, y)$
0	0	1
0	1	0
1	0	0
1	1	1

È chiaro che l'equivalenza $\alpha \leftrightarrow \beta$ deve risultare vera quando, e solo quando, α e β hanno lo stesso significato, ossia denotano lo stesso valore di verità.

Sulla base di queste funzioni è possibile calcolare il valore di verità di qualsiasi formula una volta noti i valori di verità delle variabili che in essa occorrono. Consideriamo, ad esempio, $\neg p_0 \rightarrow (p_1 \vee p_2)$. Se associamo le tre variabili enunciative p_0, p_1 e p_2 con tre variabili x, y e z che varino sui valori di verità, e se rimpiazziamo ogni connettivo con la funzione di verità ad esso associata, otteniamo la funzione di verità composta

$$f_{\rightarrow}(f_{\neg}(x), f_{\vee}(y, z)).$$

Se, ad esempio, il valore di verità di p_0 è 1, quello di p_1 è 1 e quello di p_2 è 0, per ottenere il valore di verità di $\neg p_0 \rightarrow (p_1 \vee p_2)$ basta sostituire nella funzione precedente x con 1, y con 1 e z con 0 e calcolare il risultato:

$$f_{\rightarrow}(f_{\neg}(1), f_{\vee}(1, 0)) = f_{\rightarrow}(0, 1) = 1.$$

È possibile analizzare sistematicamente tutti i possibili risultati a cui può dar luogo l'assegnamento di valori di verità alle lettere p_0, p_1 e p_2. Questa analisi sistematica si attua mediante la costruzione della *tavola di verità*, ossia la tabella di calcolo della funzione di verità $f_{\rightarrow}(f_{\neg}(x), f_{\vee}(y, z))$ associata alla formula in questione:

p_0	p_1	p_2	$\neg p_0$	$p_1 \vee p_2$	$\neg p_0 \rightarrow (p_1 \vee p_2)$
0	0	0	1	0	0
0	0	1	1	1	1
0	1	0	1	1	1
0	1	1	1	1	1
1	0	0	0	0	1
1	0	1	0	1	1
1	1	0	0	1	1
1	1	1	0	1	1

Le prime tre colonne contengono tutte le possibili triple di argomenti, la quarta e la quinta i risultati di calcoli intermedi e l'ultima contiene il valore finale. È chiaro che, in generale, la tavola di verità associata a un enunciato contenente n lettere distinte, ossia la tabella di calcolo di una funzione di verità in n variabili distinte, avrà 2^n righe. Tanti, infatti, sono i modi possibili di disporre due oggetti, per esempio 0 e 1, in successioni di lunghezza n. Per convincersene basta pensare che se la successione è di un solo elemento, vi sono solo $2 = 2^1$ possibilità, 0 o 1. Supponiamo di avere a che fare con successioni di lunghezza $n+1$. Per ipotesi induttiva le successioni di lunghezza n sono 2^n; da ognuna di esse si ottengono due successioni di lunghezza $n+1$, aggiungendo 0 o 1. Quindi in totale le successioni di lunghezza $n+1$ sono $2^n \times 2 = 2^{n+1}$.

Siamo ora in grado di giustificare la convenzione notazionale con cui abbiamo introdotto $\alpha \to \beta$ e $\alpha \leftrightarrow \beta$. È facile verificare, infatti, che le due equazioni seguenti sono vere comunque si scelgano i valori di x e y:

$$\begin{aligned} f_{\to}(x,y) &= f_{\vee}(f_{\neg}(x), y)) \\ f_{\leftrightarrow}(x,y) &= f_{\wedge}(f_{\to}(x,y), f_{\to}(y,x)). \end{aligned}$$

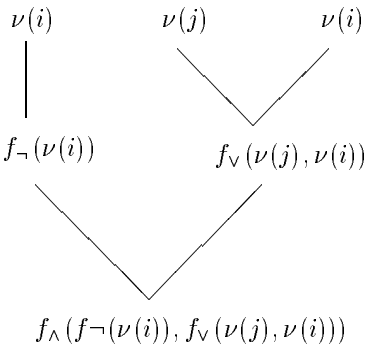
La prima equazione stabilisce che $\alpha \to \beta$ ha lo stesso significato di $\neg\alpha \vee \beta$ e la seconda che $\alpha \leftrightarrow \beta$ ha lo stesso significato di $(\alpha \to \beta) \wedge (\beta \to \alpha)$.

A questo punto dovrebbe essere chiaro che il significato di una formula α consiste non tanto in un valore di verità, quanto in una funzione che associa ad ogni assegnamento di valori di verità alle variabili di α, il valore di verità che α assume per tale assegnamento. Ciò non contraddice l'idea che il significato di un enunciato sia un valore di verità dato che, come abbiamo osservato nel paragrafo 3.1, una formula non rappresenta un singolo enunciato del linguaggio naturale, ma uno schema per formare enunciati aventi in comune la medesima forma logica isolata dalla formula in questione. Nella parte restante di questo paragrafo svilupperemo la semantica del linguaggio enunciativo distinguendo tra un significato relativo delle formule e un significato assoluto. Il significato relativo di una formula è il valore di verità che le viene attribuito sulla base di una data *valutazione* $\nu : \omega \to 2$ che associa ad ogni variabile p_i il valore di verità $\nu(i)$. Il processo attraverso il quale si conferisce alle formule un significato relativo a una data valutazione si riduce al calcolo di funzioni di verità associate ai connettivi e può essere descritto come un morfismo fra strutture dello stesso tipo. Da un lato abbiamo l'algebra delle formule $\mathcal{FM}$ e dall'altro i valori di verità organizzati nell'algebra $\mathcal{D} = (2, f_{\wedge}, f_{\vee}, f_{\neg})$, la restrizione dall'algebra di Boole con due elementi al linguaggio contenente solo $\{\wedge, \vee, \neg\}$. Ogni valutazione ν induce una funzione $g_\nu : P \to 2$, definita ponendo $g_\nu(p_i) = \nu(i)$, che attribuisce un significato relativo alle variabili enunciative. Dal teorema 3.2.1 sappiamo che $\mathcal{FM}$ è generata liberamente da P e quindi, per il teorema 2.6.1, ogni $g_\nu : P \to 2$ si estende a un'unico morfismo $Val_\nu : \mathcal{FM} \to \mathcal{D}$. Ciò significa che, scrivendo $\neg\alpha$ al posto di $\mathcal{O}_{\neg}(\alpha)$, $\alpha \wedge \beta$ al posto di $\mathcal{O}_{\wedge}(\alpha, \beta)$ e $\alpha \vee \beta$ al posto di $\mathcal{O}_{\vee}(\alpha, \beta)$, avremo

1. $Val_\nu(p_n) = g_\nu(p_n)$

2. $Val_\nu(\neg\alpha) = f_\neg(Val_\nu(\alpha))$
3. $Val_\nu(\alpha \wedge \beta) = f_\wedge(Val_\nu(\alpha), Val_\nu(\beta))$,
4. $Val_\nu(\alpha \vee \beta) = f_\vee(Val_\nu(\alpha), Val_\nu(\beta))$.

L'indice ν serve a ricordare che il significato attribuito alle formule da Val_ν è relativo a una data ν. Si vede facilmente che la funzione Val_ν trasforma il processo di generazione sintattico di una formula a partire dalle variabili, in un processo di generazione semantico del valore della formula a partire dai valori di verità associati alle variabili. I punti 2)-4) della recursione fanno in modo che la "forma" del processo di generazione sintattico sia conservata dal processo semantico, che ad ogni applicazione di un dato connettivo corrisponda quella della funzione di verità ad esso associata. Si consideri, ad esempio, la formula $\neg p_i \wedge (p_j \vee p_i)$ di cui abbiamo visto la costruzione nel paragrafo 3.1. Presa una qualsiasi valutazione ν, possiamo rappresentare il processo di attribuzione del significato relativo con l'albero



Si osservi che la forma di questo albero semantico riproduce esattamente quella dell'albero sintattico del paragrafo 3.1 e che ai nodi generati da $f_\neg$, $f_\wedge$ e $f_\vee$ corrispondono rispettivamente i nodi generati con $\mathcal{O}_\neg$, $\mathcal{O}_\wedge$ e $\mathcal{O}_\vee$.

Mentre il significato relativo di α è il suo valore di verità rispetto a un dato assetto del mondo espresso da una valutazione ν, il significato assoluto di α è l'insieme degli assetti del mondo che rendono vera α. Ogni formula denota quindi l'insieme delle circostanze che la rendono vera, ossia un insieme di valutazioni. L'attribuzione alle formule di un significato assoluto sarà allora un morfismo M dall'algebra delle formule $\mathcal{FM}$ verso l'algebra

$$\mathcal{D}(2^\omega) = (P(2^\omega), \cap, \cup, -)$$

che è la restrizione dell'algebra di Boole dei sottoinsiemi di 2^ω al linguaggio contenente solo $\{\wedge, \vee, \neg\}$. La definizione di M avviene per recursione nel modo seguente. Innanzitutto definiamo una funzione $g : P \to P(2^\omega)$ ponendo $g(p_i) = \{\nu \in 2^\omega : \nu(i) = 1\}$: quindi g assegna ad ogni variabile enunciativa l'insieme delle valutazioni che rendono vera tale variabile. Dal teorema 3.2.1 sappiamo

che $\mathcal{FM}$ è generata liberamente da P e quindi, per il teorema 2.6.1, g si estende a un'unico morfismo $M : \mathcal{FM} \to \mathcal{D}(2^\omega)$ che verifica le condizioni seguenti:

$$\begin{aligned} M(\alpha \wedge \beta) &= M(\alpha) \cap M(\beta), \\ M(\alpha \vee \beta) &= M(\alpha) \cup M(\beta), \\ M(\neg\alpha) &= -M(\alpha). \end{aligned}$$

Si osservi che essendo in realtà la notazione $\alpha \to \beta$ un'abbreviazione per $\neg\alpha \vee \beta$, avremo $M(\alpha \to \beta) = -M(\alpha) \cup M(\beta)$. Il teorema seguente mostra il rapporto tra significato assoluto e significato relativo.

Teorema 3.3.1 *Per ogni formula α e ogni valutazione ν, $Val_\nu(\alpha) = 1$ sse $\nu \in M(\alpha)$.*

La dimostrazione è per induzione su α. Se α è p_i, allora $Val_\nu(p_i) = 1$ sse $g_\nu(p_i) = 1$ sse $\nu(i) = 1$ sse $\nu \in g(p_i)$ sse $\nu \in M(p_i)$. Se α è $\neg\beta$ allora $Val_\nu(\neg\beta) = 1$ sse $Val_\nu(\beta) \neq 1$ sse $\nu \notin M(\beta)$ sse $\nu \in -M(\beta)$ sse $\nu \in M(\neg\beta)$. Se α è $\beta \wedge \gamma$ allora $Val_\nu(\beta \wedge \gamma) = 1$ sse $Val_\nu(\beta) = 1$ e $Val_\nu(\gamma) = 1$ sse $\nu \in M(\beta)$ e $\nu \in M(\gamma)$ sse $\nu \in M(\beta) \cap M(\gamma)$ sse $\nu \in M(\beta \wedge \gamma)$. Il caso in cui α è una disgiunzione è trattato in modo analogo.

Significato relativo e significato assoluto sono interdefinibili. Se assumiamo come primitiva Val_ν allora possiamo definire $M(\alpha) = \{\nu : Val_\nu(\alpha) = 1\}$, se assumiamo come primitiva M allora possiamo definire $Val_\nu(\alpha) = 1$ se $\nu \in M(\alpha)$, $Val_\nu(\alpha) = 0$ altrimenti. Nel nostro discorso saremo portati a privilegiare il significato assoluto di una formula rispetto al suo significato relativo: ciò è dovuto al fatto che il discorso logico, nella sua pretesa di universalità, tende a considerare l'insieme delle circostanze in cui una formula è vera piuttosto che specifiche situazioni in cui tale formula risulti essere vera.

