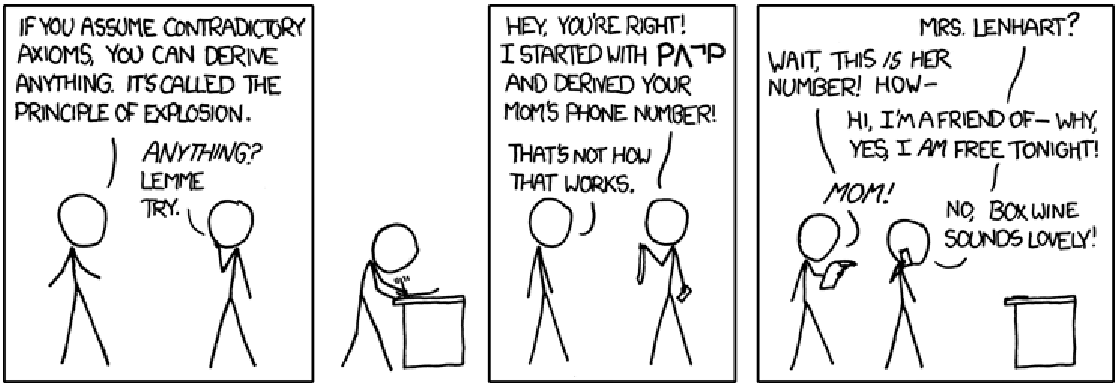
LOGICA MATEMATICA

SERAFINA LAPENTA E LUCA SPADA



per il corso di laurea triennale in Matematica

Gennaio 2024 – version 6.5

INDICE

Modifiche nella versione 6.5: (14 marzo 2024).

- Corretti alcuni refusi nel testo.

Nota per il lettore. Queste dispense sono state scritte molto frettolosamente dagli autori mentre tenevano i corsi di *Logica Matematica* per la laurea triennale in Matematica presso l'Università di Salerno e *Logica* per la laurea triennale e magistrale in Matematica presso l'Università della Basilicata. Sono state scritte perché gli autori non sono riusciti a trovare nessun libro che trattasse tutti gli argomenti presentati nei corsi (ad esempio l'intersezione dei libri che parlano approfonditamente di algebre di Boole con quelli che discutono la deduzione naturale sembrerebbe essere vuota).

Si ringraziano per gli utili consigli e le segnalazioni: Marco D'Angelo, Michele Victor Esposito, Antonio Messano, Fernanda Moccia, Luigi Riccio, Sara Vannucci

Chiunque dovesse notare errori, imprecisioni o volesse lasciare semplicemente dei commenti può scrivere a `luca.spada@gmail.com`.

PANORAMICA DEL CORSO

Questo corso è pensato come introduzione alla Logica Matematica e quindi allo studio del linguaggio e del ragionamento formale. Gli obiettivi del corso sono:

1. consapevolezza nel riconoscimento e l'uso delle regole logiche;
2. capacità di formalizzazione di informazioni in un linguaggio formale;
3. sviluppo e verifica di ragionamenti corretti;
4. conoscenza del linguaggio della logica proposizionale e del prim'ordine e dei loro principali algoritmi deduttivi;
5. conoscenza delle principali tecniche dimostrative in logica.

Gli argomenti principali del corso sono:

1. la sintassi della logica proposizionale,
2. la semantica della logica proposizionale,
3. algoritmi per riconoscere le tautologie proposizionali,
4. la completezza della logica proposizionale,
5. le algebre di Boole,
6. la completezza algebrica della logica proposizionale,
7. la sintassi della logica del primo ordine,
8. la semantica della logica del primo ordine,
9. algoritmi per riconoscere le tautologie del primo ordine,
10. la completezza della logica del primo ordine.
11. la compattezza della logica del primo ordine.
12. alcuni teoremi limitativi.

1 INTRODUZIONE

"Via via che la logica si perfeziona, diminuisce il numero delle cose in cui si crede."
Bertrand Russell (1872-1970)

Nella vita siamo abituati a gestire quotidianamente una notevole quantità di informazione: memorizziamo, rielaboriamo, verifichiamo, confutiamo, facciamo ipotesi e traiamo conclusioni. Seppure questi processi si rivelino la maggior parte delle volte corretti, succede che in alcuni casi commettiamo degli *errori di valutazione* o sbagliamo a trarre delle conclusioni. Ciò nondimeno il nostro cervello è una potentissima macchina tutt'ora inimitabile da qualsiasi computer.

Nel nostro ragionamento utilizziamo diverse tecniche che trovano base in diverse esperienze riscontrabili nella vita. Ad esempio escludiamo automaticamente ipotesi che non siano abbastanza verosimili: raramente si accetterebbe come ipotesi che il "sole non sorga domani mattina". D'altronde questo evento, seppure con una probabilità bassissima, potrebbe in qualche modo avvenire; quindi una parte del nostro ragionamento è di tipo **probabilistico**. Allo stesso modo siamo capaci, osservando un evento, di risalirne alle cause: sentendo delle gocce d'acqua in testa, penseremo che sta piovendo; seppure non sia questa l'unica ipotesi plausibile. Un tale ragionamento si chiama **abduttivo**. Ancora, siamo capaci di estrarre delle regole *universali* da casi *particolari*: vedendo una fila di uomini ed una di donne davanti a dei bagni ci metteremo in coda secondo una regola che in effetti abbiamo creato noi al momento e che potrebbe anche essere sbagliata; un tale ragionamento si chiama **induttivo**.

Infine possediamo una tecnica di ragionamento che, se usata correttamente, non ci conduce *mai* in errore, si chiama ragionamento **deduttivo**. Tale tecnica combina un certo numero di **ipotesi** (che crediamo siano vere) e produce una **tesi**, la cui verità è strettamente collegata a quella delle ipotesi:

in ogni caso in cui le ipotesi siano vere anche la tesi lo sarà.

Uno degli esempi più antichi di tale ragionamento risale agli antichi greci:

$$\begin{array}{cl}
\text{Ipotesi} & \begin{cases}\text{Ogni animale è mortale,}\\ \text{Ogni uomo è un animale,}\end{cases} \\
\hline
\text{Tesi} & \begin{cases}\text{Ogni uomo è mortale.}\end{cases}
\end{array}$$

Notiamo innanzitutto che la correttezza di tale ragionamento non dipende dalla veridicità delle frasi: il seguente ragionamento, che segue lo stesso schema di quello qui sopra, rimane corretto:

$$\frac{\text{Ogni animale è buono,} \quad \text{Ogni uomo è un animale,}}{\text{Ogni uomo è buono.}}$$

Il ragionamento è corretto: se accettiamo che le frasi "ogni animale è buono" e "ogni uomo è un animale" allora dobbiamo *necessariamente* accettare anche "ogni uomo è buono". Se tale tesi non rispecchia la realtà vorrà dire che c'è qualche problema con le nostre ipotesi, non con il nostro ragionamento.

Quindi la validità di un ragionamento non dipende dalla validità delle singole frasi, ma dalla *struttura* del ragionamento. Possiamo quindi definire un ragionamento corretto come un procedimento che *preserva la verità*, ovvero la cui conclusione è vera **ogni volta che le ipotesi sono vere**.

Un secondo fatto che andrebbe notato a proposito dei ragionamenti qui sopra è che essi ci permettono di ottenere *nuove informazioni* a partire dalle informazioni che possediamo. Consideriamo il seguente esempio.

Su un tavolo ci sono 6 scrigni; su ognuno di essi c'è un'iscrizione.

1. Sul primo scrigno l'iscrizione dice: "nessuno di questi 6 scrigni contiene un tesoro".
2. Sul secondo scrigno l'iscrizione dice: "Solo 1 di questi 6 scrigni contiene un tesoro".
3. Sul terzo scrigno l'iscrizione dice: "Esattamente 2 di questi 6 scrigni contengono un tesoro".
4. Sul quarto scrigno l'iscrizione dice: "Esattamente 3 di questi 6 scrigni contengono un tesoro".
5. Sul quinto scrigno l'iscrizione dice: "Esattamente 4 di questi 6 scrigni contengono un tesoro".
6. Sul sesto scrigno l'iscrizione dice: "Esattamente 5 di questi 6 scrigni contengono un tesoro".

Sapendo che ciascuno scrigno contiene un tesoro *se e solo se* l'iscrizione su di esso dice il vero, possiamo stabilire in quali scrigni c'è un tesoro?

Cominciamo a ragionare, innanzitutto le frasi non possono essere tutte vere, perché si contraddicono tra di loro: se è vero che "Esattamente 2 di questi 6 scrigni contengono un tesoro" allora non può anche essere vero che "Esattamente 4 di questi 6 scrigni contengono un tesoro". Quindi al più una può essere vera. E se fossero tutte false? Neanche questo può succedere, perché se fossero tutte false non ci sarebbe nessuno scrigno con un tesoro, ma questo è proprio quello che c'è scritto sul primo scrigno, quindi esso dovrebbe contenere un tesoro ed abbiamo quindi una contraddizione. Allora abbiamo stabilito che esattamente una delle frasi deve essere vera. Ovviamente la frase vera non può essere l'ultima, perché dice che ci sono cinque scrigni contenenti un tesoro, e se questo fosse vero cinque scritte dovrebbero essere vere. Per lo stesso motivo non può essere vera quella sul penultimo scrigno e così via. L'unica frase che può essere vera è quella che dice "1 solo di questi 6 scrigni contiene un tesoro", per cui ora sappiamo che l'unico scrigno che contiene un tesoro è il secondo.

Il ragionamento eseguito qui sopra è logicamente corretto, esso rimane valido a prescindere che le informazioni che ci hanno dato sugli scrigni e sulle scritte siano vere o false. Ciò che conta è che **se** le informazioni che ci hanno dato sono corrette, allora la nostra tesi deve per forza valere.

Ricapitolando, la nostra mente è capace di manipolare informazioni in vari modi, alcuni di questi funzionano nella maggior parte dei casi, ma non sempre. Una delle nostre tecniche di ragionamento invece ci permette di avere estrema certezza che, se le informazioni che stiamo manipolando sono corrette, allora lo sarà anche la nostra conclusione. Chiameremo tale tecnica **ragionamento logico** ed esso sarà l'oggetto del nostro studio.