Il significato assoluto di una formula α può anche essere concepito in termini funzionali, identificandolo con la funzione caratteristica di $M(\alpha)$, ossia la funzione f_α da valutazioni a valori di verità tale che

$$f_\alpha(\nu) = \begin{cases} 1 & \text{se} \quad \nu \in M(\alpha) \\ 0 & \qquad \text{altrimenti.} \end{cases}$$

Diremo che f_α è la *funzione di verità infinitaria associata* ad α. Si verifica facilmente che, per ogni ν, $f_\alpha(\nu) = Val_\nu(\alpha)$.

Diremo che ν è *modello* di α sse $\nu \in M(\alpha)$, in simboli $\nu \vDash \alpha$. Diremo che α è *soddisfacibile* se possiede un modello. Quando ν è modello di α diremo che α è *vera* nella valutazione ν. Quindi il significato di una formula (d'ora in poi sottointenderemo assoluto) è l'insieme delle valutazioni che la rendono vera, l'insieme dei suoi modelli. Diremo che una formula α è una *tautologia* se $M(\alpha) = 2^\omega$, vale a dire se ogni valutazione è modello di α. Scriveremo $\models \alpha$ per indicare che α è una tautologia, sottolineando in tal modo con la notazione che la sua verità non dipende dalla valutazione. Diremo che α è una *contraddizione* se $M(\alpha) = \emptyset$, ossia se nessuna valutazione è modello di α. Mostriamo, ad esempio, che $\alpha \vee \neg\alpha$ è una tautologia. A tale scopo basta verificare che $M(\alpha) \cup$

$-M(\alpha) = 2^\omega$ ossia che nell'algebra di Boole vale $x \vee \neg x = 1$, il che è evidente. Analogamente si dimostra che $\alpha \wedge \neg\alpha$ è una contraddizione. In generale, per verificare che una formula è una tautologia siamo condotti a verificare la validità di un'equazione booleana. Ad esempio, nel caso di $\neg(\alpha\wedge\beta) \to \neg\alpha\vee\neg\beta$ dobbiamo verificare che

$$- - (M(\alpha) \cap M(\beta)) \cup (-M(\alpha) \cup -M(\beta)) = 2^\omega$$

ossia che nell'algebra di Boole vale $- - (x \wedge y) \vee (-x \vee -y) = 1$. Utilizzando le leggi della doppia negazione, di De Morgan e del terzo escluso otteniamo

$$\neg\neg(x \wedge y) \vee (\neg x \vee \neg y) = (x \wedge y) \vee (\neg x \vee \neg y) = (x \wedge y) \vee \neg(x \wedge y) = 1.$$

Teorema 3.3.2 *Le proposizioni seguenti sono equivalenti.*

1. *α è una tautologia,*
2. *per ogni ν, $f_\alpha(\nu) = 1$,*
3. *per ogni ν, $Val_\nu(\alpha) = 1$.*

1) sse 2): se $M(\alpha) = 2^\omega$ allora f_α è la funzione costante 1 e viceversa. 2) sse 3): per il teorema 3.3.1.

Diremo che α è *equivalente* a β se $M(\alpha) = M(\beta)$, quindi due formule sono equivalenti se hanno lo stesso significato. Il teorema seguente mostra che α e β sono equivalenti se e solo se la loro equivalenza è una tautologia.

Teorema 3.3.3 *Per ogni α e β,*

1. *$\models \alpha \to \beta$ sse $M(\alpha) \subseteq M(\beta)$,*
2. *$\models \alpha \leftrightarrow \beta$ sse $M(\alpha) = M(\beta)$.*

Per quanto riguarda la prima proposizione, si osservi che $\models \alpha \to \beta$ sse $M(\alpha \to \beta) = 2^\omega$ sse $-M(\alpha) \cup M(\beta) = 2^\omega$ sse $M(\alpha) \subseteq M(\beta)$. L'ultimo passaggio dipende dal fatto che nelle algebre di Boole $\neg x \vee y = 1$ sse $x \leq y$.

Per quanto riguarda la seconda, $\models \alpha \leftrightarrow \beta$ sse $M(\alpha \leftrightarrow \beta) = 2^\omega$ sse $M(\alpha \to \beta) \cap M(\beta \to \alpha) = 2^\omega$ sse $M(\alpha \to \beta) = 2^\omega$ e $M(\beta \to \alpha) = 2^\omega$ sse $M(\alpha) \subseteq M(\beta)$ e $M(\beta) \subseteq M(\alpha)$ sse $M(\alpha) = M(\beta)$.

Il teorema precedente è particolarmente utile quando occorre dimostrare che formule di tipo $\alpha \to \beta$ o $\alpha \leftrightarrow \beta$ sono tautologie. La formula $\neg(\alpha\wedge\beta) \leftrightarrow \neg\alpha\vee\neg\beta$ è detta legge di De Morgan: verifichiamo che si tratta di una tautologia mostrando che, dati due insiemi $X, Y \subseteq 2^\omega$, $-(X \cap Y) = -X \cup -Y$. A tale scopo possiamo verificare direttamente che, per ogni $\nu \in 2^\omega$, $\nu \in -(X \cap Y)$ sse $\nu \notin (X \cap Y)$ sse $\nu \notin X$ o $\nu \notin Y$ sse $\nu \in -X$ o $\nu \in -Y$ sse $\nu \in -X \cup -Y$. Oppure è possibile ricavare l'equazione $\neg(x \wedge y) = \neg x \vee \neg y$ dagli assiomi booleani (teorema 2.4.5) e concludere che la stessa equazione vale nell'algebra dei significati $\mathcal{D}(2^\omega)$.

È possibile sviluppare la logica enunciativa utilizzando il linguaggio basato sui connettivi di negazione e implicazione. Innanzitutto poniamo $\mathcal{L}^* =$

$P \cup \{\neg, \to\}$ e definiamo induttivamente l'insieme Fm^* delle formule di $\mathcal{L}^*$ procedendo come nel paragrafo 3.1, otteniamo così l'algebra delle formule $\mathcal{FM}^* = (Fm^*, \mathcal{O}_\to, \mathcal{O}_\neg)$. L'algebra dei significati sarà $\mathcal{D}^* = (2, f_\to, f_\neg)$. Il significato relativo si ottiene con un morfismo Val^*_ν da $\mathcal{FM}^*$ verso $\mathcal{D}^*$ indotto dalla valutazione ν, le cui proprietà fondamentali sono date dalle seguenti equazioni:

1. $Val^*_\nu(\neg\alpha) = f_\neg(Val^*_\nu(\alpha))$,
2. $Val^*_\nu(\alpha \to \beta) = f_\to(Val^*_\nu(\alpha), Val^*_\nu(\beta))$.

Il significato assoluto si ottiene con un morfismo M^* da $\mathcal{FM}^*$ verso la struttura $(2^\omega, \Rightarrow, -)$, dove $\Rightarrow$ è l'operazione binaria su insiemi tale che $X \Rightarrow Y = -X \cup Y$. Come al solito poniamo $M^*(p_i) = \{\nu \in 2^\omega : \nu(i) = 1\}$ e le proprietà fondamentali del morfismo indotto sono espresse dalle equazioni seguenti:

1. $M^*(\neg\alpha) = -M^*(\alpha)$,
2. $M^*(\alpha \to \beta) = M^*(\alpha) \Rightarrow M^*(\beta)$.

A questo punto è possibile dimostrare un teorema che stabilisce i rapporti tra significato assoluto e significato relativo, analogo al teorema 3.3.1. Lasciamo questo compito al lettore e ci occupiamo invece della traducibilità fra i linguaggi $\mathcal{L}$ e $\mathcal{L}^*$, dalla quale otterremo come corollario tali rapporti. Definiamo per recursione una funzione di traduzione τ da Fm^* verso Fm, ponendo

1. $\tau(p_i) = p_i$,
2. $\tau(\neg\alpha) = \neg\tau(\alpha)$,
3. $\tau(\alpha \to \beta) = \neg\tau(\alpha) \vee \tau(\beta)$.

Lasciamo al lettore il compito di formulare correttamente le condizioni che rendono applicabile il teorema di recursione. Il teorema seguente mostra che la traduzione τ associa ad ogni formula di $\mathcal{L}^*$ una formula di $\mathcal{L}$ dello stesso significato.

Teorema 3.3.4 *Per ogni α di $\mathcal{L}^*$,*

1. $M^*(\alpha) = M(\tau(\alpha))$,
2. $Val^*_\nu(\alpha) = Val_\nu(\tau(\alpha))$.

1. La dimostrazione è per induzione sulle formule. Ovviamente $M^*(p_i) = M(\tau(p_i))$. Nel caso della negazione, poiché per ipotesi induttiva $M^*(\beta) = M(\tau(\beta))$, abbiamo

$$M^*(\neg\beta) = -M^*(\beta) = -M(\tau(\beta)) = M(\neg\tau(\beta)) = M(\tau(\neg\beta)).$$

Nel caso dell'implicazione, poiché per ipotesi induttiva vale $M^*(\beta) = M(\tau(\beta))$ e $M^*(\gamma) = M(\tau(\gamma))$, abbiamo

$$\begin{aligned} M^*(\tau(\beta \to \gamma)) &= M(\neg\tau(\beta) \vee \tau(\gamma)) \\ &= -M(\tau(\beta)) \cup M(\tau(\gamma)) \\ &= -M(\beta) \cup M(\gamma) \\ &= M(\beta) \Rightarrow M(\gamma) \\ &= M(\beta \to \gamma). \end{aligned}$$

2. La dimostrazione è analoga alla precedente.

Siamo ora in grado di dimostrare il rapporto tra significato assoluto e significato relativo nel caso di $\mathcal{L}^*$.

Corollario 3.3.5 *Per ogni α di $\mathcal{L}^*$, $Val^*_\nu(\alpha) = 1$ sse $\nu \in M^*(\alpha)$.*

Per il secondo punto del teorema precedente, $Val^*_\nu(\alpha) = 1$ sse $Val_\nu(\tau(\alpha)) = 1$. Per il teorema 3.3.1, $Val_\nu(\tau(\alpha)) = 1$ sse $\nu \in M(\tau(\alpha))$. Infine $\nu \in M(\tau(\alpha))$ sse $\nu \in M^*(\alpha)$, per il primo punto del teorema precedente.

In seguito si rivelerà utile anche la traduzione ψ da Fm verso Fm^* definita ponendo

1. $\psi(p_i) = p_i$
2. $\psi(\neg\alpha) = \neg\psi(\alpha)$,
3. $\psi(\alpha \wedge \beta) = \neg(\psi(\alpha) \to \neg\psi(\beta))$,
4. $\psi(\alpha \vee \beta) = \neg\psi(\alpha) \to \psi(\beta)$.

Tale traduzione assegna ad ogni formula di $\mathcal{L}$ una formula di $\mathcal{L}^*$ di significato identico, come mostra il teorema seguente.