La prima cosa da fare per studiare le regole che governano il ragionamento logico è cercare di minimizzare le ambiguità contenute nel linguaggio quotidiano. Quando per esempio si dice "aiuteremo gli anziani o i bambini" si intende dire che verrà aiutata l'una o l'atra classe di persone ma non entrambe? Oppure potrebbero anche essere aiutate entrambe? Quando si dice "Se viene Marco io non vengo e Antonio viene" si intende dire che Antonio viene se viene Marco? Oppure Antonio viene comunque?

Per eliminare questo tipo di ambiguità costruiremo un linguaggio formale in cui saranno presenti nuovi simboli di cui definiremo **univocamente** il significato logico, in maniera che essi si comportino come le parti del discorso che vogliamo studiare. Cominceremo a costruire prima un linguaggio più semplice, che chiameremo **linguaggio proposizionale**, per poi passare a uno un po' più complesso (che però possiede più potere espressivo) che chiameremo **linguaggio del primo ordine**.

2 SINTASSI E SEMANTICA DELLA LOGICA PROPOSIZIONALE.

2.1 PROPOSIZIONI.

Il primo passo da compiere è definire quali sono le parti del discorso che ci interessano in questo studio. Chiameremo *proposizione* una qualsiasi affermazione di cui ha senso dire se è vera o falsa, a cui quindi è possibile attribuire un valore di verità

Ad esempio:

- "Marco è alto 1,75m",
- "5 è un numero dispari",
- "Roma è la capitale della Francia",

sono proposizioni. Al contrario, l'affermazione "Alzati!' non è una proposizione (esprime un ordine e non un fatto che può essere vero o falso). Le proposizioni più semplici sono quelle formate da un soggetto e da un predicato, che esprime una proprietà del soggetto, oppure da un soggetto, un predicato, un oggetto (il predicato collega il soggetto all'oggetto). Nei ragionamenti, però, spesso utilizziamo proposizioni più complesse, ottenute a partire da quelle più semplici. Le proposizioni più complesse possono essere ottenute combinando tra loro quelle semplici attraverso l'uso dei connettivi, quali " e", " o", "non", "se... allora ...", ecc. Ad esempio:

1. "Se m e n sono numeri pari allora anche $m+n$ è un numero pari",
2. "Se c'è il sole allora vado al mare".

2.2 IL LINGUAGGIO FORMALE

Il primo passo da fare per poter studiare le regole logiche è costruire un *linguaggio formale* in cui sia possibile studiare i ragionamenti. Infatti il linguaggio che usiamo quotidianamente è complesso e soprattuto ambiguo per poter portare avanti al suo interno uno studio matematico dei ragionamenti. Abbiamo bisogno di un linguaggio abbastanza espressivo da poter tradurre i ragionamenti di tutti i giorni, ma costituito da una rigida sintassi e un significato univoco per ogni suo oggetto, in maniera da poterlo studiare matematicamente. Chiameremo questo sistema il **linguaggio formale**, mentre chiameremo **linguaggio naturale** quello usato quotidianamente. Per costruire un linguaggio formale bisogna fissare un **alfabeto**, cioè un insieme di simboli che ci serviranno a costruire delle *frasi* (che, in questo contesto, chiameremo *formule* o *proposizioni*). Le *frasi* non sono altro che delle sequenze finite (**stringhe**) di simboli che appartengono all'alfabeto che abbiamo fissato. Servirà poi una sintassi, cioè un insieme di regole per stabilire quali sequenze di simboli sono accettabili nel nostro linguaggio e quali no. Attenzione: la sintassi si occupa solo della forma delle frasi, è l'insieme delle regole che ne permettono la formazione, indipendentemente dai significati, di cui, invece, si occupa la semantica.

Esempio 2.1. Nel linguaggio dell'Aritmetica, consideriamo le seguenti "frasi" (cioè formule):

- $2 \cdot (3+1) = 8$, formula sintatticamente corretta,
- $2 + (4(- ==))$, formula sintatticamente non corretta
- 2+1= 6, formula sintatticamente corretta.

Si noti che la prima e la terza formula sono entrambe sintatticamente corrette (anche se la prima è vera e la terza è falsa). In particolare si noti che, nel caso di una formula non sintatticamente corretta, non ha nessun senso chiederci se è vera o falsa; essa è semplicemente una sequenza di simboli priva di senso. Le formule sintatticamente corrette saranno chiamate Formule Ben Formate. Quindi il compito della sintassi è quello di fornire un insieme di regole per costruire le Formule Ben Formate. Solo quando una formula è sintatticamente corretta si può discutere del suo significato. Questo è il compito della semantica: assegnare un significato a tutte le frasi sintatticamente corrette.

2.3 IL LINGUAGGIO DELLA LOGICA PROPOSIZIONALE

Come abbiamo visto, per capire se un certo ragionamento è corretto oppure no, non è importante sapere se le particolari proposizioni usate sono vere o false. Tra l'altro, bisogna stare attenti perché una stessa frase può essere vera in un contesto e falsa in un altro. Ad esempio, la frase "Nessuno capisce la lingua cinese" può essere vera nell'insieme degli alunni di una classe italiana, ma falsa in una classe di studenti cinesi. Quello che ci interessa è che il ragionamento *preservi la verità delle ipotesi nella tesi*, ovvero ci interessa la correttezza del procedimento per ricavare nuove affermazioni vere a partire da quelle supposte vere. Possiamo quindi del tutto abbandonare le frasi concrete e sostituirle con dei simboli. Nel Calcolo Proposizionale manipoleremo delle proposizioni atomiche che indicheremo con delle lettere minuscole (se necessario indicizzate) $p, q, r \ldots, p_1, \ldots, p_n, \ldots$. Le proposizioni atomiche si possono poi combinare tra loro mediante l'uso dei connettivi. Pertanto il nostro **alfabeto** conterrà:

- Un insieme infinito arbitrario di simboli che chiameremo variabili **proposizionali** (o **proposizioni atomiche**):
$$\mathsf{Var} := \{p, q, r \ldots, p_1, \ldots, p_n, \ldots\}$$
- Simboli per indicare i connettivi: $\neg, \wedge$
- Simboli accessori, come le parentesi: (e).

Ovviamente non siamo interessati a *qualsiasi* stringa di simboli dell'alfabeto precedente, per poter assegnare un significato alle stringhe di simboli esse devono essere state costruite secondo una *sintassi* che ci apprestiamo a specificare. Le stringhe di simboli a cui siamo interessati sono le *formule ben formate*.

Definizione 2.2 (Formule proposizionali)

L'insieme Form delle **formule proposizionali** (o **formule ben formate**) è il più piccolo insieme chiuso rispetto alle seguenti regole:

- tutti gli elementi di Var sono in Form;
- se $\varphi \in \mathtt{Form}$, allora anche $(\neg\varphi) \in \mathtt{Form}$;
- se $\varphi, \psi \in \mathtt{Form}$, allora anche $(\varphi \wedge \psi) \in \mathtt{Form}$.

Osservazione 2.3. Si noti che abbiamo usato le lettere greche $\varphi, \psi, \dots$ per indicare delle formule arbitrarie. Se dunque i simboli in Var sono le variabili nel **linguaggio oggetto** di studio, le lettere greche rappresentano **meta-variabili** appartenenti al meta-linguaggio che utilizziamo per parlare del linguaggio oggetto.

Esempio 2.4. Le seguenti stringhe sono in Form:

- $((p \wedge q) \wedge (r \wedge s))$,
- $((p \wedge q) \wedge (\neg r))$,
- $(((\neg p) \wedge q) \wedge (\neg q))$.

Al contrario, la seguente sequenza di simboli non è in Form: $\wedge\neg p(\neg$. In maniera più sottile, neanche $(\varphi \wedge \psi)$ appartiene a Form, poiché φ e ψ non sono in Var. La stringa $(\varphi \wedge \psi)$ appartiene al meta-linguaggio e denota una qualsiasi formula ottenuta congiungendo due formule arbitrarie (si veda anche Osservazione 2.3).

Notazione 2.5. Introduciamo anche degli ulteriori connettivi, intesi come abbreviazioni per formule più complicate:

$$
\begin{array}{lll}
\varphi \vee \psi & \text{sta per per} & \neg(((\neg\varphi) \wedge (\neg\psi))), \\
\varphi \to \psi & \text{sta per per} & \neg((\varphi \wedge (\neg\psi))), \\
\varphi \leftrightarrow \psi & \text{sta per per} & ((\varphi \to \psi) \wedge (\psi \to \varphi)),
\end{array}
$$

Va notato che, in senso stretto, la stringa di simboli $(p \to q)$ non appartiene a Form, ma poiché la Notazione 2.5 associa univocamente ad essa la stringa di simboli $\neg((\varphi \wedge (\neg\psi)))$, che invece appartiene a Form, nel seguito considereremo informalmente anche le stringhe che coinvolgono i connettivi $\vee, \to, \leftrightarrow$ come membri di Form (ovviamente, solo se rispettano regole di formazione simili a quelle della Definizione 2.2).

Osservazione 2.6. Si noti che (per ora) i simboli $\neg, \wedge, \vee, \to, \leftrightarrow$ non hanno nessun significato; essi sono solo dei simboli che devono essere manipolati in modo puramente formale, secondo le regole della sintassi enunciate prima.

Notazione 2.7. Le regole che abbiamo stabilito conducono a un uso eccessivo delle parentesi. Per semplificare l'aspetto delle formule conviene stabilire delle priorità tra i vari simboli:

priorità più alta	$\neg$
$\vdots$	$\wedge$
$\vdots$	$\vee$
$\vdots$	$\rightarrow$
priorità più bassa	$\leftrightarrow$

Pertanto la formula $p \wedge \neg q \rightarrow r$ deve essere interpretata come $((p \wedge (\neg q)) \rightarrow r)$, mentre la formula

$$\neg p \wedge q \vee r \rightarrow \neg s$$

significa

$$((((\neg p) \wedge q) \vee r) \rightarrow (\neg s)) \ .$$

Invece, nella formula $(p \rightarrow q) \vee r$ non si possono togliere le parentesi, perché la formula $p \rightarrow q \vee r$ verrebbe interpretata come $(p \rightarrow (q \vee r))$.