Teorema 3.3.6 *Per ogni α di $\mathcal{L}$, $M(\alpha) = M^*(\psi(\alpha))$.*

La dimostrazione è per induzione sulle formule. Il caso delle variabili enunciative è banale. Il caso della negazione segue immediatamente dall'ipotesi induttiva. Supponiamo ora che α sia $\beta \wedge \gamma$. Per ipotesi induttiva abbiamo $M(\beta) = M^*(\psi(\beta))$ e $M(\gamma) = M^*(\psi(\gamma))$. Vale allora

$$\begin{aligned} M^*(\psi(\beta \wedge \gamma)) &= M^*(\neg(\psi(\beta) \to \neg\psi(\gamma))) \\ &= -(M^*(\psi(\beta)) \Rightarrow -M^*(\psi(\gamma))) \\ &= -(-M^*(\psi(\beta)) \cup -M^*(\psi(\gamma))) \\ &= M^*(\psi(\beta)) \cap M^*(\psi(\gamma)) \\ &= M(\beta) \cap M(\beta) \\ &= M(\beta \wedge \gamma). \end{aligned}$$

In modo analogo si procede quando α è $\beta \vee \gamma$.

Esercizio 3.3.1 Utilizzando il teorema 3.3.3, si verifichi che le formule seguenti sono tautologie:

1. $\alpha \to \alpha$ (legge d'identità),
2. $\neg\neg\alpha \leftrightarrow \alpha$ (legge della doppia negazione),
3. $\alpha \to (\beta \to \alpha)$ (a fortiori),
4. $\neg(\alpha \vee \beta) \leftrightarrow (\neg\alpha \wedge \neg\beta)$ (legge di De Morgan),
5. $(\alpha \to \beta) \leftrightarrow (\neg\beta \to \neg\alpha)$ (legge di contrapposizione),
6. $(\alpha \to (\beta \to \gamma)) \leftrightarrow (\beta \to (\alpha \to \gamma))$ (scambio di premesse),
7. $(\alpha \to (\beta \to \gamma)) \leftrightarrow (\alpha \wedge \beta \to \gamma)$,
8. $\alpha \to (\neg\alpha \to \beta)$ (ex falso sequitur quodlibet o legge di Duns Scoto).

Esercizio 3.3.2 Si dimostri che, per ogni $\alpha \in Fm$ e ogni $\nu \in 2^\omega$, $f_\alpha(\nu) = Val_\nu(\alpha)$.

Esercizio 3.3.3 Si considerino i linguaggi $\mathcal{L}_\wedge$ e $\mathcal{L}_\vee$ basati rispettivamente sui connettivi $\{\neg, \wedge\}$ e $\{\neg, \vee\}$. Dopo aver definito per essi una semantica nel modo usuale, si definiscano traduzioni verso e da $\mathcal{L}$ in modo che a ogni formula di $\mathcal{L}_\wedge$ e $\mathcal{L}_\vee$ sia associata una formula di $\mathcal{L}$ con lo stesso significato e viceversa.

Esercizio 3.3.4 Diciamo che $X \subseteq 2^\omega$ è n-completo se, per ogni ν, $\mu \in 2^\omega$, $\nu \in X$ e $\nu \restriction n = \mu \restriction n$ implica $\mu \in X$. Si dimostri che gli insiemi n-completi formano un'algebra di Boole $\mathcal{A}$ che è sottoalgebra di $\mathcal{B}(2^\omega)$, l'algebra dei sottoinsiemi di 2^ω. Si consideri la funzione $f : P(2^\omega) \to P(2^n)$ definita ponendo $f(X) = X \restriction n$. Si verifichi che f non è un morfismo, mentre la restrizione di f ad $\mathcal{A}$ lo è. Si dimostri che gli n-completi coincidono con le immagini delle formule n-arie in M.

3.4 Significato finitario

È possibile ricondurre la semantica a un ambito finitario e riconnettersi al discorso iniziale sulle tavole di verità introducendo il concetto di formula n-aria. Per ogni $n > 0$, poniamo $P_n = \{p_0, ..., p_{n-1}\}$ e quindi consideriamo la sottostruttura $\mathcal{FM}_n$ generata in $\mathcal{FM}$ da P_n, ossia la minima sottostruttura dell'algebra delle formule contenente l'insieme P_n. Il dominio Fm_n di $\mathcal{FM}_n$ è l'insieme definito induttivamente in $\mathcal{FM}$ dalla coppia $(B, \mathcal{F})$, dove $B = P_n$ e $\mathcal{F} = \{\mathcal{O}_\wedge, \mathcal{O}_\vee, \mathcal{O}_\neg\}$. Definiamo *formule n-arie* gli elementi di Fm_n: indicheremo con $\alpha(p_0, \ldots, p_{n-1})$ una generica formula n-aria per sottolineare che in essa possono occorrere solo variabili di indice minore di n. Il teorema seguente fornisce una definizione esplicita delle formule n-arie che permette di riconoscerle facilmente in Fm.

Teorema 3.4.1 *Fm_n è l'insieme delle formule in cui occorrono solo variabili di indice minore di n.*

Sia X l'insieme delle formule in cui occorrono solo variabili di indice minore di n. Per dimostrare che $Fm_n \subseteq X$ basta osservare che X è il dominio di una sottostruttura di $\mathcal{FM}$ contenente P_n: infatti ogni p_i, con $i < n$, appartiene a X e inoltre X è chiuso rispetto alle operazioni di $\mathcal{FM}$. L'asserto segue allora dal fatto che $\mathcal{FM}_n$ è la minima sottostruttura di $\mathcal{FM}$ che include P_n. Dimostriamo ora che $X \subseteq Fm_n$, ossia che per ogni formula $\alpha \in Fm$, se $\alpha \in X$ allora $\alpha \in Fm_n$. La dimostrazione è per induzione sulle formule e quindi dobbiamo provare che l'insieme $Y = \{\alpha \in Fm : \alpha \in X \text{ implica } \alpha \in Fm_n\}$ include P_n ed è chiuso rispetto a $\mathcal{O}_\neg$, $\mathcal{O}_\wedge$ e $\mathcal{O}_\vee$. Evidentemente $p_i \in X$ implica $i < n$ e quindi $p_i \in P_n$ e $p_i \in Fm_n$. Mostriamo ora che se β e γ appartengono a Y allora anche $\beta \wedge \gamma \in Y$: infatti se $\beta \wedge \gamma \in X$ allora anche β e γ contengono solo variabili di indice minore di n e quindi appartengono a X, ma allora appartengono a Fm_n per ipotesi e quindi anche $\beta \wedge \gamma$ appartiene a Fm_n, dato che quest'ultimo è chiuso rispetto a $\mathcal{O}_\wedge$. Lo stesso discorso vale per i connettivi $\neg$ e $\vee$.

Si osservi, ad esempio, che $p_0 \wedge p_1$ è una formula 2-aria e quindi del tipo di $\alpha(p_0, p_1)$. La medesima formula, però, è anche 3-aria, dato che le sue variabili hanno indice minore di 3, e quindi è anche del tipo di $\alpha(p_0, p_1, p_2)$. La formula $p_1 \wedge p_2$ *non* è 2-aria, anche se contiene esattamente due variabili, e quindi non è del tipo di $\alpha(p_0, p_1)$. Essa è 3-aria, e in generale n-aria per ogni $n > 2$, quindi possiamo pensarla come $\alpha(p_0, \ldots, p_{n-1})$, per ogni $n > 2$. Per le stesse ragioni, ogni variabile p_i è una formula j-aria, per ogni $j > i$. È quindi evidente che una stessa formula può essere considerata come formula n-aria per infiniti valori di n e che $Fm_i \subseteq Fm_j$, per ogni $i \leq j$. Il fatto che una formula possa avere arietà diverse e che l'arietà non coincida col numero delle variabili che essa contiene è certamente poco intuitivo, tuttavia questa definizione di formula n-aria permette di vedere l'insieme delle formule n-arie come un insieme definito induttivamente da P_n in $\mathcal{FM}$. Se definissimo "formula n-aria" come "formula in cui occorrono esattamente n variabili distinte" o come "formula in cui n è il massimo degli indici delle variabili effettivamente occorrenti in essa", otterremmo che ogni formula α sarebbe n-aria per un unico valore di n, ma non potremmo più dimostrare il teorema precedente e quindi non potremmo più definire per recursione sulle formule n-arie, come ci accingiamo a fare.

Associamo alle formule n-arie un significato finitario nel modo seguente. Innanzitutto osserviamo che come $\mathcal{FM}$ è generata liberamente da P, così $\mathcal{FM}_n$ è generata liberamente da P_n: ciò rende possibile definire per recursione un morfismo M^n da $\mathcal{FM}_n$ verso l'algebra

$$\mathcal{D}(2^n) = (P(2^n), \cap, \cup, -)$$

facendolo indurre da una funzione $g : P_n \to P(2^n)$ tale che $g(p_i) = \{s \in 2^n : s(i) = 1\}$: per il teorema 2.6.1 g si estende a un unico morfismo M^n dall'algebra delle formule n-arie verso $\mathcal{D}(\,2^n)$. Chiameremo $M^n(\alpha)$ significato n-ario di α.

Il significato n-ario può anche essere pensato in termini funzionali, identificandolo con la funzione caratteristica di $M^n(\alpha)$, ossia con la funzione n-aria f^n_α

da 2^n verso 2 tale che, per ogni $s \in 2^n$,

$$f_\alpha^n(s) = \begin{cases} 1 & \text{se} \quad s \in M^n(\alpha) \\ 0 & \qquad \text{altrimenti.} \end{cases}$$

Diremo che f_α^n è la *funzione di verità n-aria associata* ad α: le tavole di verità, dalle quali ha preso avvio il nostro discorso sulla semantica, non sono altro che le tabelle di calcolo delle funzioni di verità n-arie associate alle formule.

Il significato n-ario ha il vantaggio di essere un insieme finito, mentre $M(\alpha)$ è in genere un insieme infinito, addirittura più che numerabile. Naturalmente possiamo parlare di significato n-ario solo per formule n-arie e ciò costituisce un limite quando si vogliono confrontare i significati di un insieme infinito di formule. Infatti, mentre due formule α e β possono sempre essere considerate n-arie per qualche n, un insieme infinito di formule può contenere formule di arietà arbitrariamente grande e quindi può non esistere un n tale che tutte siano formule n-arie. In questo caso i significati delle formule possono essere confrontati solo come valori di M e quindi M non è sostituibile dalla totalità delle M^n.

I significati $M(\alpha)$ e $M^n(\alpha)$ sono stati definiti per recursione in modo indipendente, ma si tratta di due concetti correlati: il significato finitario $M^n(\alpha)$ si ottiene troncando le valutazioni di $M(\alpha)$ al livello n. Ricordiamo che $\nu \restriction n = (\nu(0), ..., \nu(n-1))$ e definiamo, per ogni $X \subseteq 2^\omega$, $X \restriction n = \{\nu \restriction n : \nu \in X\}$.

Teorema 3.4.2 *Se α è n-aria e se ν e μ sono valutazioni tali che $\nu \restriction n = \mu \restriction n$ allora $\nu \in M(\alpha)$ sse $\mu \in M(\alpha)$.*

La dimostrazione è per induzione su α. Se $\alpha = p_i$ è certamente $i < n$ e poiché da $\nu \restriction n = \mu \restriction n$ deriva $\nu(i) = \mu(i)$ per $i < n$, abbiamo $\nu \in (p_i)$ sse $\nu(i) = 1$ sse $\mu(i) = 1$ sse $\mu \in (p_i)$. Se $\alpha = \neg\beta$, allora β è n-aria e per ipotesi induttiva abbiamo $\nu \in M(\beta)$ sse $\mu \in M(\beta)$, quindi

$$\nu \in M(\neg\beta) \text{ sse } \nu \notin M(\beta) \text{ sse } \mu \notin M(\beta) \text{ sse } \mu \in M(\neg\beta).$$

Se $\alpha = \beta \wedge \gamma$ allora β e γ sono n-arie, quindi $\nu \in M(\beta)$ sse $\mu \in M(\beta)$ e $\nu \in M(\gamma)$ sse $\mu \in M(\gamma)$. Abbiamo allora

$$\begin{array}{lll} \nu \in M(\beta \wedge \gamma) & \text{sse} & \nu \in M(\beta) \text{ e } \nu \in M(\gamma) \\ & \text{sse} & \mu \in M(\beta) \text{ e } \mu \in M(\gamma) \\ & \text{sse} & \mu \in M(\beta \wedge \gamma). \end{array}$$

Il caso della disgiunzione è trattato in modo analogo.