2.4 LA SEMANTICA DELLA LOGICA PROPOSIZIONALE

Bisogna ora attribuire un significato e, dunque, un valore di verità (*vero* o *falso*) a tutte le formule sintatticamente corrette (le formule in `Form`). Indichiamo i valori di verità vero con 1 e falso con 0. Si tratta quindi di definire una funzione $v\colon \mathtt{Form} \rightarrow \{0, 1\}$, che associa ad ogni formula ben formata φ il suo valore di verità $v(\varphi)$. Dato che ogni fbf si ottiene combinando tra loro delle proposizioni atomiche mediante l'uso dei connettivi (secondo le regole della sintassi), per definire una tale funzione v sull'insieme `Form` di tutte le formule ben formate basta definirla per le proposizioni atomiche e poi descrivere il comportamento dei vari connettivi. Per ogni variabile proposizionale p scriveremo $v(p) = 1$ per intendere che p è vera e $v(p) = 0$ per intendere che p è falsa.

Analizziamo ora il comportamento dei vari connettivi. Per fare ciò costruiamo per ognuno di essi una tabella, la sua **tavola di verità**, che indica, in corrispondenza dei casi possibili, se la proposizione ottenuta è vera o falsa.

Tavola della verità della **negazione** ($\neg$ = NOT)

p	$\neg p$
0	1
1	0

Tavola della verità della **congiunzione** ($\wedge$ = AND)

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1

Tavola della verità della **disgiunzione** ($\vee$ = OR)

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

Tavola della verità della **implicazione** ($\rightarrow$)

p	q	$p \rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

Tavola della verità della **doppia implicazione** ($\leftrightarrow$)

p	q	$p \leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

Utilizzando le tavole di verità appena presentate, possiamo costruire il valore di verità di una qualunque proposizione composta. Vediamo come.

Esempio 2.8. Descriviamo la tavola di verità della formula

$$(p \rightarrow (q \wedge \neg p)) \wedge q.$$

Cominciamo prendendo in esame quali sono i possibili valori di verità delle formule atomiche coinvolte, considerando tutte le possibili combinazioni.

p	q
0	0
0	1
1	0
1	1

Quanto scritto sopra è una maniera breve per descrivere le uniche quattro situazioni possibili: p e q potrebbero essere entrambe false, p è falsa ma q è vera, viceversa p è vera ma q è falsa e, infine, p e q potrebbero essere entrambe vere. A questo punto possiamo proseguire studiando le formule composte più semplici che sono presenti nella formula data.

p	q	$\neg p$	$(q \wedge \neg p)$
0	0	1	0
0	1	1	1
1	0	0	0
1	1	0	0

Ed infine possiamo utilizzare i conti intermedi fatti finora per arrivare ai possibili valori di verità della formula data inizialmente.

p	q	$\neg p$	$(q \wedge \neg p)$	$(p \to (q \wedge \neg p))$	$(p \to (q \wedge \neg p)) \wedge q$
0	0	1	0	1	0
0	1	1	1	1	1
1	0	0	0	0	0
1	1	0	0	0	0

Esercizio 2.9. Nella Sezione 2.3 abbiamo definito i connettivi $\vee, \to, \leftrightarrow$ come abbreviazioni di formule più complicate, mentre qui sopra abbiamo dato delle tavole di verità indipendenti per ogni connettivo. Un utile esercizio per prendere confidenza con le tavole di verità è quello di controllare che le tavole di verità dei connettivi $\vee, \to, \leftrightarrow$ coincidono con quelle delle loro rispettive definizioni sintattiche. In altre parole l'ultima colonna della tavola di verità di $\varphi \vee \psi$ coincide con quelle di $\neg(((\neg\varphi) \wedge (\neg\psi)))$; l'ultima colonna della tavola di verità di $\varphi \to \psi$ coincide con quella di $\neg((\varphi \wedge (\neg\psi)))$; e l'ultima colonna della tavola di verità di $\varphi \leftrightarrow \psi$ coincide con quella di $((\varphi \to \psi) \wedge (\psi \to \varphi))$.

Definizione 2.10

Una **valutazione** è una qualsiasi funzione $v\colon \mathsf{Var} \to \{0, 1\}$.

Ogni valutazione si può estendere in un'unica maniera a una funzione $\tilde{v}\colon \mathtt{Form} \to \{0, 1\}$ che si comporta sui connettivi come nelle tavole di verità descritte qui sopra. In altre parole, data una valutazione $v\colon \mathsf{Var} \to \{0, 1\}$ si definisce $\tilde{v}$ su una formula arbitraria φ come segue:

- se $\varphi \in \mathsf{Var}$ allora $\tilde{v}(\varphi) = v(\varphi)$,
- se $\varphi = \varphi_1 \wedge \varphi_2$ allora $\tilde{v}(\varphi) = \min\{\tilde{v}(\varphi_1), \tilde{v}(\varphi_2)\}$,
- se $\varphi = \neg\varphi_1$ allora $\tilde{v}(\varphi) = 1 - \tilde{v}(\varphi_1)$.

Si noti che per definire $\tilde{v}$ abbiamo sfruttato il fatto che una stringa appartiene a `Form` esattamente se è una variabile proposizionale o se è stata ottenuta secondo le regole della Definizione 2.2. Questa proprietà, che a volte va sotto il nome di **leggibilità unica** delle formula verrà sfruttata spesso nel seguito.

Esercizio 2.11. Usando il fatto che $\vee$, $\to$ e $\leftrightarrow$ sono state definite come abbreviazioni, mostrare che se v è una valutazione e $\tilde{v}$ è definita come sopra, allora

- $\tilde{v}(\varphi_1 \vee \varphi_2) = \max\{\tilde{v}(\varphi_1), \tilde{v}(\varphi_2)\}$,
- $\tilde{v}(\varphi_1 \to \varphi_2) = \max\{1 - \tilde{v}(\varphi_1), \tilde{v}(\varphi_2)\}$
- $\tilde{v}(\varphi_1 \leftrightarrow \varphi_2) = |\tilde{v}(\varphi_1)) - \tilde{v}(\varphi_2)|$

Osservazione 2.12. Da quanto detto risulta evidente che una valutazione sull'insieme `Form` è univocamente determinata dai valori che essa assume sulle proposizioni atomiche, poiché tutte le formule in `Form` si ottengono combinando proposizioni atomiche mediante l'uso di connettivi. Per questo motivo nel seguito, con un abuso di notazione, a volte confonderemo le valutazioni v con le loro estensioni $\tilde{v}$. La proprietà della semantica di dipendere esclusivamente da quella delle sue componenti atomiche è detta **vero-funzionalità**.

Esempio 2.13. Data la formula

$$(\neg p \to (\neg q \vee \neg p)) \wedge q$$

descriviamone la tavola di verità.

p	q	$\neg p$	$\neg q$	$(\neg q \vee \neg p)$	$(\neg p \to (\neg q \vee \neg p))$	$(\neg p \to (\neg q \vee \neg p)) \wedge q$
0	0	1	1	1	1	0
0	1	1	0	1	1	1
1	0	0	1	1	1	0
1	1	0	0	0	1	1

Esempio 2.14. Data la formula

$$q \to (p \vee (\neg q \to p))$$

descriviamone la tavola di verità.

p	q	$\neg q$	$\neg q \to p$	$p \vee (\neg q \to p))$	$q \to (p \vee (\neg q \to p))$
0	0	1	0	0	1
0	1	0	1	1	1
1	0	1	1	1	1
1	1	0	1	1	1

Esempio 2.15. Data la formula

$$(p \to (q \vee \neg p)) \wedge q$$

descriviamone la tavola di verità.

p	q	$\neg p$	$(q \vee \neg p)$	$(p \to (q \vee \neg p))$	$(p \to (q \vee \neg p)) \wedge q$
0	0	1	1	1	0
0	1	1	1	1	1
1	0	0	0	0	0
1	1	0	1	1	1

Esempio 2.16. Verifichiamo ora che per qualunque $\varphi, \psi \in \mathtt{Form}$ la formula $\varphi \to \psi$ ha la stessa tavola della verità di $\neg\varphi \vee \psi$.

Poiché i possibili valori di verità di φ e ψ sono solo 1 e 0, per costruire le tavole di verità di $\varphi \to \psi$ e $\neg\varphi \vee \psi$ non abbiamo necessità di sapere come sono effettivamente fatte φ e ψ, ma ci basta sapere quale sarà il comportamento delle formule composte in ognuno dei possibili casi. Abbiamo quindi:

φ	ψ	$\neg\varphi$	$\neg\varphi \vee \psi$	$\varphi \to \psi$
0	0	1	1	1
0	1	1	1	1
1	0	0	0	0
1	1	0	1	1

Definizione 2.17

Dato un insieme di formule Γ ed una formula φ, diremo che φ è **conseguenza logica** di Γ, in simboli $\Gamma \models \varphi$ se per ogni valutazione $v\colon \mathsf{Var} \to \{0, 1\}$, se $\tilde{v}(\gamma) = 1$ per ogni $\gamma \in \Gamma$ allora $\tilde{v}(\varphi) = 1$.

In generale se due proposizioni hanno la stessa tavola di verità, cioè hanno lo stesso valore di verità in corrispondenza di ogni caso possibile, allora si dicono *logicamente equivalenti*. Più precisamente

Definizione 2.18

Due formule proposizionali φ e ψ sono dette **logicamente equivalenti** se, per ogni valutazione $v\colon \mathtt{Form} \to \{0, 1\}$, $v(\varphi) = v(\psi)$. In tal caso scriveremo $\varphi \equiv \psi$.

Esempio 2.19. Nell'Esempio 2.16 è stato dimostrato che $\neg\varphi \vee \psi$ e $\varphi \to \psi$ sono logicamente equivalenti, qualunque siano le formule $\varphi, \psi \in \mathtt{Form}$.

Consideriamo una formula proposizionale φ nella quale compaiono soltanto le variabili proposizionali $p_1, \dots, p_n$. Possiamo pensare alla sua tavola di verità come a una funzione $f_\varphi \colon \{0,1\}^n \to \{0,1\}$: ogni riga della tavola si può suddividere in un vettore $\mathbf{v}$ di $\{0,1\}^n$ e un ulteriore valore in $0,1$, la i-esima componente del vettore $\mathbf{v}$ è il valore assunto dalla variabile p_i e l'ultimo valore dà il risultato di $f_\varphi(\mathbf{v})$. Ad esempio, se φ coincide con la formula $(\neg p \to (\neg q \vee \neg p)) \wedge q$ dell'Esempio 2.13, $f_\varphi : \{0,1\}^2 \to \{0,1\}$ è la funzione data da

$$f_\varphi(0,0) = 0, \qquad f_\varphi(0,1) = 1$$
$$f_\varphi(1,0) = 0, \qquad f_\varphi(1,1) = 1.$$

Quindi, ogni formula proposizionale in n variabili "genera" una funzione da $\{0,1\}^n$ in $\{0,1\}$. Il viceversa di questa affermazione è il contenuto del prossimo teorema.