Teorema 3.4.3 *Per ogni formula n-aria α, $M^n(\alpha) = M(\alpha) \restriction n$.*

La dimostrazione è per induzione su α. Evidentemente, essendo $i < n$, $M^n(p_i) = \{s \in 2^n : s(i) = 1\} = M(p_i) \restriction n$.

Se $\alpha = \neg\beta$ allora $M^n(\neg\beta) = -M^n(\beta) = -M(\beta) \restriction n$ per ipotesi induttiva. Resta da dimostrare che $-M(\beta) \restriction n = M(\neg\beta) \restriction n$. Assumiamo $s \in -M(\beta) \restriction n$,

allora $s \notin M(\beta) \restriction n$ e quindi per ogni ν tale che $\nu \restriction n = s$, $\nu \notin M(\beta)$ e perciò $\nu \in M(\neg\beta)$, ma allora $s \in M(\neg\beta) \restriction n$. Viceversa, se $s \in M(\neg\beta) \restriction n$ allora esiste ν tale che $\nu \restriction n = s$ e $\nu \in M(\neg\beta)$. Quindi $\nu \in -M(\beta)$ e $\nu \notin M(\beta)$. Se valesse $s \in M(\beta) \restriction n$ allora esisterebbe μ tale che $\mu \restriction n = s$ e $\mu \in M(\beta)$, ma per il teorema precedente allora anche $\nu \in M(\beta)$, il che è assurdo. Quindi $s \notin M(\beta) \restriction n$ e $s \in -M(\beta) \restriction n$.

Se $\alpha = \beta \wedge \gamma$ allora $M^n(\beta \wedge \gamma) = M^n(\beta) \cap M^n(\gamma) = M(\beta) \restriction n \cap M(\gamma) \restriction n$ per ipotesi induttiva. Resta da dimostrare che $M(\beta) \restriction n \cap M(\gamma) \restriction n = M(\beta \wedge \gamma) \restriction n$. Assumiamo $s \in M(\beta) \restriction n$ e $s \in M(\gamma) \restriction n$. Allora esiste ν tale che $\nu \restriction n = s$ e $\nu \in M(\beta)$ ed esiste μ tale che $\mu \restriction n = s$ e $\mu \in M(\gamma)$. Per il teorema precedente $\nu \in M(\gamma)$ e quindi, poiché $\nu \in M(\beta)$, $\nu \in M(\beta \wedge \gamma)$ e $s \in M(\beta \wedge \gamma) \restriction n$. Viceversa, se $s \in M(\beta \wedge \gamma) \restriction n$ allora esiste ν tale che $\nu \restriction n = s$ e $\nu \in M(\beta \wedge \gamma)$, ma allora $\nu \in M(\beta)$ e $\nu \in M(\gamma)$ e quindi $s \in M(\beta) \restriction n$ e $s \in M(\gamma) \restriction n$, perciò $s \in M(\beta) \restriction n \cap M(\gamma) \restriction n$.

Se α è $\beta \vee \gamma$ la dimostrazione è analoga.

Possiamo ora ricondurre il concetto di tautologia all'ambito finitario e alle tavole di verità dimostrando che, se α è n-aria, allora α è una tautologia sse $M^n(\alpha) = 2^n$. Infatti α è una tautologia sse $M(\alpha) = 2^\omega$ sse $M(\alpha) \restriction n = 2^\omega \restriction n$, usando il teorema 3.4.2, sse $M^n(\alpha) = 2^n$, usando il teorema 3.4.3.

Corollario 3.4.4 *Per ogni $\alpha \in Fm_n$ e ogni $\nu \in 2^\omega$, $f_\alpha(\nu) = f^n_\alpha(\nu \restriction n)$.*

Per le definizioni di f^n_α e di f_α e per il teorema precedente, $f^n_\alpha(\nu \restriction n) = 1$ sse $\nu \restriction n \in M^n(\alpha)$ sse $\nu \restriction n \in M(\alpha) \restriction n$ sse $\nu \in M(\alpha)$ sse $f_\alpha(\nu) = 1$.

Anche per $\mathcal{L}^*$, il linguaggio basato sui connettivi $\neg$ e $\rightarrow$, possiamo parlare di formule n-arie e possiamo definire il significato significato finitario come un morfismo M^*_n che assegna a ogni formula n-aria un insieme di n-ple di valori di verità. Lasciamo al lettore il compito di formulare le definizioni dell'algebra delle formule n-arie nel caso di $\mathcal{L}^*$ e dell'algebra in cui tali formule assumono i loro significati. Come abbiamo già dimostrato per $\mathcal{L}$, il significato finitario di una formula si può ottenere con una restrizione delle valutazioni che ne costituiscono il significato. Osserviamo innanzitutto che la traduzione τ, definita nel paragrafo 3.3, porta formule n-arie su formule n-arie: ciò permette di dimostrare il teorema seguente.

Teorema 3.4.5 *Per ogni formula n-aria α di $\mathcal{L}^*$, $M^*_n(\alpha) = M^n(\tau(\alpha))$.*

La dimostrazione, per induzione sulle formule, ricalca quella del teorema 3.3.4 ed è lasciata al lettore.

Corollario 3.4.6 *Per ogni formula n-aria α di $\mathcal{L}^*$, $M^*_n(\alpha) = M^*(\alpha) \restriction n$.*

Vale $s \in M^*_n(\alpha)$ sse $s \in M^n(\tau(\alpha))$, per il teorema precedente, sse $s \in M(\tau(\alpha)) \restriction n$ per il teorema 3.4.3, sse $s \in M^*(\alpha) \restriction n$, per il teorema 3.3.4.

Ogni formula del linguaggio enunciativo esprime un significato costituito da un sottoinsieme di 2^ω. Per ragioni di cardinalità non tutti i sottoinsiemi di 2^ω sono il significato di qualche formula, tuttavia è possibile dimostrare che ogni

sottoinsieme di 2^n è il significato di una formula n-aria e che per ogni funzione $f : 2^n \to 2$ esiste una formula n-aria α tale che $f = f^n_\alpha$, vale a dire f è la funzione di verità n-aria associata ad α.

Innanzitutto introduciamo una notazione che permetta di rappresentare in modo abbreviato le congiunzioni e le disgiunzioni finite di formule. Poniamo quindi, per ogni $n > 0$ e ogni $\alpha_0, ..., \alpha_{n-1}$,

$$\bigwedge_{i<n} \alpha_i = \alpha_0 \wedge ... \wedge a_{n-1} \text{ e } \bigvee_{i<n} \alpha_i = \alpha_0 \vee ... \vee a_{n-1}.$$

Diremo allora che una congiunzione $\bigwedge_{i<n} \eta_i$ è una *congiunzione fondamentale* n-aria se, per ogni $i < n$, $\eta_i = p_i$ oppure $\eta_i = \neg p_i$. Osserviamo che ad ogni congiunzione fondamentale $\bigwedge_{i<n} \eta_i$ è associata esattamente una n-pla $s \in 2^n$ tale che $M^n(\bigwedge_{i<n} \eta_i) = \{s\}$, e precisamente la n-pla s tale che $s_i = 1$ se $\eta_i = p_i$ e $s_i = 0$ se $\eta_i = \neg p_i$. Viceversa, per ogni $s \in 2^n$ esiste un'unica congiunzione fondamentale $\bigwedge_{i<n} \eta_i$ tale che $M^n(\bigwedge_{i<n} \eta_i) = \{s\}$. Diremo che una formula n-aria α è in *forma normale disgiuntiva* se è una disgiunzione di congiunzioni fondamentali. Supponiamo, ad esempio, che sia $n = 3$: esistono allora 2^3 congiunzioni fondamentali 3-arie:

$$\begin{array}{rcc} \beta_0 & = & p_0 \wedge p_1 \wedge p_2 \\ \beta_1 & = & p_0 \wedge p_1 \wedge \neg p_2 \\ \beta_2 & = & p_0 \wedge \neg p_1 \wedge p_2 \\ \vdots & & \vdots \\ \beta_7 & = & \neg p_0 \wedge \neg p_1 \wedge \neg p_2 \end{array}$$

Ogni disgiunzione $\bigvee_{j<k} \gamma_j$ di formule γ_i scelte tra le $\beta_0, ..., \beta_7$ è una forma normale disgiuntiva 3-aria. Una forma normale disgiuntiva n-aria conterrà al massimo 2^n disgiunti, scelti tra le 2^n possibili congiunzioni fondamentali n-arie.

Teorema 3.4.7 *Per ogni $X \subseteq 2^n$ esiste una forma normale disgiuntiva n-aria α tale che $M^n(\alpha) = X$.*

Per ogni $s \in X$ esiste una congiunzione fondamentale β_s tale che $M^n(\beta_s) = \{s\}$ e quindi consideriamo la forma normale disgiuntiva $\bigvee_{s \in X} \beta_s$. Abbiamo allora

$$M^n(\bigvee_{s \in X} \beta_s) = \bigcup_{s \in X} M^n(\beta_s) = X,$$

dato che $M^n(\beta_s) = \{s\}$ per ogni $s \in X$.

Corollario 3.4.8 *Per ogni formula n-aria β esiste una formula α in forma normale disgiuntiva n-aria equivalente ad β, ossia tale che $M(\beta) = M(\alpha)$.*

Dal teorema 3.4.3 sappiamo che $M(\beta) \restriction n = M^n(\beta)$. D'altra parte $M^n(\beta)$ è un sottoinsieme di 2^n e quindi, per il teorema precedente, esiste una formula n-aria α in forma normale disgiuntiva tale che $M^n(\alpha) = M^n(\beta)$. Sempre per il

teorema 3.4.3 abbiamo $M^n(\alpha) = M(\alpha) \restriction n$ e quindi $M(\beta) \restriction n = M(\alpha) \restriction n$. Per il teorema 3.4.2 possiamo concludere che $M(\alpha) = M(\beta)$.

Il significato finitario può essere pensato come una funzione di verità da 2^n verso 2: il corollario seguente mostra che anche da questo punto vista ogni significato finitario è esprimibile mediante una formula.

Corollario 3.4.9 *Per ogni $n > 0$ e ogni $f : 2^n \to 2$ esiste una formula n-aria α tale che $f = f^n_\alpha$.*

Ogni funzione $f : 2^n \to 2$ è la funzione caratteristica di un insieme $X \subseteq 2^n$. Per il teorema precedente $X = M^n(\alpha)$ per qualche formula n-aria α e quindi, per definizione, f è la funzione di verità n-aria associata ad α ossia $f = f^n_\alpha$.

Come abbiamo visto alla fine del paragrafo 3.3, i linguaggi $\mathcal{L}$ e $\mathcal{L}^*$ sono equivalenti, nel senso che è possibile tradurre ogni formula dell'uno in una formula dell'altro avente lo stesso significato. Quindi anche $\mathcal{L}^*$ è in grado di esprimere tutti i possibili significati finitari: se $X \subseteq 2^n$ dal teorema precedente sappiamo che esiste una formula α di $\mathcal{L}$ tale che $X = M^n(\alpha)$, per il teorema 3.4.3 $M^n(\alpha) = M(\alpha) \restriction n$, per il teorema 3.3.6 $M(\alpha) = M^*(\psi(\alpha))$ e quindi $M(\alpha) \restriction n = M^*(\psi(\alpha)) \restriction n$, infine $M^*(\psi(\alpha)) \restriction n = M^*_n(\psi(\alpha))$ per il corollario 3.4.6.