Teorema 2.20 (Completezza funzionale)

Per ogni funzione $f \colon \{0,1\}^n \to \{0,1\}$ *esiste una formula proposizionale* φ *tale che* $f = f_\varphi$.

Dimostrazione. Se f è la funzione costantemente uguale a 1, scegliamo $\varphi = p_1 \vee \neg p_1 \vee \dots \vee p_n \vee \neg p_n$, mentre se è identicamente uguale a zero scegliamo $p_1 \wedge \neg p_1 \wedge \dots \wedge p_n \wedge \neg p_n$.

Sia f non costante. Possiamo pensare al suo dominio come ad una matrice con 2^n righe ed n colonne e, per ogni riga $a_{h1}, \dots, a_{hn}$, denotiamo con c_h il valore di $f(a_{h1}, \dots, a_{hn})$. Siano k le n-ple $(a_{i1}, \dots, a_{in}) \in \{0,1\}^n$ tali che $c_i = f(a_{i1}, \dots, a_{in}) =$

x_1	x_2	$\dots$	x_n	$f(x_1, \dots, x_n)$
0	0	$\dots$	0	c_1
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
a_{h1}	a_{h2}	$\dots$	a_{hn}	c_h
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$a_{2^n 1}$	$a_{2^n 2}$	$\dots$	$a_{2^n n}$	c_{2^n}

Tabella 1: Rappresentazione di f.

1 per ogni $i = 1, \dots k$. Fissato un $i = 1, \dots, k$, consideriamo le variabili proposizionali $p_1, \dots, p_n$ e per ogni $j = 1, \dots, n$ denotiamo con ψ_{ij} la formula definita nel seguente modo:

$$\psi_{ij} \text{ coincide con } \begin{cases} p_j & \text{se } a_{ij} = 1, \\ \neg p_j & \text{se } a_{ij} = 0. \end{cases}$$

Sia $\psi_i = \psi_{i1} \wedge \cdots \wedge \psi_{in}$. Osserviamo che il valore di verità di ψ_i è 1 se, e solo se, tutte le ψ_{ij} assumono valore di verità 1 e questo accade se, e solo se, a p_j assegniamo valore di verità a_{ij}. Sia ora $\varphi = \psi_1 \vee \cdots \vee \psi_k$. Vediamo che $f = f_\varphi$ e cioè che la Tabella 1 coincide con la tavola di verità di φ.

Sia $v(p_1) = b_1, \ldots, v(p_n) = b_n$ una qualsiasi assegnazione dei valori di verità delle variabili proposizionali. Poiché ogni b_j vale 0 oppure 1, esisterà una riga, diciamo la riga l, della Tabella 1 tale che $a_{l1} = b_1, \ldots, a_{ln} = b_n$. Il teorema è dimostrato se il valore di verità di φ rispetto alla valutazione v indotta dalla assegnazione fissata coincide con c_l. Se $c_l = 1$ si ha che ψ_l è uno dei disgiunti che costituiscono φ e, per la costruzione di ψ_l, questa vale 1 esattamente quando p_j viene valutata a_{lj}, quindi $v(\psi_{lj}) = 1$ per ogni $j = 1, \ldots, n$ e $v(\varphi) = 1$. Se $c_l = 0$ allora ψ_l non è uno dei disgiunti di φ. Ma per le osservazioni precedenti l'assegnazione che determina v è tale che $v(\psi_i) = 0$ per ogni $i \neq l$ e di conseguenza $v(\varphi) = 0$. □

Esempio 2.21. Consideriamo la funzione $f : \{0,1\}^3 \to \{0,1\}$ definita da

x_1	x_2	x_3	$f(x_1,x_2,x_3)$
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

Le triple da considerare sono $(0,0,0)$, $(0,1,1)$, $(1,0,1)$ e $(1,1,1)$, la prima, quarta, sesta e ottava riga della tabella. Si ha che

$$\psi_1 = \neg p \wedge \neg q \wedge \neg r, \qquad \psi_4 = \neg p \wedge q \wedge r,$$
$$\psi_6 = p \wedge \neg q \wedge, r \qquad \psi_8 = p \wedge q \wedge r.$$

Quindi $\psi = \psi_1 \vee \psi_4 \vee \psi_6 \vee \psi_8$ è la formula tale che $f_\psi = f$.

Notiamo che la dimostrazione del Teorema 2.20 si mantiene valida scambiando tra di loro 0 e 1, $\vee$ e $\wedge$. Inoltre, dal Teorema di completezza funzionale possiamo ricavare un importante corollario, per il quale è necessario dare una definizione preliminare.

Definizione 2.22

Una formula proposizionale φ è detta in **forma normale**:

- **congiuntiva** se è una congiunzione di uno o più componenti, ciascuno dei quali è una disgiunzione di una o più variabili proposizionali o negazioni di variabili proposizionali;

- **disgiuntiva** se è una disgiunzione di uno o più componenti, ciascuno dei quali è una congiunzione di una o più variabili proposizionali o negazioni di variabili proposizionali.

Teorema 2.23 (Forma normale)

Ogni formula proposizionale ψ è logicamente equivalente ad una formula proposizionale in forma normale congiuntiva e ad una in forma normale disgiuntiva.

Dimostrazione. Basta considerare la tavola di verità di ψ e applicare la dimostrazione del Teorema 2.20 alla funzione f_ψ. Il risultato sarà una formula in forma normale disgiuntiva. □

Esempio 2.24. Sia φ la formula $(\neg p \to (\neg q \vee \neg p)) \wedge q$ dell'Esempio 2.13. La sua tavola di verità è

p	q	$(\neg p \to (\neg q \vee \neg p)) \wedge q$
0	0	0
0	1	1
1	0	0
1	1	1

Per ottenere la rappresentazione in forma normale disgiuntiva, consideriamo la seconda e la quarta riga, ottenendo:

$$\varphi \equiv (\neg p \wedge q) \vee (p \wedge q).$$

Per ottenere la forma normale congiuntiva possiamo applicare la stessa tecnica però considerando le righe per le quali φ assume valore di verità 0, invertendo le negazioni e scambiando $\vee$ e $\wedge$. In questo modo otteniamo:

$$\varphi \equiv (p \vee q) \wedge (\neg p \vee q).$$

Alternativamente per ottenere la forma normale congiuntiva si può applicare la stessa tecnica di Teorema 2.20 a $\neg\varphi$, mettendo una negazione davanti alla formula in forma normale disgiuntiva e poi applicare le leggi di De Morgan e della doppia negazione (si veda Esempio 2.33) per far arrivare la negazione davanti alle singole variabili proposizionali.

Osservazione 2.25. I simboli usati per denotare i vari connettivi non sono standard. In contesti diversi si usano spesso simboli diversi da quelli che noi abbiamo introdotto. Ad esempio, nel linguaggio di programmazione C, il simbolo per il connettivo logico AND è &&, mentre quello per il connettivo logico OR è ||.

Definizione 2.26

Sia $\varphi \in \texttt{Form}$ e v una valutazione. Se $v(\varphi) = 1$, diremo che φ è **soddisfatta** dalla valutazione v, oppure che v è un **modello** per φ. In tal caso si scrive $v \models \varphi$.

Una formula ben formata φ è **soddisfacibile** se ha almeno un modello, cioè se esiste almeno una valutazione in cui φ è soddisfatta. In caso contrario φ è **insoddisfacibile** (si dice anche che φ è una **contraddizione**).

Esempio 2.27. La seguente formula è soddisfacibile: $(p \wedge \neg q) \vee (q \to p)$. Infatti, se consideriamo una valutazione v tale che $v(p) = 1$ e $v(q) = 0$, si ha $v(\neg q) = 1$, quindi $v(p \wedge \neg q) = 1$, da cui segue che

$$v((p \wedge \neg q) \vee (q \to p)) = 1 \,.$$

Un esempio di formula insoddisfacibile (contraddizione) è dato dalla formula seguente: $p \wedge \neg p$. Infatti, dato che per una qualunque valutazione v, $v(p)$ può solo essere 0 o 1, la tavola di verità della formula precedente è:

p	$\neg p$	$p \wedge \neg p$
0	1	0
1	0	0

il che significa che la proposizione $p \wedge \neg p$ è sempre falsa, indipendentemente dal fatto che p sia vera o falsa.

Definizione 2.28

Una formula ben formata φ è una **tautologia** se ogni valutazione v è un modello per φ, cioè se φ risulta vera in ogni valutazione (ovvero, qualunque siano i valori di verità delle proposizioni che la compongono). In tal caso si scriverà $\models \varphi$.

Esempio 2.29. La formula

$$p \to p \vee q$$

è una tautologia. Infatti, dato che per una qualunque valutazione v, $v(p)$ e $v(q)$ possono solo essere 0 o 1, la tavola di verità della formula precedente è:

p	q	$p \vee q$	$p \to p \vee q$
0	0	0	1
0	1	1	1
1	0	1	1
1	1	1	1

il che significa che la proposizione $p \to p \vee q$ è sempre vera, indipendentemente dal fatto che p o q siano vere o false.

Esempio 2.30. Ci chiediamo se la formula $p \to \neg p$ sia soddisfacibile. Scriviamo la tavola di verità:

p	$\neg p$	$p \to \neg p$
0	1	1
1	0	0

Ciò significa che la proposizione $p \to \neg p$ è soddisfacibile e la valutazione che la soddisfa è quella che assegna ad p il valore 0, cioè $\nu(p) = 0$ (in altre parole, la proposizione $p \to \neg p$ è vera solo quando p è falsa).

Proposizione 2.31. *Una formula ben formata φ è una tautologia se, e solo se, $\neg\varphi$ è insoddisfacibile.*

Dimostrazione. Supponiamo che φ sia una tautologia. Questo vuol dire che qualsiasi valutazione $\nu\colon \mathtt{Form} \to \{0, 1\}$ la rende vera, in altre parole $\nu(\varphi) = 1$. Poiché ν è una valutazione, deve comportarsi su tutte le formule composte come descritto dalle tavole di verità dei connettivi, in particolare se consideriamo la negazione di φ, data da $\neg\varphi$, avremo $\nu(\neg\varphi) = 0$. Ciò vale per ogni valutazione e dunque la negazione di φ é una contraddizione.