Esercizio 3.4.1 Si dimostri che per ogni α, $\beta \in Fm_n$,

1. $M(\alpha) \subseteq M(\beta)$ sse $M^n(\alpha) \subseteq M^n(\beta)$,
2. $M(\alpha) = M(\beta)$ sse $M^n(\alpha) = M^n(\beta)$.

3.5 Sostituzione

Consideriamo l'insieme E delle espressioni di un linguaggio $\mathcal{L}$ strutturato dall'operazione $*$ di concatenazione di successioni finite. Intuitivamente un'espressione b occorre in un'espressione a se esistono due espressioni x e y tali che $a = x * b * y$. (È possibile che x o y o entrambe siano la successione vuota.) Ad esempio, $\neg p_0$ occorre in $\wedge\neg p_0 \neg p_1$, ponendo x uguale a $\wedge$ e y a $\neg p_1$. Tuttavia a può occorrere in luoghi diversi di b. Ad esempio, $\neg p_0$ occorre due volte in $\wedge\neg p_0 \wedge \neg p_0$: la prima occorrenza si ottiene ponendo x uguale a $\wedge$ e y a $\wedge\neg p_0$ e la seconda ponendo x uguale a $\wedge\neg p_0\wedge$ e y alla successione vuota. Per individuare le varie occorrenze di a in b possiamo numerarle da sinistra a destra; nel caso precedente, quindi, parleremo della prima e della seconda occorrenza di $\neg p_0$ in $\wedge\neg p_0 \wedge \neg p_0$. Se in a vi sono n occorrenze di b, allora esistono delle espressioni $x_1, \ldots, x_{n+1}$ tali che

$$a = x_1 * b * x_2 * b * \ldots * x_n * b * x_{n+1}.$$

Se a contiene n occorrenze di b, definiamo sezione determinata dalla i-esima occorrenza di b, $(0 \leq i \leq n)$, la coppia di espressioni (y, z) dove

$$y = x_1 * b * x_2 * \ldots * x_{i-1} * b * x_i$$

e

$$z = x_{i+1} * b * x_{i+2} * \ldots * x_n * b * x_{n+1}.$$

Evidentemente vale $a = y * b * z$. Diremo infine che a' è ottenuta da a per *rimpiazzamento* dell'n-esima occorrenza di b con c se (y, z) è la sezione determinata in a dall'n-esima occorrenza di b e $a' = y * c * z$. Quindi se nell'espressione $\wedge\neg p_0 \wedge \neg p_0$ rimpiazziamo la prima occorrenza di $\neg p_0$ con p_1 otterremo $\wedge p_1 \wedge \neg p_0$, se rimpiazziamo la seconda otterremo $\wedge\neg p_0 \wedge p_1$.

A differenza del rimpiazzamento, che è un'operazione di tipo locale che agisce su singole occorrenze di una data espressione, l'operazione di sostituzione è di tipo globale ed agisce simultaneamente su tutte le occorrenze di una data variabile. Potremmo definire l'operazione di sostituzione nei termini dell'operazione di rimpiazzamento nel modo seguente: per ogni coppia di formule α, β e ogni variabile p_i, il risultato della sostituzione di p_i con β in α si ottiene rimpiazzando simultaneamente con β ogni occorrenza di p_i in α. In tal modo rimarrebbe tuttavia da dimostrare che il risultato della sostituzione di una variabile con una formula sia ancora una formula, e non un'espressione qualsiasi. Preferiamo quindi presentare la sostituzione come un morfismo dell'algebra delle formule in se stessa. Definiamo *sostituzione* una funzione $\sigma : P \to Fm$. Poiché l'algebra delle formule è generata liberamente da P, è possibile estendere ogni sostituzione σ ad un'unico morfismo $So_\sigma : \mathcal{FM} \to \mathcal{FM}$. Avremo quindi

1. $So_\sigma(p_i) = \sigma(p_i)$
2. $So_\sigma(\neg\alpha) = \neg So_\sigma(\alpha)$
3. $So_\sigma(\alpha \wedge \beta) = So_\sigma(\alpha) \wedge So_\sigma(\beta)$,
4. $So_\sigma(\alpha \vee \beta) = So_\sigma(\alpha) \vee So_\sigma(\beta)$.

Se α è una formula n-aria e $\sigma(p_i) = \beta_i$, indicheremo spesso $So_\sigma(a)$ con la notazione più intuitiva

$$\alpha(p_0/\beta_0, ..., p_{n-1}/\beta_{n-1}) \text{ o } \alpha(\beta_0, ..., \beta_{n-1}),$$

poiché So_σ compie sulle formule una trasformazione che dipende unicamente dai valori di σ relativi alle variabili p_i di indice $i < n$, esattamente come Val_ν assegna un significato che dipende solo dai valori di ν per $i < n$. Possiamo visualizzare il processo di sostituzione operato da So_σ sulla formula α generando la costruzione ad albero di α, cambiando nei nodi terminali ogni variabile p_i con la formula $\sigma(p_i)$, e quindi procedendo verso il basso applicando nello stesso ordine le operazioni $\mathcal{O}_\neg$, $\mathcal{O}_\wedge$ e $\mathcal{O}_\vee$. Al termine di questo processo la formula che occupa la radice sarà $So_\sigma(\alpha)$. La sostituzione può operare anche tra due linguaggi diversi. Se $\mathcal{L}_0 = C \cup P_0$ e $\mathcal{L}_1 = C \cup P_1$, possiamo estendere il concetto di sostituzione al caso di una funzione $\sigma : P_0 \to Fm_1$, dato che anche in questo caso è possibile estendere σ a un'unica funzione $So_\sigma : Fm_0 \to Fm_1$. Se supponiamo che P_0 sia l'insieme delle variabili metalinguistiche α, $\beta, \ldots$, diremo che una

formula di $\mathcal{L}_0$ è uno *schema* perché può dare origine a una infinità di formule di $\mathcal{L}_1$ al variare di $\sigma : P_0 \to Fm_1$.

Concludiamo osservando che l'ordine in cui si compiono le sostituzioni è essenziale. Supponiamo ad esempio che valga $\sigma_0(p_i) = p_j$ e che σ_0 sia l'identità per ogni altro argomento. Supponiamo inoltre che valga $\sigma_1(p_j) = p_k$ e che σ_1 sia l'identità in ogni altro caso. Abbiamo allora

$$So_{\sigma_1}(So_{\sigma_0}(p_i \wedge p_j)) = p_k \wedge p_k$$

e

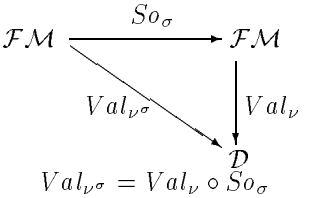
$$So_{\sigma_0}(So_{\sigma_1}(p_i \wedge p_j)) = p_j \wedge p_k.$$

Possiamo ora dimostrare un teorema che considera l'azione combinata di So_σ e Val_ν. Data una sostituzione σ e una valutazione ν, definiamo una valutazione ν^σ ponendo $\nu^\sigma(i) = Val_\nu(\sigma(p_i))$. Potremmo dire che con ν^σ viene rappresentata sul piano semantico la sostituzione che σ compie sul piano sintattico: ν^σ attribuisce a p_i il significato che ν attribuisce alla formula che σ sostituisce a p_i.

Teorema 3.5.1 *Per ogni sostituzione σ, valutazione ν e formula α,*

$$Val_\nu(So_\sigma(\alpha)) = Val_{\nu^\sigma}(\alpha).$$

Dobbiamo dimostrare che i due morfismi $Val_\nu \circ So_\sigma$ e Val_{ν^σ} coincidono, come mostra la figura seguente:



$$Val_{\nu^\sigma} = Val_\nu \circ So_\sigma$$

Poiché entrambi sono morfismi dalla struttura $\mathcal{FM}$ verso $\mathcal{D}$ e poiché $\mathcal{FM}$ è generata da P, per il teorema 2.5.2 è sufficiente dimostrare che i due morfismi coincidono sui generatori, ossia $Val_\nu(So_\sigma(p_i)) = Val_{\nu^\sigma}(p_i)$ per ogni $i \in \omega$. Vale infatti $Val_\nu(So_\sigma(p_i)) = Val_\nu(\sigma(p_i)) = \nu^\sigma(i) = Val_{\nu^\sigma}(p_i)$.

È anche possibile dimostrare il teorema procedendo per induzione sulle formule, senza ricorrere al teorema 2.5.2: la facile dimostrazione è lasciata al lettore. Il corollario seguente permette di concepire ogni tautologia come una forma da cui è possibile ricavare per sostituzione un numero infinito di tautologie.

Corollario 3.5.2 *Per ogni formula α e ogni sostituzione σ, se α è una tautologia allora anche $So_\sigma(\alpha)$ lo è.*

Basta osservare che, al variare di ν, $Val_{\nu^\sigma}(\alpha) = 1$, poiché α è una tautologia e quindi, per il teorema, anche $Val_\nu(So_\sigma(\alpha)) = 1$.

Teorema 3.5.3 *Siano α, β e ν tali che $Val_\nu(\alpha) = Val_\nu(\beta)$. Se σ_0 e σ_1 sono due sostituzioni tali che $\sigma_0(p_i) = \alpha$ e $\sigma_1(p_i) = \beta$ e per ogni $j \neq i$, $\sigma_0(p_j) = \sigma_1(p_j)$, allora per ogni formula γ,*

$$Val_\nu(So_{\sigma_0}(\gamma)) = Val_\nu(So_{\sigma_1}(\gamma)).$$

Occorre dimostrare che $Val_\nu \circ So_{\sigma_0} = Val_\nu \circ So_{\sigma_1}$ e, come nel teorema precedente, possiamo ridurci a dimostrare che, per ogni $j \in \omega$,

$$Val_\nu(So_{\sigma_0}(p_j) = Val_\nu(So_{\sigma_1}(p_j).$$

Se $j \neq i$ allora $So_{\sigma_0}(p_j) = So_{\sigma_1}(p_j)$, perché per ipotesi $\sigma_0(p_j) = \sigma_1(p_j)$, e da ciò segue subito l'asserto. Se $j = i$ allora $So_{\sigma_0}(p_j) = \alpha$ e $So_{\sigma_1}(p_j) = \beta$, ma allora per ipotesi $Val_\nu(\alpha) = Val_\nu(\beta)$.

Corollario 3.5.4 *Se α e β sono equivalenti e se le sostituzioni σ_0 e σ_1 sono come nel teorema precedente, allora anche $So_{\sigma_0}(\gamma)$ e $So_{\sigma_1}(\gamma)$ sono equivalenti.*

È chiaro che se α e β sono equivalenti allora $M(\alpha) = M(\beta)$ e quindi, per il teorema 3.3.1, $Val_\nu(\alpha) = Val_\nu(\beta)$ per ogni ν, ma allora, per il teorema precedente, anche $So_{\sigma_0}(\gamma)$ e $So_{\sigma_1}(\gamma)$ sono equivalenti.

Il corollario seguente è di importanza fondamentale perché garantisce che il rimpiazzamento di formule equivalenti non muta il significato della formula al cui interno il rimpiazzamento viene compiuto.