Viceversa, se $\neg\varphi$ è una contraddizione, allora, per definizione, qualsiasi valutazione $\nu\colon \mathtt{Form} \to \{0, 1\}$ la rende falsa, cioè $\nu(\neg\varphi) = 0$. Ancora una volta, ν è una valutazione, quindi sulle formule composte agisce come descritto dalle tavole di verità dei connettivi, in particolare se consideriamo $\neg\varphi$ senza il simbolo di negazione, cioè φ, avremo $\nu(\varphi) = 1$. Ciò vale per ogni valutazione e dunque φ è una tautologia. $\square$

Osservazione 2.32. La proposizione precedente afferma una cosa piuttosto ovvia e cioè che una proposizione φ è "sempre vera" se, e solo se, la sua negazione $\neg\varphi$ è "sempre falsa."

Esempio 2.33. Le seguenti sono (schemi di) tautologie della logica proposizionale;

$(\varphi \vee \psi) \vee \xi \leftrightarrow \varphi \vee (\psi \vee \xi)$	**Associatività di $\vee$**,
$(\varphi \wedge \psi) \wedge \xi \leftrightarrow \varphi \wedge (\psi \wedge \xi)$	**Associatività di $\wedge$**,
$\varphi \vee \psi \leftrightarrow \psi \vee \varphi$	**Commutatività di $\vee$**,
$\varphi \wedge \psi \leftrightarrow \psi \wedge \varphi$	**Commutatività di $\wedge$**,
$(\varphi \vee \psi) \wedge \xi \leftrightarrow (\varphi \wedge \xi) \vee (\psi \wedge \xi)$	**Distributività 1**,
$(\varphi \wedge \psi) \vee \xi \leftrightarrow (\varphi \vee \xi) \wedge (\psi \vee \xi)$	**Distributività 2**,
$(\varphi \vee \psi) \leftrightarrow \neg(\neg\varphi \wedge \neg\psi)$	**Legge di De Morgan 1**,
$(\varphi \wedge \psi) \leftrightarrow \neg(\neg\varphi \vee \neg\psi)$	**Legge di De Morgan 2**,
$\varphi \vee \neg\varphi$	**Terzo escluso**,
$\neg(\varphi \wedge \neg\varphi)$	**Principio di non contraddizione**,
$\neg(\neg\varphi) \leftrightarrow \varphi$	**Legge della doppia negazione**,
$(\neg\varphi \to \varphi) \to \varphi$	**Consequentia mirabilis**,
$((\varphi \to \psi) \to \varphi) \to \varphi$	**Legge di Peirce**,
$((\varphi \wedge \psi) \vee \psi) \leftrightarrow \psi$	**Assorbimento 1**,
$((\varphi \vee \psi) \wedge \psi) \leftrightarrow \psi$	**Assorbimento 2**.

Concludiamo questa sezione con un'utile definizione che ci permetterà di dimostrare teoremi guardando la *struttura* di una formula arbitraria.

Definizione 2.34

La **complessità** di una formula $\varphi \in \mathtt{Form}$, in simboli $\#(\varphi)$ è definita come segue:

1. se $\varphi \in \mathsf{Var}$ allora $\#(\varphi) = 0$,
2. se $\varphi = \neg\varphi_1$ allora $\#(\varphi) = \#(\varphi_1) + 1$,
3. se $\varphi = \varphi_1 \wedge \varphi_2$ allora $\#(\varphi) = \max\{\#(\varphi_1), \#(\varphi_2)\} + 1$.

2.5 IL TEOREMA DI COMPATTEZZA PER LA LOGICA PROPOSIZIONALE

Definizione 2.35

Un insieme di formule Γ è detto **soddisfacibile** se, e soltanto se, esiste una valutazione v tale che $v(\gamma) = 1$ per ogni $\gamma \in \Gamma$. Se Γ non è soddisfacibile diremo che è **insoddisfacibile**.

Osservazione 2.36. Esistono insiemi non soddisfacibili di formule soddisfacibili, es.: $\Gamma = \{p, \neg p\}$; le formule p e $\neg p$ sono entrambe soddisfacibili, ma l'insieme Γ non è soddisfacibile perché qualsiasi valutazione che renda vera p, deve rendere falsa $\neg p$.

La dimostrazione del seguente lemma è una banale applicazione delle definizioni e per questo è lasciata per esercizio al lettore.

Lemma 2.37. *Sia Γ un insieme di formule, per ogni formula φ, ψ, χ valgono le seguenti:*

1. *Se $\Gamma \models \varphi$ allora $\Gamma \cup \{\psi\} \models \varphi$.*
2. *Se $\Gamma \models \varphi$ e $\varphi \equiv \psi$ allora $\Gamma \models \psi$.*
3. *Se $\Gamma \cup \{\psi\} \models \varphi$ e $\psi \equiv \chi$ allora $\Gamma \cup \{\chi\} \models \varphi$.*

Il punto 1 del Lemma 2.37 afferma che la relazione $\models$ è **monotona**, nel senso che se $\Gamma \subseteq \Gamma'$ allora da Γ' seguono logicamente tutte le formule che seguono logicamente da Γ. I punti punto 2 e punto 3 affermano che $\models$ è invariante per equivalenza logica.

Lemma 2.38. *Se Γ è un insieme di formule, allora per ogni formula φ valgono:*

1. *Se Γ è insoddisfacibile allora $\Gamma \setminus \{\neg\varphi\} \models \varphi$ e $\Gamma \setminus \{\varphi\} \models \neg\varphi$.*
2. *$\Gamma \models \varphi$ se, e soltanto se, $\Gamma \cup \{\neg\varphi\}$ è insoddisfacibile.*

Dimostrazione.

PUNTO 1 Dimostriamo la contronominale, supponiamo che

$$\Gamma \setminus \{\neg\varphi\} \not\models \varphi \text{ oppure } \Gamma \setminus \{\varphi\} \not\models \neg\varphi.$$

Supponiamo di essere nel primo caso, allora esiste una valutazione che rende vere tutte le formule in $\Gamma \setminus \{\neg\varphi\}$ e rende falsa φ; in altre parole, esiste una valutazione che rende vere tutte le formula in $\Gamma \setminus \{\neg\varphi\}$ e inoltre rende vera $\neg\varphi$. Tale valutazione rende allora vere tutte le formule in Γ, quindi Γ risulta soddisfacibile. La dimostrazione dell'altro caso (cioè quando $\Gamma \setminus \{\varphi\} \not\models \neg\varphi$) è simile.

PUNTO 2 L'implicazione da destra verso sinistra è data dal Punto 1. Per l'altra implicazione supponiamo che $\Gamma \models \varphi$, quindi per ipotesi sappiamo che ogni valutazione che manda le formule di Γ in 1 deve mandare anche φ in 1. Ma allora è chiaro che $\Gamma \cup \{\neg\varphi\}$ è insoddisfacibile, perché non può esistere una valutazione che mandi tutte le formule di Γ e $\neg\varphi$ in 1.

□

In questa sezione dimostreremo un teorema di fondamentale importanza. Esso asserisce che se ogni parte finita di un insieme di formule è soddisfacibile, allora lo è tutto l'insieme. Per comodità chiamiamo **finitamente soddisfacibile** un insieme di formule in cui ogni parte finita è soddisfacibile.

Lemma 2.39. *Ogni insieme finitamente soddisfacibile è contenuto in un insieme massimale rispetto a questa proprietà.*

Dimostrazione. Sia Γ un insieme finitamente soddisfacibile. Consideriamo la famiglia di insiemi

$$\mathcal{F} := \{\Lambda \mid \Gamma \subseteq \Lambda \text{ e } \Lambda \text{ è finitamente soddisfacibile}\}.$$

La famiglia $\mathcal{F}$ non è vuota, perché Γ le appartiene. Inoltre $\mathcal{F}$ è parzialmente ordinata dalla relazione $\subseteq$. Infine ogni catena in $\mathcal{F}$ ha una maggiorante. Infatti se $\mathcal{C} \subseteq \mathcal{F}$ è una catena (e cioè un sottoinsieme linearmente ordinato) allora consideriamo $\bigcup \mathcal{C}$. L'insieme $\bigcup \mathcal{C}$ è ovviamente un maggiorante per $\mathcal{C}$, infatti per definizione per ogni $\Psi \in \mathcal{C}$, $\Psi \subseteq \bigcup \mathcal{C}$. Per concludere dobbiamo verificare che $\bigcup \mathcal{C}$ appartenga a $\mathcal{F}$. Ma $\bigcup \mathcal{C}$ contiene sicuramente Γ, poiché ogni insiemi in $\mathcal{F}$ contiene Γ; inoltre $\bigcup \mathcal{C}$ è finitamente soddisfacibile, perché se non lo fosse dovrebbe contenere un insieme finito non soddisfacibile F, ma se $F \subseteq \bigcup \mathcal{C}$ allora deve esistere $G \in \mathcal{C}$, tale che $F \subseteq G$, contro l'ipotesi che $\mathcal{C} \subseteq \mathcal{F}$.

Dunque per il *Lemma di Zorn* possiamo concludere che $\mathcal{F}$ ha un elemento massimale. In altre parole esiste un insieme di formule che estende Γ ed è massimale rispetto all'essere finitamente consistente. □

Osservazione 2.40. Si noti che l'uso del Lemma di Zorn non è necessario quando il linguaggio è numerabile. Tuttavia, per illustrare un'applicazione del teorema di compattezza avremo bisogno della sua versione estesa a linguaggi di cardinalità più che numerabili.

Lemma 2.41. *Se M è un insieme massimale rispetto all'essere finitamente soddisfacibile, allora per ogni $\varphi, \psi \in \texttt{Form}$ valgono*

1. $\varphi \in M$ *oppure* $\neg\varphi \in M$.
2. $\varphi \wedge \psi \in M$ *se, e soltanto se,* $\varphi, \psi \in M$

Dimostrazione.