Corollario 3.5.5 *Se α occorre in β, α' è una formula equivalente ad α e β' è ottenuta da β rimpiazzando in essa un'occorrenza di α con α', allora β è equivalente a β'.*

Sia (x, y) la sezione relativa alla data occorrenza di α in β e quindi sia $\beta = x * \alpha * y$. Consideriamo $\gamma = x * p_k * y$, dove p_k è una variabile che non occorre in β. Possiamo descrivere il risultato β' del rimpiazzamento di quella occorrenza di α in β mediante α' in termini di sostituzioni nel modo seguente. Definiamo σ_0 e σ_1 in modo tale che siano l'identità su tutte le variabili diverse da p_k, mentre porremo

$$\sigma_0(p_k) = \alpha \text{ e } \sigma_1(p_k) = \alpha'.$$

Abbiamo sia $So_{\sigma_0}(\gamma) = \beta$ sia $So_{\sigma_1}(\gamma) = \beta'$, quindi, per il corollario precedente, se α è equivalente ad α' allora β è equivalente a β'.

Il teorema seguente illustra i rapporti tra l'operazione di sostituzione sul piano sintattico e l'operazione di composizione di funzioni sul piano semantico.

Teorema 3.5.6 *Se α è una formula k-aria e $\beta_0, ..., \beta_{k-1}$ sono formule n-arie, allora*

$$f^n_{\alpha(\beta_0,...,\beta_{n-1})} = Comp^n_k(f^k_\alpha, g^n_{\beta_0}, ..., g^n_{\beta_{n-1}}).$$

Sia $s \in 2^n$ e sia ν una valutazione coincidente con s sui primi n posti, ossia $\nu \restriction n = s$. Sia σ una sostituzione tale che $\sigma(p_i) = \beta_i$ per $i < k$. Abbiamo allora

$$\nu^\sigma(i) = Val_\nu(\sigma(p_i)) = Val_\nu(\beta_i) = f_{\beta_i}(\nu) = f^n_{\beta_i}(\nu \restriction n),$$

dove l'ultimo passaggio deriva dal corollario 3.4.4. Abbiamo allora

$$\begin{aligned} Comp^n_k(f^k_\alpha, g^n_{\beta_0}, \ldots, g^n_{\beta_{k-1}})(s) &= Comp^n_k(f^k_\alpha, g^n_{\beta_0}, \ldots, g^n_{\beta_{k-1}})(\nu \restriction n) \\ &= f^k_\alpha(f^n_{\beta_0}(\nu \restriction n), \ldots, f^n_{\beta_{k-1}}(\nu \restriction n)) \\ &= f^k_\alpha(\nu^\sigma(0), \ldots, \nu^\sigma(k-1)) \\ &= f^k_\alpha(\nu^\sigma \restriction k) \\ &= f_\alpha(\nu^\sigma). \end{aligned}$$

Ricordando che $Val_{\nu^\sigma}(\alpha) = Val_\nu(\alpha(\beta_0, \ldots, \beta_{k-1}))$ per il teorema 3.5.1, abbiamo che $\nu^\sigma \in M(\alpha)$ sse $\nu \in M(\alpha(\beta_0, \ldots, \beta_{k-1}))$, per il teorema 3.3.1, e quindi

$$\begin{aligned} f_\alpha(\nu^\sigma) &= f_{\alpha(\beta_0, \ldots, \beta_{k-1})}(\nu) \\ &= f^n_{\alpha(\beta_0, \ldots, \beta_{k-1})}(\nu \restriction n) \\ &= f^n_{\alpha(\beta_0, \ldots, \beta_{k-1})}(s). \end{aligned}$$

Da questo teorema si ottiene immediatamente un'altra dimostrazione del fatto che la sostituzione trasforma tautologie in tautologie.

Esercizio 3.5.1 Elencare le formule α e le sostituzioni σ tali che $So_\sigma(\alpha) = p_0 \wedge (\neg p_1 \vee p_0)$.

Esercizio 3.5.2 Il rimpiazzamento trasforma sempre tautologie in tautologie?

3.6 Conseguenza logica

A questo punto possiamo ritornare al tema fondamentale del nostro discorso: la teoria dell'inferenza e la nozione di conseguenza logica. In prima istanza abbiamo definito un'inferenza corretta quando tra premesse e conclusione dell'inferenza sussiste una relazione di conseguenza logica, ossia se in ogni circostanza in cui le premesse sono vere anche la conclusione risulta vera. Se identifichiamo l'insieme delle circostanze in cui una formula è vera con l'insieme delle valutazioni per cui risulta vera, ossia con il suo significato, possiamo allora dire che β è *conseguenza logica* di α, in simboli $\alpha \models \beta$, se $M(\alpha) \subseteq M(\beta)$. Vale a dire, $\alpha \models \beta$ sse ogni valutazione che rende vera α rende vera anche β, ossia ogni modello di α è anche modello di β. Ad esempio, si verifica facilmente che $p_0 \models p_0 \vee p_1$, dato che $M(p_0) \subseteq M(p_0) \cup M(p_1)$.

Se vogliamo estendere il concetto di conseguenza logica al caso in cui vi siano più premesse, occorre estendere la funzione M a insiemi di formule: poniamo

allora, per ogni $\Gamma \subseteq Fm$, $M(\Gamma) = \bigcap\{M(\alpha) : \alpha \in \Gamma\}$. Quindi il significato di un insieme di formule è l'intersezione dei significati delle formule che lo compongono, l'insieme dei modelli comuni. In particolare, quando Γ è l'insieme finito $\{\alpha_0, \ldots, \alpha_{n-1}\}$ abbiamo $M(\Gamma) = M(\alpha_0) \cap \ldots \cap M(\alpha_{n-1})$. Diremo che una valutazione ν è *modello* di Γ, indicandolo con $\nu \models \Gamma$, quando $\nu \in M(\Gamma)$: quindi una valutazione è modello di un insieme di formule quando è modello di ogni formula dell'insieme. Diremo che un insieme di formule Γ è *soddisfacibile* se esiste un ν tale che $\nu \models \Gamma$. (La notazione $\nu \models \alpha$ introdotta nel paragrafo precedente può essere vista come un'abbreviazione di $\nu \models \{\alpha\}$.)

Possiamo ora definire la nozione generale di conseguenza logica nel modo seguente: β è conseguenza logica dell'insieme di premesse Γ, in simboli $\Gamma \models \beta$, se $M(\Gamma) \subseteq M(\beta)$. (Quando Γ è un insieme finito, scriveremo semplicemente $\alpha_0, \ldots, \alpha_{n-1} \models \beta$ invece di $\{\alpha_0, \ldots, \alpha_{n-1}\} \models \beta$.) In altri termini, β è conseguenza logica di Γ sse ogni valutazione che renda vera simultaneamente ogni formula $\alpha \in \Gamma$ rende vera anche β, ossia ogni modello di Γ è modello di β. In particolare, β è conseguenza logica di $\alpha_0, \ldots, \alpha_{n-1}$ sse $M(\alpha_0) \cap \ldots \cap M(\alpha_{n-1}) \subseteq M(\beta)$ e nel caso di $n = 1$ riotteniamo la nozione iniziale. Il concetto di conseguenza logica è di importanza fondamentale e richiede alcune osservazioni.

1) Non bisogna confondere l'uso del simbolo $\models$ nell'esprimere la relazione tra valutazioni e formule, $\nu \models \beta$, ossia ν è modello di β, con l'uso appena introdotto per indicare la relazione di conseguenza logica tra insiemi di formule e singole formule.

2) Non bisogna confondere i significati di $\models$ e $\rightarrow$. Il simbolo $\rightarrow$ serve per costruire formule del linguaggio oggetto, ossia del linguaggio formale $\mathcal{L}$, come $\alpha \rightarrow \beta$. Il simbolo $\models$ fa parte del metalinguaggio, ossia del linguaggio naturale, e serve per costruire asserzioni dotate di un significato intuitivo come $\alpha \models \beta$, che semplicemente abbrevia "β è conseguenza logica di α".

3) Bisogna considerare attentamente la struttura della definizione di conseguenza logica $\Gamma \models \beta$: per ogni ν (se per ogni $\alpha \in \Gamma$ accade che $\nu \models \alpha$, allora $\nu \models \beta$). Si osservi che il primo "per ogni" riguarda tutta l'implicazione tra parentesi ed è una quantificazione su valutazioni, mentre il secondo riguarda solo l'antecedente dell'implicazione ed è una quantificazione sulle formule di Γ. Quando $\Gamma = \{\alpha\}$ il secondo "per ogni" scompare e asserire $\alpha \models \beta$ significa semplicemente asserire che, per ogni valutazione ν, se $\nu \models \alpha$ allora $\nu \models \beta$. Quando $\Gamma = \{\alpha_0, \ldots, \alpha_{n-1}\}$ possiamo leggere il secondo "per ogni" come una congiunzione finita e asserire $\alpha_0, \ldots, \alpha_{n-1} \models \beta$ significa asserire che, per ogni ν, se ($\nu \models \alpha_1$ e $\ldots$ e $\nu \models \alpha_{n-1}$) allora $\nu \models \alpha$.

4) Per quanto riguarda il primo "per ogni", non bisogna commettere l'errore di distribuirlo sull'antecedente e il conseguente dell'implicazione, leggendo $\alpha \models \beta$ come se fosse: *se* per ogni ν, $\nu \models \alpha$, *allora* per ogni ν, $\nu \models \beta$. Ciò equivarrebbe ed asserire: se $\models \alpha$ allora $\models \beta$, ossia se α è una tautologia allora β è una tautologia. È facile vedere che se $\alpha \models \beta$ allora "se α è una tautologia allora β è una tautologia": infatti se α è una tautologia abbiamo $M(\alpha) = 2^\omega$ e quindi, essendo $M(\alpha) \subseteq M(\beta)$, anche $M(\beta) = 2^\omega$, quindi anche β è una tautologia. Non vale invece l'implicazione inversa: ad esempio, se p_0 è una tautologia allora anche p_1 è una tautologia, ma non vale $p_0 \models p_1$.

5) Per quanto riguarda il secondo "per ogni", se per una data valutazione ν accade che non tutte le premesse $\alpha \in \Gamma$ sono vere in ν, allora l'implicazione (se per ogni $\alpha \in \Gamma$ accade che $\nu \models \alpha$ allora $\nu \models \beta$) è vera. Se ciò accade per tutte le valutazioni, ossia se $M(\Gamma)$ è vuoto, ad esempio perché Γ contiene sia α che $\neg\alpha$, allora $\Gamma \models \beta$ qualunque sia β.

Illustriamo la nozione di conseguenza logica con un esempio. Si verifica facilmente che

$$p_0 \vee p_1, p_2 \to \neg p_1, p_2 \models p_0,$$

poiché $M(p_0 \vee p_1) \cap M(p_2 \to \neg p_1) \cap M(p_2)$, vale a dire $(M(p_0) \cup M(p_1)) \cap (-M(p_2) \cup -M(p_1)) \cap M(p_2)$, è incluso in $M(p_0)$. Per verificarlo basta dimostrare che nell'algebra Boole vale $(x \vee y) \wedge (\neg z \vee \neg y) \wedge z \leq x$. Infatti

$$\begin{aligned}
(x \vee y) \wedge (\neg z \vee \neg y) \wedge z &= (x \vee y) \wedge ((\neg z \wedge z) \vee (\neg y \wedge z)) \\
&= (x \vee y) \wedge (\neg y \wedge z) \\
&= (x \wedge \neg y \wedge z) \vee (y \wedge \neg y \wedge z) \\
&= x \wedge \neg y \wedge z \\
&\leq x.
\end{aligned}$$

Quando l'insieme delle premesse è finito si può verificare se sussiste la relazione di conseguenza utilizzando il significato finitario delle formule: per verificare se $\alpha_0, \ldots, \alpha_{n-1} \models \beta$ possiamo considerare il minimo n tale che le formule coinvolte nella conseguenza logica siano tutte n-arie e limitarci a verificare se $M^n(\alpha_0) \cap \ldots \cap M^n(\alpha_{n-1}) \subseteq M^n(\beta)$. Infatti $M(\alpha_0) \cap \ldots \cap M(\alpha_{n-1}) \subseteq M(\beta)$ sse $M(\alpha_0 \wedge \ldots \wedge \alpha_{n-1}) \subseteq M(\beta)$, d'altra parte per l'esercizio 3.4.1 quest'ultima inclusione equivale a $M^n(\alpha_0 \wedge \ldots \wedge \alpha_{n-1}) \subseteq M^n(\beta)$ che a sua volta equivale a $M^n(\alpha_0) \cap \ldots \cap M^n(\alpha_{n-1}) \subseteq M^n(\beta)$.