1. Supponiamo, per assurdo, che $\varphi \notin M$ e $\neg\varphi \notin M$. Allora, per la massimalità di M, abbiamo che né $M \cup \{\varphi\}$ né $M \cup \{\neg\varphi\}$ sono finitamente soddisfacibili. Dunque, esistono $S, S' \subseteq M$ finiti, tale che $S \cup \{\varphi\}$ e $S' \cup \{\neg\varphi\}$ non sono soddisfacibili. Se poniamo $T := S \cup S'$ è facile vedere che $T \cup \{\varphi \vee \neg\varphi\}$ non è soddisfacibile. Per il Punto 1 del Lemma 2.38, questo è equivalente a $T \models \neg(\varphi \vee \neg\varphi)$. Infine, utilizzando le leggi di De Morgan (vedi Esempio 2.33), abbiamo $T \models \neg\varphi \wedge \varphi$, da cui segue che T non è soddisfacibile, assurdo.
2. Supponiamo che $\varphi \wedge \psi \in M$ e, per assurdo, $\varphi \notin M$. Allora, per la massimalità di M, l'insieme $M \cup \varphi$ non è finitamente soddisfacibile. Dunque esiste $S \subseteq M$ finito tale che $S \cup \{\varphi\}$ non è soddisfacibile. In altre parole: non esiste nessuna valutazione che renda vere le formule in S e φ. Ma allora il sottoinsieme finto di M dato da $S \cup \{\varphi \wedge \psi\}$ non è soddisfacibile, perché una valutazione che lo soddisfi dovrebbe rendere vere tutte le formule in S e $\varphi \wedge \psi$ e quindi *a fortiori* dovrebbe rendere vera anche φ. Ma questo contraddice il fatto che M è finitamente soddisfacibile e dunque $\varphi \in M$. In maniera simile si può dimostrare che anche $\psi \in M$. Per il viceversa, supponiamo che $\varphi, \psi \in M$ e, per assurdo, che $\varphi \wedge \psi \notin M$. Allora, per la massimalità di M, l'insieme $M \cup \varphi \wedge \psi$ non è finitamente soddisfacibile. Dunque esiste $S \subseteq M$ finito tale che $S \cup \{\varphi \wedge \psi\}$ non è soddisfacibile. In altre parole: non esiste nessuna valutazione che renda vere le formule in S e $\varphi \wedge \psi$. Ma allora il sottoinsieme finto di M dato da $S \cup \{\varphi, \psi\}$ non è soddisfacibile, perché una valutazione che lo soddisfi dovrebbe rendere vere

tutte le formule in S e $\varphi \wedge \psi$. Ma questo contraddice il fatto che M è finitamente soddisfacibile e dunque $\varphi \wedge \psi \in M$.

□

Lemma 2.42. *Dato un insieme M di formule massimale rispetto all'essere finitamente soddisfacibile esiste una valutazione che rende vere esattamente le formule che appartengono a M.*

Dimostrazione. Dato M come nell'asserto definiamo ν_M come segue: per ogni $p \in \mathsf{Var}$,

$$\nu_M(p) := \begin{cases} 1 & \text{se } p \in M \\ 0 & \text{se } p \notin M \end{cases}$$

Dimostriamo ora per induzione sulla complessità di φ che per ogni $\varphi \in \mathtt{Form}$,

$$\nu_M(\varphi) = 1 \text{ se, e soltanto se, } \varphi \in M.$$

Il passo base è dato direttamente dalla definizione di $\nu_M(p)$.

Supponiamo quindi che $\varphi = \varphi_1 \wedge \varphi_2$. Allora si ha $\nu_M(\varphi) = 1$ se, e soltanto se, $\nu_M(\varphi_1 \wedge \varphi_2) = 1$ se, e soltanto se, $\nu_M(\varphi_1) = \nu_M(\varphi_2) = 1$ se, e soltanto se, per ipotesi induttiva, $\varphi_1, \varphi_2 \in M$ se, e soltanto se, per il punto 2 del Lemma 2.41, $\varphi_1 \wedge \varphi_2 \in M$. Se invece $\varphi = \neg\varphi_1$. Si ha che $\nu_M(\varphi) = 1$ se, e soltanto se, $\nu_M(\varphi_1) = 0$. Per ipotesi induttiva quest'ultima è equivalente a $\varphi_1 \notin M$. A sua volta, per il Lemma 2.41 ciò è equivalente a $\varphi = \neg\varphi_1 \in M$. □

Teorema 2.43 (Compattezza della logica proposizionale)

Un insieme Γ di formule è soddisfacibile, se, e soltanto se, ogni suo sottoinsieme finito è soddisfacibile.

Dimostrazione. L'implicazione da sinistra verso destra è ovvia. Dimostriamo quindi l'altra implicazione. Supponiamo che Γ sia finitamente soddisfacibile, per il Lemma 2.39 esiste un insieme M che estende Γ ed è massimale rispetto all'essere finitamente soddisfacibile. Dunque possiamo applicare il Lemma 2.42 ad M per ottenere una valutazione che rende vere tutte le formule in M e dunque tutte le formule in Γ. In conclusione Γ è soddisfacibile □

2.5.1 *Un'applicazione della compattezza*

Vediamo ora un'applicazione del teorema di compattezza che permette di dimostrare un teorema di matematica combinatoria transfinita.

Per poter applicare il teorema ricordiamo alcune definizioni di teoria dei grafi.

Definizione 2.44

Un **grafo semplice** (non orientato) è dato da una coppia (A, R) dove A è un insieme non vuoto, i cui elementi sono detti **nodi**, e R è una relazione binaria su A, $R \subseteq A^2$, irriflessiva e simmetrica; le coppie in R vengono chiamate **archi**.

Definizione 2.45

Sia dato un grafo (A, R) e e $k \in \mathbb{N}$, con $k \neq 0$. Una k-**colorazione** di (A, R) è una funzione $f\colon A \to \{1, 2, \ldots, k\}$ tale che aRa' implica $f(a) \neq f(a')$. Diremo che un grafo (A, R) è k-colorabile se esiste una k-colorazione di (A, R).

Per capire da dove viene questa terminologia possiamo pensare ai vertici di particolare grafi semplici come gli stati su una cartina e ad R come la relazione di "essere confinante". In questa interpretazione una k-colorazione è una maniera di colorare la mappa senza dare lo stesso colore a due stati adiacenti.

La logica proposizionale è abbastanza espressiva da poter parlare di k colorazioni. Per vedere ciò sia (A, R) un grafo semplice tale che $|A| = \rho$ e consideriamo un insieme di variabili proposizionali di cardinalità $k \cdot \rho$. Stabiliamo una corrispondenza tra le variabili proposizionali e le coppie ordinate (x, i) con $x \in A$ e $1 \leqslant i \leqslant k$. In altre parole, supponiamo senza perdere di generalità che l'insieme delle variabili proposizionali sia $K := \{1, \ldots, k\}$ e

$$\mathrm{Var}_A := \{p_i \mid p \in A, i \in K\}.$$

Se immaginiamo di assegnare valore di verità 1 alla formula p_i se, e soltanto se, il vertice p ha colore i, allora possiamo esprimere certe proprietà del grafo (A, R) tramite formule proposizionali. Ad esempio, il fatto che *a un nodo venga assegnato almeno un colore* può essere scritto formalmente nella seguente maniera:

$$\alpha_p := \bigvee_{i \in K} p_i,$$

Esiste infatti una biezione tra le valutazioni che rendono vera α_p e i diversi modi di assegnare un "colore" $i \leqslant k$ a p. Se α_p è resa vera da una valutazione $v\colon \mathrm{Var}_A \to \{0, 1\}$ allora una delle formule proposizionali disgiunte in α_p deve essere vera, diciamo p_j, dunque scegliamo di assegnare il colore j al nodo p. Viceversa, se scegliamo di assegnare il colore j a p allora possiamo considerare la valutazione v che rende vera p_j se, e solo se, a p è stato assegnato colore j. Tale valutazione rende vera α_p.

Un'altra proprietà definibile tramite una formula proposizionale è che al nodo p viene associato al più un colore. Essa è espressa dalla formula

$$\beta_p := \bigwedge_{i \neq j, i, j \in K} \neg(p_i \wedge p_j).$$

Un'altra proprietà ancora esprimibile nel linguaggio della logica proposizionale è che due nodi p e q hanno colori distinti:

$$\gamma_{p,q} := \bigwedge_{i \in K} \neg(p_i \wedge q_i).$$

Se ne deduce che, detto T il seguente insieme di formule

$$T := \{\alpha_p \mid p \in A\} \cup \{\beta_p \mid p \in A\} \cup \{\gamma_{p,q} \mid (p,q) \in R\},$$

esiste una biezione tra le valutazioni che rendono vere tutte le formule in T e le k-colorazioni di (A, R). Infatti, se $v\colon Var_A \to \{0,1\}$ è rende vere tutte le formule in T, allora per ogni $p \in A$ esiste esattamente un $i \in K$ tale che $v(p_i) = 1$; definiamo la colorazione $f : A \to K$ come $f(p) = i$. Viceversa, se $f\colon A \to K$ è una k-colorazione, definiamo la valutazione v come $v(p_i) = 1$ sse $f(p) = i$.

Diremo che (B, S) è un sottografo di (A, R) se $B \subseteq A$ e $S \subseteq R$ tale che immagini delle due proiezioni canoniche di S su A ($\pi_1(a_1, a_2) := a_1$ e $\pi_2(a_1, a_2) := a_2$) sono sottoinsiemi di B. Un grafo e finitamente k-colorabile, se ogni suo sottografo finito è k-colorabile.

Dimostriamo ora, utilizzando la compattezza un teorema riguardante la k-colorabilità di grafi semplici infiniti.

Teorema 2.46 (De Bruijn, Erdös, 1951)

Siano (A, R) un grafo semplice e $1 \leqslant k$ un numero naturale. Il grafo (A, R) è k-colorabile se, e soltanto se, ogni suo sottografo finito è k-colorabile.

Dimostrazione. È chiaro che se (A, R) è k-colorabile, allora è finitamente k-colorabile. Supponiamo ora che ogni sottografo finito di (A, R) sia k-colorabile. Consideriamo l'insieme di formule T definito sopra. Abbiamo visto che l'esistenza di una k-colorazione di (A, R) è equivalente all'esistenza di una valutazione che renda vere tutte le formule in T. Per stabilire il teorema è dunque sufficiente stabilire che T è soddisfacibile. Ma T è finitamente soddisfacibile perché il grafo (A, R) è finitamente k-colorabile, dunque per il teorema di compattezza T è soddisfacibile. □

2.6 DEDUZIONE NATURALE

2.6.1 *Le regole della deduzione naturale*

In questa sezione presenteremo una maniera alternativa di definire i connettivi: la **deduzione naturale**. Se le valutazioni ci permettono di specificare il comportamento dei connettivi in maniera *estensiva*, cioè descrivendo il loro funzionamento in ogni caso possibile, la deduzione naturale descrive il comportamento dei connettivi in maniera *intensiva*, cioè specificando come essi vengono introdotti o rimossi all'interno di un ragionamento logico.