$p_0 \vee p_1$	$p_2 \to \neg p_1$	p_2	p_0
111		111	111
110	110		110
101	101	101	101
100	100		100
011		011	
010	010		
	001	001	
	000		

La tabella precedente riporta sotto a ogni formula i suoi modelli e si vede chiaramente che l'insieme dei modelli delle premesse è incluso nell'insieme dei modelli della conclusione. Il teorema seguente mostra il fondamentale rapporto che esiste tra conseguenza logica e implicazione.

Teorema 3.6.1 *$\Gamma, \alpha \models \beta$ sse $\Gamma \models \alpha \to \beta$.*

Valgono le equivalenze

$$\begin{aligned}\Gamma, \alpha \models \beta \qquad & \text{sse } M(\Gamma) \cap M(\alpha) \subseteq M(\beta)\\ & \text{sse } M(\Gamma) \subseteq -M(\alpha) \cup M(\beta)\\ & \text{sse } M(\Gamma) \subseteq M(\neg\alpha \vee \beta)\\ & \text{sse } \Gamma \models \alpha \to \beta,\end{aligned}$$

dove il passaggio dalla prima alla seconda riga è giustificato dal punto 6) del teorema 2.4.5.

Il teorema seguente mostra che la verifica della correttezza di un'inferenza con un numero finito di premesse si riduce a controllare se una certa formula sia una tautologia. È quindi fondamentale saper riconoscere le tautologie, perché in esse sono condensate tutte le forme di inferenze corrette. (Nel paragrafo 3.11 dimostreremo che ogni inferenza corretta da un insieme infinito di premesse è riducibile a un'inferenza corretta da un sottoinsieme finito di tali premesse.)

Teorema 3.6.2 *Le asserzioni seguenti sono equivalenti:*

1. $\alpha_0, \ldots, \alpha_{n-1} \models \beta$,
2. $\alpha_0 \wedge \ldots \wedge \alpha_{n-1} \models \beta$,
3. $\models \alpha_0 \wedge \ldots \wedge \alpha_{n-1} \to \beta$,
4. $\models \alpha_0 \to (\alpha_1 \to \ldots (\alpha_{n-1} \to \beta) \ldots)$.

La 1) equivale alla 2) perché $M(\{\alpha_0, \ldots, \alpha_{n-1}\}) = M(\alpha_0) \cap \ldots \cap M(\alpha_{n-1})$. La 2) equivale alla 3) per il teorema precedente: basta porre $\Gamma = \emptyset$. Per verificare che la 3) equivale alla 4) basta dimostrare che le due formule sono equivalenti e a tale scopo basta verificare che $-(X_0 \cap \ldots \cap X_{n-1}) \cup Y = -X_0 \cup (-X_1 \cup \ldots \cup (-X_{n-1} \cup Y) \ldots)$, ciò si ottiene dalla legge di De Morgan.

Si osservi che $\emptyset \models \beta$ sse β è una tautologia. Infatti le premesse α_i, quando sono presenti, restringono le valutazioni ν che devono rendere vera β a quelle che rendono vere tutte le α_i: se l'insieme delle premesse è vuoto, non si opera alcuna limitazione e ogni valutazione deve rendere vera β, che quindi risulta essere una tautologia. Allo stesso risultato arriviamo osservando che $M(\emptyset) = \bigcap\{M(\alpha) : \alpha \in \emptyset\} = \bigcap \emptyset = 2^\omega$.

Proponiamo di analizzare il concetto intuitivo di inferenza corretta in questi termini: se rappresentiamo con $\alpha_0, \ldots, \alpha_{n-1}$ le premesse di un'inferenza e con β la conclusione, diremo che l'inferenza è corretta se la conclusione è conseguenza logica delle premesse. Vediamo ora all'opera questa analisi in un caso concreto. Consideriamo i seguenti quattro enunciati:

Antonio ama Maria o Antonio ama Sara	$p_0 \vee p_1$
Se Antonio ama Maria allora Antonio tradisce Sara	$p_0 \to p_2$
Se Antonio ama Sara allora Antonio tradisce Maria	$p_1 \to p_3$
Antonio tradisce Sara o Antonio tradisce Maria	$p_2 \vee p_3$

Possiamo rappresentare il legame inferenziale che sussiste tra l'insieme dei primi tre enunciati, le premesse, e il quarto, la conclusione, con

$$p_0 \vee p_1 , p_0 \to p_2 , p_1 \to p_3 \models p_2 \vee p_3 .$$

Per verificare l'esistenza di questo legame inferenziale possiamo controllare se nell'algebra di Boole valga

$$(x \vee y) \wedge (\neg x \vee z) \wedge (\neg y \vee w) \leq z \vee w,$$

oppure possiamo applicare il teorema precedente e verificare se

$$(p_0 \vee p_1) \wedge (p_0 \to p_2) \wedge (p_1 \to p_3) \to (p_2 \vee p_3)$$

sia una tautologia. Lasciamo al lettore queste verifiche che in ogni caso confermano la correttezza dell'inferenza. (Si veda l'esercizio 3.6.1.) Quello che ci preme sottolineare è la natura logica del legame individuato tra premesse e conclusioni. L'inferenza risulta corretta indipendentemente dal fatto che si tratti di Antonio, di Maria, di amore e tradimento. Non solo questi contenuti sono indifferenti, ma la stessa verità o falsità delle asserzioni coinvolte è irrilevante per la correttezza dell'inferenza. Infatti un'inferenza corretta stabilisce un legame tra premesse e conclusione che è indipendente da come va il mondo e indipendente dal significato relativo a una particolare valutazione delle formule coinvolte. Il legame tra premesse e conclusione deve essere di natura logica e quindi deve sussistere in ogni possibile circostanza, deve essere compatibile con ogni significato relativo. Le formule del linguaggio formale sono particolarmente adatte ad esprimere ciò che rimane dopo questo processo di astrazione, perché in esse non c'è più traccia dei contenuti specifici degli enunciati del linguaggio naturale. Una volta rappresentata nel linguaggio formale, l'inferenza perde la sua specificità e diventa uno schema d'inferenza, poiché le variabili enunciative che vi compaiono possono essere sostituite con enunciati qualsiasi del linguaggio naturale, ottenendo in ogni caso un'inferenza corretta.

Passiamo ora a studiare la relazione di conseguenza logica all'interno di un discorso più generale riguardante il rapporto tra linguaggio e realtà. Tale rapporto può presentarsi in due modi opposti e complementari. Se lo assumiamo nella direzione dal linguaggio verso la realtà, utilizziamo le formule del linguaggio per imporre condizioni a cui la realtà deve conformarsi, per caratterizzare un certo ambito di realtà. Agiamo in questo modo quando fissiamo un insieme di leggi a cui deve sottostare un insieme di oggetti, per configurare una situazione che potremmo chiamare un "modello" di tali leggi. Se lo assumiamo nella direzione opposta, immaginiamo che vi sia anzitutto una realtà che vogliamo descrivere nei termini delle formule del nostro linguaggio e quindi consideriamo come questa realtà si rifletta in tali formule. Quindi in un caso le formule hanno funzione normativa nei confronti della realtà, nell'altro sono utilizzate per rispecchiare una realtà che si è già costituita in modo indipendente: in un caso il modello è qualcosa da sintetizzare a partire dal linguaggio di cui si dispone, nell'altro il modello è all'origine di una serie di asserzioni formulate entro il linguaggio. Lo

studio di questo rapporto è uno degli aspetti fondamentali della logica e si può presentare a diversi livelli di complessità, secondo il tipo di linguaggio adottato. In questo paragrafo esamineremo il caso del linguaggio enunciativo $\mathcal{L}$ e intenderemo come "realtà descrivibile da $\mathcal{L}$" una qualsiasi valutazione $\nu : P \to 2$ o un insieme di tali valutazioni.

Consideriamo dapprima il rapporto nella direzione dalla realtà verso il linguaggio definendo una funzione $Th : P(2^\omega) \to P(Fm)$ tale che, per ogni $X \subseteq 2^\omega$,

$$Th(X) = \{\alpha : \nu \models \alpha, \text{ per ogni } \nu \in X\}.$$

Diremo che $Th(X)$ è la *teoria di* X, una descrizione che si attaglia ad ogni particolare $\nu \in X$, anzi, la più esauriente di tali descrizioni. In particolare, quando $X = \{\nu\}$ scriveremo $Th(\nu)$ per indicare l'insieme delle formule vere in ν. È facile verificare che Th è una funzione antitona, ossia che $X \subseteq Y$ implica $Th(Y) \subseteq Th(X)$: se si dilata l'insieme delle valutazioni, l'insieme delle realtà prese in esame, si contrae l'insieme delle verità comuni ad ogni valutazione, la teoria corrispondente alle realtà considerate. Nei casi limite, quando X è $\emptyset$, $Th(X)$ è Fm, la teoria banale che contiene ogni formula, e quando X è 2^ω, $Th(X)$ è l'insieme delle tautologie, la teoria minima.

Per quanto riguarda il rapporto nell'altra direzione, dal linguaggio verso la realtà, disponiamo già della funzione $M : P(Fm) \to P(2^\omega)$ tale che, per ogni $\Gamma \subseteq Fm$,

$$M(\Gamma) = \{\nu : \nu \models \alpha, \text{ per ogni } \alpha \in \Gamma\}.$$

Diremo che $M(\Gamma)$ è la *classe assiomatica di* Γ, l'insieme delle realtà descritte da Γ. Quando Γ contiene un unico enunciato parleremo di *classe elementare*. Si verifica facilmente che M è una funzione antitona, ossia che $\Gamma \subseteq \Sigma$ implica $M(\Sigma) \subseteq M(\Gamma)$: se si dilata l'insieme delle realtà, si contrae l'insieme delle verità condivise da tali realtà. È facile stabilire una condizione necessaria e sufficiente perché sia $M(\Gamma) = 2^\omega$: basta richiedere che Γ sia $\emptyset$ o un insieme di tautologie. Più difficile è stabilire un'analoga condizione per $M(\Gamma) = \emptyset$. Potremo ottenerne una dal teorema di completezza, per ora possiamo accontentarci di una condizione sufficiente: esiste una formula α tale che $\alpha, \neg\alpha \in \Gamma$.