Le regole della deduzione naturale sono molto intuitive, perché rappresentano schematicamente l'usuale maniera di trattare i connettivi nelle dimostrazioni. Vedremo presto che ogni connettivo può essere completamente descritto da due regole: una per la sua introduzione e una per la sua eliminazione.

2.6.1.1 *Congiunzione*

Cominciamo dal connettivo $\wedge$. Per *introdurre* una congiunzione in una dimostrazione, cioè per dimostrare qualcosa della forma $\varphi \wedge \psi$ di solito si dimostra φ, poi si dimostra ψ e poi se ne deduce la loro congiunzione. Rappresentiamo questa costruzione logica nella seguente maniera:

$$\mathrm{I}\wedge\ \dfrac{\begin{matrix}\Gamma & \Gamma' \\ \vdots & \vdots \\ \varphi & \psi\end{matrix}}{\varphi \wedge \psi} \tag{1}$$

dove

$$\begin{matrix}\Gamma \\ \vdots \\ \varphi\end{matrix}$$

rappresenta una dimostrazione non meglio specificata di φ utilizzando le ipotesi all'interno dell'insieme di formule Γ. I puntini di sospensione tra Γ e φ servono a esprimere il fatto che per il momento non siamo interessati a sapere come esattamente siamo arrivati a dedurre φ da Γ, ma solo al fatto che esiste una dimostrazione di questo tipo. Dunque la regola qui sopra può essere letta nella seguente maniera

> date una dimostrazione di φ con ipotesi in Γ e una dimostrazione di ψ con ipotesi in Γ' possiamo combinarle tra loro, utilizzando la regola Equazione (1), ottenendo una dimostrazione con ipotesi in $\Gamma \cup \Gamma'$ della formula $\varphi \wedge \psi$.

Passiamo ora alle regole per *eliminare* una congiunzione. Se abbiamo già dimostrato una formula del tipo $\varphi \wedge \psi$, sappiamo che da essa possiamo dedurre sia φ che ψ, dunque abbiamo due regole per l'eliminazione della congiunzione:

$$\mathrm{E}\wedge\mathrm{S}x\ \dfrac{\begin{matrix}\Gamma \\ \vdots \\ \varphi \wedge \psi\end{matrix}}{\varphi} \qquad \mathrm{E}\wedge\mathrm{D}x\ \dfrac{\begin{matrix}\Gamma \\ \vdots \\ \varphi \wedge \psi\end{matrix}}{\psi}$$

2.6.1.2 *Negazione*

Discutiamo ora la negazione. Ciò che è da tenere a mente è che la negazione $\neg\varphi$ può essere pensata come $\varphi \to \bot$. Dunque, per introdurre una negazione basta dedurre un assurdo a partire da ipotesi in $\Gamma \cup \{\varphi\}$, a quel punto si può **scaricare** l'ipotesi φ e dedurre $\neg\varphi$.

$$\dfrac{\begin{array}{c}\Gamma, [\varphi]^1 \\ \vdots \\ \bot\end{array}}{\neg\varphi}\ \mathrm{I}\neg_1$$

Le parentesi servono a dire che l'ipotesi φ è stata cancellata, o scaricata come si dice in gergo. In altre parole, nella deduzione finale, se φ era in Γ, questa può essere stata rimossa da Γ con l'applicazione dell'ultima regola. Sia il numero vicino alle parentesi, che l'uso delle parentesi quadre invece di una semplice cancellatura servono semplicemnte a rendere più leggibile la derivazione: la prima convenzione serve a tenere traccia del passo della deduzione in cui un'ipotesi è stata scaricata, la seconda a rendere più facile la lettura dell'ipotesi rimossa. Si noti che anche se un'ipotesi è utilizzata varie volta in un teorema, questa è enunciata una sola volta. In ragione di ciò, quando si utilizza una regola che permette di scaricare le ipotesi, se ne può scaricare qualsiasi numero di occorrenze dalle foglie dell'albero di derivazione; la cosa più naturale è scaricarle tutte, ma è lecito scaricarne anche solo alcune o anche nessuna.

Per eliminare una negazione si può congiungere questa con una dimostrazione del suo opposto e raggiungere un assurdo:

$$\dfrac{\begin{array}{c}\Gamma \\ \vdots \\ \varphi\end{array} \quad \begin{array}{c}\Gamma' \\ \vdots \\ \neg\varphi\end{array}}{\bot}\ \mathrm{E}\neg$$

Infine un'ultima regola essenziale per poter dimostrare tutto ciò che è logicamente valido nella logica proposizionale è la seguente che schematizza il ragionamento per assurdo.

$$\dfrac{\begin{array}{c}\Gamma, [\neg\varphi]^1 \\ \vdots \\ \bot\end{array}}{\varphi}\ \mathrm{RA}_1$$

A una lettura poco attenta potrebbe sembrare che le regole I¬ e RA siano uguali, ma fondamentale tra le esse è che nella prima l'ipotesi φ appare positiva e nella conclusione appare nella forma negativa, mentre nella seconda regola, dal fatto che la negazione di una formula porti a contraddizione si deduce che vale la formula non negata. Intuitivamente la differenza sta nel fatto che aver dimostrato che φ porta a contraddizione effettivamente ci dice che $\neg\varphi$ vale (ricordando che $\neg\varphi$ può essere pensato come $\varphi \to \bot$). Mentre il fatto che la negazione di una formula porti a contraddizione richiede in aggiunta un applicazione del principio del terzo escluso ($\varphi \vee \neg\varphi$) per poter concludere che φ deve valere.

2.6.1.3 *Implicazione*

Sebbene non siano strettamente necessarie, poiché l'implicazione è riducibile ai connettivi $\wedge$ e $\neg$, discutiamo le regole di introduzione e eliminazione per $\to$, vista l'importanza di tale connettivo in matematica. Introdurre un'implicazione corrisponde a scaricare un'ipotesi. In altre parole, se abbiamo dimostrato ψ utilizzando le ipotesi in $\Gamma \cup \{\varphi\}$, possiamo incorporare l'ipotesi φ nella formula dimostrata e cancellarla dalle ipotesi. In altra parole abbiamo una dimostrazione di $\varphi \to \psi$ che utilizza ipotesi solo in Γ. In simboli:

$$\begin{array}{c} \Gamma, [\varphi]^1 \\ \vdots \\ \mathrm{I}{\to}_1 \dfrac{\psi}{\varphi \to \psi} \end{array}$$

Per capire come eliminare un'implicazione, dobbiamo pensare a come tale operazione ha luogo in una dimostrazione concreta. Se abbiamo dimostrato $\varphi \to \psi$, allora sappiamo che se vale φ allora vale ψ. Dunque se abbiamo una dimostrazione di $\varphi \to \psi$ e una dimostrazione di φ allora possiamo combinarle in una dimostrazione di ψ:

$$\begin{array}{c} \Gamma \qquad \Gamma' \\ \vdots \qquad\;\; \vdots \\ \mathrm{E}{\to} \dfrac{\varphi \quad \varphi \to \psi}{\psi} \end{array}$$

Questa regola viene a volte chiamata **modus ponens**.

2.6.1.4 *Disgiunzione*

Passiamo ora al connettivo $\vee$. Se volessimo introdurre una disgiunzione in una dimostrazione, una possibile maniera sarebbe quella di indebolire quanto già ottenuto, ad esempio φ, aggiungendo qualcosa della forma "oppure ψ" ottenendo dunque $\varphi \vee \psi$. Si noti che in maniera simile, si potrebbe giungere anche alla conclusione $\psi \vee \varphi$ (abbiamo già dimostrato che $\varphi \vee \psi \equiv \psi \vee \varphi$, ma le due formule sono oggetti sintattici diversi. Poiché in questa sezione siamo tornati al lavorare con la sintassi pura, dobbiamo specificare entrambi i casi). Dunque abbiamo due possibili regole di introduzione:

$$\begin{array}{c} \Gamma \\ \vdots \\ \mathrm{I}{\vee}\mathrm{Sx} \dfrac{\varphi}{\varphi \vee \psi} \end{array} \qquad \begin{array}{c} \Gamma \\ \vdots \\ \mathrm{I}{\vee}\mathrm{Dx} \dfrac{\psi}{\varphi \vee \psi} \end{array}$$

Per trovare un possibile candidato per la regola di eliminazione del $\vee$ bisogna pensare a come utilizziamo nella pratica matematica una formula del tipo $\varphi \vee \psi$. Un possibile uso si ha nel ragionamento per casi. Infatti, sapere che $\varphi \vee \psi$ è vera equivale a dire che i casi in cui è vera φ insieme a quelli in cui è vera ψ esauriscono tutti i casi possibili. Possiamo dunque utilizzare una formula $\varphi \vee \psi$ ragionando come segue: se da φ si può dedurre una formula χ e se da dalla formula ψ si può dedurre la stessa formula χ, ciò vuol dire che χ vale in tutti i casi possibili e dunque è vera senza assumere né φ né ψ. Rappresentiamo questo ragionamento in simboli come segue:

$$\dfrac{\begin{matrix}\Gamma \\ \vdots \\ \varphi \vee \psi\end{matrix} \qquad \begin{matrix}\Gamma, [\varphi]^1 \\ \vdots \\ \chi\end{matrix} \qquad \begin{matrix}\Gamma, [\psi]^1 \\ \vdots \\ \chi\end{matrix}}{\chi}\,E\vee_1$$

Le ipotesi φ e ψ sono state scaricate poiché non sono necessarie a dimostrare χ. Si pensi a una dimostrazione che si divide in due casi: n pari o n dispari; tali assunzioni non vengono citate nell'enunciato del teorema, poiché si è fatto vedere che in qualunque caso la tesi è comunque vera e tali casi esauriscono tutti quelli possibili.

Per comodità del lettore riassumiamo tutte le regole di deduzione nella Tabella 2.