Vi sono dunque formule che non hanno alcun effetto di caratterizzazione sulla realtà: le tautologie e le contraddizioni. In secondo luogo osserviamo che nessuna formula può caratterizzare un unico modello, anzi, per ogni formula α, se l'insieme dei modelli di α non è vuoto, allora è infinito. Ciò accade perché le variabili occorrenti in una formula α sono sempre in numero finito e per il teorema 3.4.2 tutte le valutazioni coincidenti sulle variabili di α sono equivalenti rispetto alla soddisfacibilità di α. Un discorso analogo vale anche per gli insiemi finiti. Infatti è chiaro che ν è modello dell'insieme $\{\alpha_0, \ldots, \alpha_{n-1}\}$ sse è modello della formula $\alpha_0 \wedge \ldots \wedge \alpha_{n-1}$, quindi la capacità di caratterizzare di un insieme finito equivale a quella di una singola formula. Con un Γ infinito è evidentemente possibile forzare la scelta di un'unica realtà. Ad esempio, $\Gamma = P$ caratterizza il modello ν costituito dalla funzione costante 1. È facile stabilire una condizione

su Γ che garantisca l'unicità della realtà descritta. Diremo che un insieme Γ di formule è *completo* se, per ogni formula α, $\alpha \in \Gamma$ o $\neg\alpha \in \Gamma$. Un esempio di insieme completo è $Th(\nu)$, per ogni ν. Si verifica facilmente che se Γ è completo allora, se ha un modello, ne ha uno solo. Supponiamo infatti che Γ abbia due modelli ν e ν'. Poiché Γ è completo, per ogni variabile avremo $p_i \in \Gamma$ o $\neg p_i \in \Gamma$. Se $p_i \in \Gamma$ avremo $\nu(i) = 1 = \nu'(i)$ e se $\neg p_i \in \Gamma$ avremo $\nu(i) = 0 = \nu'(i)$, quindi $\nu = \nu'$. Si osservi che un insieme completo può non avere modelli, ad esempio quando contiene sia p_i che $\neg p_i$..

Le funzioni Th e M mettono dunque in relazione la realtà con il linguaggio e il linguaggio con la realtà. Se consideriamo le funzioni composte $M \circ Th$ e $Th \circ M$ otteniamo rispettivamente una funzione da $P(2^\omega)$ in se stesso e da $P(Fm)$ in se stesso. Innanzitutto osserviamo che, essendo Th e M antitone, le funzioni composte $M \circ Th$ e $Th \circ M$ sono monotone. Inoltre $M \circ Th$ e $Th \circ M$ sono evidentemente progressive, ossia $X \subseteq M(Th(X))$ e $\Gamma \subseteq Th(M(\Gamma))$. Il teorema seguente dimostra che ogni $M(\Gamma)$ è un punto fisso della funzione $M \circ Th$ e ogni $Th(X)$ è un punto fisso della funzione $Th \circ M$.

Teorema 3.6.3 *Per ogni $\Gamma \subseteq Fm$ e per ogni $X \subseteq {}^\omega 2$,*

1. $M(Th(M(\Gamma))) = M(\Gamma)$,
2. $Th(M(Th(X))) = Th(X)$.

Dimostriamo la 1). Poiché $M \circ Th$ è progressiva, $M(\Gamma) \subseteq M(Th(M(\Gamma)))$. Poiché $Th \circ M$ è progressiva, $\Gamma \subseteq Th(M(\Gamma))$ e quindi $M(Th(M(\Gamma))) \subseteq M(\Gamma)$ poiché M è antitona. La 2) si dimostra in modo analogo.

Se ora restringiamo $P(2^\omega)$ all'insieme $A = \{M(\Gamma) : \Gamma \subseteq Fm\}$ contenente solo le classi di modelli che sono classi assiomatiche, e parallelamente restringiamo $P(Fm)$ all'insieme $B = \{Th(X) : X \subseteq 2^\omega\}$, contenente solo gli insiemi di formule che sono teorie di qualche classe di modelli, si vede facilmente che Th e M sono l'una inversa dell'altra e che tali funzioni stabiliscono una biiezione tra A e B.

Vediamo ora come si inserisce in questo discorso la relazione di conseguenza logica. Innanzitutto definiamo una funzione $Cn : P(Fm) \to P(Fm)$ ponendo, per ogni $\Gamma \subseteq Fm$, $Cn(\Gamma) = \{\alpha : \Gamma \models \alpha\}$. Possiamo considerare $Cn(\Gamma)$ come l'insieme di tutte le conoscenze che sono ricavabili dalle (o riconducibili alle) formule Γ, l'esplicitazione di tutto ciò che è implicito in Γ. È possibile definire Cn nei termini di Th e M.

Teorema 3.6.4

$$Cn(\Gamma) = Th(M(\Gamma)).$$

Se $\alpha \in Cn(\Gamma)$ allora $M(\Gamma) \subseteq M(\alpha)$ e quindi $Th(M(\alpha)) \subseteq Th(M(\Gamma))$, essendo Th antitona. Ma $\alpha \in Th(M(\alpha))$ e quindi $\alpha \in Th(M(\Gamma))$. Supponiamo ora $\alpha \in Th(M(\Gamma))$, allora $\{\alpha\} \subseteq Th(M(\Gamma))$ e quindi, poiché M è antitona vale $M(Th(M(\Gamma))) \subseteq M(\alpha)$. Per il teorema precedente $M(Th(M(\Gamma))) = M(\Gamma)$ e quindi $M(\Gamma) \subseteq M(\alpha)$ da cui si ricava $\Gamma \models \alpha$.

Da questo teorema e dalle proprietà di $Th \circ M$ messe in luce in precedenza si ricava immediatamente che Cn è una funzione progressiva e monotona. Ciò collima con la nozione intuitiva di conseguenza logica, infatti aumentando l'insieme delle premesse l'insieme delle conseguenze non può diminuire e ogni premessa è sempre ottenibile come conseguenza. Inoltre risulta chiaro che è inutile iterare Cn nella speranza di ottenere nuove conseguenze, perché $Cn(Cn(\Gamma)) = Cn(\Gamma)$, ossia ogni insieme di formule $Cn(\Gamma)$ è un punto fisso di Cn: infatti dal teorema precedente e dal teorema 3.6.3 si ricava immediatamente $Th(M(Th(M(\Gamma)))) = Th(M(\Gamma))$.

Possiamo concepire una teoria come un sistema di conoscenze che contiene tutto ciò che è ricavabile con strumenti puramente logici da un insieme di enunciati considerati come assiomi della teoria. Da questo punto di vista una teoria non è caratterizzata dai suoi assiomi, di fatto la stessa teoria si può ottenere da differenti insiemi di assiomi, ma dal costituire un insieme di conoscenze che ha raggiunto una condizione di equilibrio, che non ammette crescite ulteriori. Ciò non significa che una teoria non possa essere estesa con ulteriori conoscenze, ma che queste estensioni, ove possibili, non sono più un fatto logico. Diremo allora che un insieme di formule T è una *teoria* se è chiuso rispetto alla conseguenza logica, ossia per ogni formula α, se $T \models \alpha$, allora $\alpha \in T$. In altri termini, T è una teoria se è un punto fisso di Cn, ovvero se $T = Cn(T)$.

L'insieme $Cn(\Gamma)$ è sempre una teoria, per ogni Γ, dato che è un punto fisso di Cn. La più piccola delle teorie è $Cn(\emptyset)$, l'insieme delle tautologie, e la più grande $Cn(Fm) = Fm$, la teoria banale che contiene ogni possibile asserzione. Si osservi che quando per qualche formula α vale sia $\alpha \in Cn(\Gamma)$ sia $\neg\alpha \in Cn(\Gamma)$, allora $Cn(\Gamma) = Fm$. Infatti se accade che $\Gamma \models \alpha$ e $\Gamma \models \neg\alpha$, allora Γ non ha modelli. (Se vi fosse un modello di Γ, dovrebbe essere sia modello di α sia modello di $\neg\alpha$, ma ciò è impossibile.) Se Γ non ha modelli, allora è banalmente vero che $\Gamma \models \alpha$, per ogni $\alpha \in Fm$.

Non bisogna confondere questa nozione di teoria come punto fisso di Cn, con $Th(X)$, la teoria di X, l'insieme degli enunciati veri in ogni valutazione di X. Tuttavia i due concetti di teoria sono strettamente legati. Da un lato, se Γ è una teoria, ossia $Cn(\Gamma) = \Gamma$, allora esiste un insieme di valutazioni X tale che $\Gamma = Th(X)$. Infatti, per il teorema precedente, basta porre $X = M(\Gamma)$. Dall'altro, la teoria di X è un punto fisso di Cn e quindi è una teoria. Infatti per il teorema precedente e il teorema 3.6.3,

$$Cn(Th(X)) = Th(M(Th(X))) = Th(X).$$

Se T è una teoria possiamo porci il problema dell'individuazione di un insieme di formule Γ che generi T mediante conseguenze logiche, ossia tale che $T = Cn(\Gamma)$: diremo che un Γ siffatto è un *insieme di assiomi* per T, ovvero *assiomatizza* T. È chiaro che si può sempre assiomatizzare in modo banale una teoria T adottando T stessa come insieme di assiomi, poiché vale $Cn(T) = T$. Diremo che T è *finitamente assiomatizzabile* se è assiomatizzata da un Γ finito. A questo proposito osserviamo che, se T è assiomatizzabile da $\Gamma = \{\alpha_0, \ldots, \alpha_{n-1}\}$, allora T è assiomatizzabile dalla singola formula $\alpha_0 \wedge \ldots \wedge \alpha_{n-1}$: infatti Γ e

$\alpha_0 \wedge \ldots \wedge \alpha_{n-1}$ hanno le stesse conseguenze. Questo discorso non è estendibile agli insiemi infiniti di assiomi, perché il nostro linguaggio non ammette formule infinite.

Esercizio 3.6.1 Si dimostri che nell'algebra di Boole vale:

1. $(x \vee y) \wedge (\neg x \vee z) \leq z \vee y$,
2. $(z \vee y) \wedge (\neg y \vee w) \leq z \vee w$,
3. $((x \vee y) \wedge (\neg x \vee z)) \wedge (\neg y \vee w) \leq (z \vee y) \wedge (\neg y \vee w) \leq z \vee w$.

Si concluda che $p_0 \vee p_1, p_0 \to p_2, p_1 \to p_3 \models p_2 \vee p_3$.

Esercizio 3.6.2 Si dimostri che

1. $\alpha \wedge \neg\alpha \models \beta$,
2. $\alpha \models \beta \vee \neg\beta$,
3. se $\alpha \vee \neg\alpha \models \beta$ allora β è una tautologia e se $\alpha \models \beta \wedge \neg\beta$ allora α è una contraddizione.

Esercizio 3.6.3 Verificare se la conseguenza logica sussiste:

1. $p_0 \to p_1 \models p_0 \wedge p_1$
2. $p_0 \to (p_1 \to p_2), p_0 \to p_1 \models p_0 \to p_2$
3. $p_0 \to \neg p_1, \neg p_2, p_1 \to (p_0 \vee p_2) \models \neg p_1$
4. $(p_0 \to p_1) \vee (p_0 \wedge \neg p_1) \models p_0$
5. $p_0 \vee p_1, p_2 \leftrightarrow p_3, \neg p_0 \wedge p_3 \models \neg p_3 \vee \neg p_1$
6. $\neg p_0 \wedge p_1, p_0 \vee \neg p_2, p_3 \to \neg p_1 \models p_2 \wedge \neg p_3$.

Esercizio 3.6.4 Tradurre le seguenti inferenze nel linguaggio formale individuando un insieme $\alpha_0, \ldots, \alpha_{n-1}$ di premesse e una conclusione α. Verificare se l'inferenza è corretta.

1. Se c'è una perdita nel radiatore, allora l'olio si surriscalda e la pressione dell'olio si abbassa. Se la pressione dell'olio si abbassa i cuscinetti possono essere danneggiati. Quindi se c'è una perdita nel radiatore i cuscinetti possono essere danneggiati.
2. Se fossi colpevole sarei stato a New York al momento del delitto. Se ciò fosse vero, sul mio passaporto dovrebbe esserci un visto d'ingresso negli Stati Uniti. Ma non è così, quindi non sono colpevole.