Siamo pronti per dare una definizione formale di "dimostrazione". Chiameremo questi oggetti matematici *derivazioni* o *deduzioni* per poter continuare a usare senza confusione il termine *dimostrazione* per riferirci a quelle fatte nel meta-linguaggio. La struttura delle derivazione è una struttura ad albero. Al fine di rendere più brevi le dimostrazioni, diamo una definizione succinta di derivazione utilizzando solo le regole per $\wedge$ e $\neg$; lasciamo come esercizio la dimostrazione del fatto che tutte le altre regole di deduzione fin qui introdotte possono essere pensate come abbreviazioni per deduzioni più lunghe che utilizzino solo i connettivi $\wedge$ e $\neg$.

$$\mathrm{I}\wedge\ \dfrac{\begin{matrix}\Gamma & \Gamma' \\ \vdots & \vdots \\ \varphi & \psi\end{matrix}}{\varphi\wedge\psi} \qquad \mathrm{E}\wedge\mathrm{Sx}\ \dfrac{\begin{matrix}\Gamma \\ \vdots \\ \varphi\wedge\psi\end{matrix}}{\varphi} \qquad \mathrm{E}\wedge\mathrm{Dx}\ \dfrac{\begin{matrix}\Gamma \\ \vdots \\ \varphi\wedge\psi\end{matrix}}{\psi}$$

$$\mathrm{I}\vee\mathrm{Sx}\ \dfrac{\begin{matrix}\Gamma \\ \vdots \\ \varphi\end{matrix}}{\varphi\vee\psi} \qquad \mathrm{I}\vee\mathrm{Dx}\ \dfrac{\begin{matrix}\Gamma \\ \vdots \\ \psi\end{matrix}}{\varphi\vee\psi} \qquad \dfrac{\begin{matrix}\Gamma & \Gamma,[\varphi]^1 & \Gamma,[\psi]^1 \\ \vdots & \vdots & \vdots \\ \varphi\vee\psi & \chi & \chi\end{matrix}}{\chi}\ \mathrm{E}\vee_1$$

$$\mathrm{E}\!\to\ \dfrac{\begin{matrix}\Gamma & \Gamma' \\ \vdots & \vdots \\ \varphi & \varphi\to\psi\end{matrix}}{\psi} \qquad \mathrm{I}\!\to_1\ \dfrac{\begin{matrix}\Gamma,[\varphi]^1 \\ \vdots \\ \psi\end{matrix}}{\varphi\to\psi}$$

$$\mathrm{I}\neg_1\ \dfrac{\begin{matrix}\Gamma,[\varphi]^1 \\ \vdots \\ \bot\end{matrix}}{\neg\varphi} \qquad \mathrm{RA}_1\ \dfrac{\begin{matrix}\Gamma,[\neg\varphi]^1 \\ \vdots \\ \bot\end{matrix}}{\varphi} \qquad \mathrm{E}\neg\ \dfrac{\begin{matrix}\Gamma & \Gamma' \\ \vdots & \vdots \\ \varphi & \neg\varphi\end{matrix}}{\bot}$$

$$\mathrm{I}\!\leftrightarrow\ \dfrac{\begin{matrix}[\psi]^1 & [\varphi]^1 \\ \vdots & \vdots \\ \varphi & \psi\end{matrix}}{\varphi\leftrightarrow\psi} \qquad \mathrm{E}\!\leftrightarrow\ \dfrac{\begin{matrix}\Gamma & \Gamma' \\ \vdots & \vdots \\ \psi & \varphi\leftrightarrow\psi\end{matrix}}{\varphi} \qquad \mathrm{E}\!\leftrightarrow\ \dfrac{\begin{matrix}\Gamma & \Gamma' \\ \vdots & \vdots \\ \varphi & \varphi\leftrightarrow\psi\end{matrix}}{\psi}$$

Tabella 2: Regole della deduzione naturale

Definizione 2.47

Le **derivazioni** sono definite ricorsivamente dalle seguenti regole.

1. Se Γ è un insieme di formule e $\varphi \in \Gamma$, allora $\dfrac{\Gamma}{\varphi}$ è una derivazione di φ con ipotesi in Γ.
2. Se $\begin{array}{c}\Gamma\\ \vdots\\ \varphi\end{array}$ è una derivazione di φ con ipotesi in Γ e $\begin{array}{c}\Gamma'\\ \vdots\\ \psi\end{array}$ è una derivazione di ψ con ipotesi in Γ' allora $\dfrac{\begin{array}{cc}\Gamma & \Gamma'\\ \vdots & \vdots\\ \varphi & \psi\end{array}}{\varphi \wedge \psi}$ è una derivazione di $\varphi \wedge \psi$ con ipotesi in $\Gamma \cup \Gamma'$.
3. Se $\begin{array}{c}\Gamma\\ \vdots\\ \varphi \wedge \psi\end{array}$ è una derivazione di $\varphi \wedge \psi$ con ipotesi in Γ allora

$$\mathrm{E}\wedge\mathrm{Sx}\ \dfrac{\begin{array}{c}\Gamma\\ \vdots\\ \varphi \wedge \psi\end{array}}{\varphi} \qquad \text{e} \qquad \mathrm{E}\wedge\mathrm{Dx}\ \dfrac{\begin{array}{c}\Gamma\\ \vdots\\ \varphi \wedge \psi\end{array}}{\psi}$$

   sono derivazioni di φ e ψ, rispettivamente, entrambe con ipotesi in Γ.
4. Se $\begin{array}{c}\Gamma\\ \vdots\\ \perp\end{array}$ è una derivazione di $\perp$ con ipotesi in Γ allora $\mathrm{I}\neg_1\ \dfrac{\begin{array}{c}\Gamma, [\varphi]^1\\ \vdots\\ \perp\end{array}}{\neg\varphi}$ è una derivazione di $\neg\varphi$ con ipotesi in $\Gamma \setminus \{\varphi\}$.
5. Se $\begin{array}{c}\Gamma\\ \vdots\\ \varphi\end{array}$ e $\begin{array}{c}\Gamma'\\ \vdots\\ \neg\varphi\end{array}$ sono derivazioni allora lo è anche $\mathrm{E}\neg\ \dfrac{\begin{array}{cc}\Gamma & \Gamma'\\ \vdots & \vdots\\ \varphi & \neg\varphi\end{array}}{\perp}$.
6. Se $\begin{array}{c}\Gamma\\ \vdots\\ \perp\end{array}$ è una derivazione di $\perp$ con ipotesi in Γ, allora $\mathrm{RA}_1\ \dfrac{\begin{array}{c}\Gamma, [\neg\varphi]^1\\ \vdots\\ \perp\end{array}}{\varphi}$ è una derivazione di φ con ipotesi in $\Gamma \setminus \{\neg\varphi\}$.

Definizione 2.48

Diremo che una formula φ è **derivabile** da Γ se esiste una derivazione di φ con ipotesi (non scaricate) in Γ; diremo anche che φ è la conclusione della derivazione. In questo caso scriveremo $\Gamma \vdash \varphi$. Se φ deriva da un insieme vuoto di ipotesi (non scaricate) diremo che φ è un **teorema** e scriveremo $\vdash \varphi$.

Esempio 2.49. Di solito per trovare una derivazione di una formula si procede a ritroso partendo dalla formula e concentrarsi sull'ultimo connettivo applicato per costruire la formula e risalendo immaginando che l'ultima regola applicata è quella di introduzione di quel connettivo. Ovviamente questo modo di operare non si rivela sempre corretto, ma è sicuramente la prima ipotesi da controllare. Quindi se volessimo verificare che $\varphi \vdash \neg\neg\varphi$ procederemmo come segue. Poiché l'ultimo connettivo applicato per costruire $\neg\neg\varphi$ è la negazione, possiamo immaginare che la derivazione cercata si concluda con un'applicazione della regola $I_\neg$:

$$\begin{array}{c} [\neg\varphi]^1 \\ \vdots \\ \mathrm{I}\neg_1 \dfrac{\bot}{\neg\neg\varphi}\,, \end{array}$$

dove abbiamo indicato in alto la possibilità di scaricare ogni eventuale occorrenza della formula $\neg\varphi$ durante l'applicazione di quest'ultima regola. Ora, sappiamo che per giungere a $\bot$ abbiamo bisogno di due formule che siano una la negazione dell'altra, quindi perché non provare con φ e $\neg\varphi$:

$$\mathrm{I}\neg_1 \dfrac{\mathrm{E}\neg \dfrac{[\neg\varphi]^1 \qquad \varphi}{\bot}}{\neg\neg\varphi}\,.$$

Siamo così pervenuti a una dimostrazione di $\neg\neg\varphi$ con ipotesi in $\{\varphi\}$, cioè quanto voluto.

Proviamo ora a dimostrare che $\neg\neg\varphi \vdash \varphi$. In questo caso la conclusione non presenta connettivi espliciti, quindi l'ultima regola applicata non può essere un introduzione di un connettivo. Proviamo allora con un ragionamento per assurdo:

$$\begin{array}{c} [\neg\varphi]^1 \\ \vdots \\ \mathrm{RA}_1 \dfrac{\bot}{\varphi}\,. \end{array}$$

Dobbiamo allora scegliere come potremmo essere arrivati a una contraddizione. Poiché sappiamo di poter usare $\neg\neg\varphi$ nelle ipotesi proviamo come segue:

$$\mathrm{RA}_1\,\dfrac{\mathrm{E}\neg\,\dfrac{\neg\neg\varphi \qquad [\neg\varphi]^1}{\bot}}{\varphi}\quad .$$

Siamo dunque arrivati a scrivere una derivazione di φ con ipotesi in $\{\neg\neg\varphi\}$. Ciò dimostra che $\neg\neg\varphi \vdash \varphi$.

Esempio 2.50. Facciamo vedere che $\vdash \neg(\varphi \wedge \neg\neg(\psi \wedge \neg\varphi))$. Cominciamo scrivendo la formula per la quale vogliamo trovare una derivazione e concentriamoci sull'ultimo connettivo utilizzato nella costruzione della formula. In questo caso è una negazione, quindi possiamo provare a supporre che l'ultima regola di derivazione sia I$\neg$.

$$\mathrm{I}\neg_1\,\dfrac{\begin{array}{c}[\varphi \wedge \neg\neg(\psi \wedge \neg\varphi)]^1\\ \vdots\\ \bot\end{array}}{\neg(\varphi \wedge \neg\neg(\psi \wedge \neg\varphi))}\ .$$

Ci troviamo ora a dover dimostrare un assurdo avendo come ipotesi $\varphi \wedge \neg\neg(\psi \wedge \neg\varphi)$. Banalmente dall'ipotesi sappiamo di poter ottenere sia φ che $\neg\neg(\psi \wedge \neg\varphi)$ tramite E$\wedge$Sx e E$\wedge$Dx. Inoltre, grazie a quanto visto nell'Esempio 2.49, sappiamo che da $\neg\neg(\psi \wedge \neg\varphi)$ è possibile derivare $\psi \wedge \neg\varphi$. Da quest'ultimo, con E$\wedge$Dx, sappiamo derivare $\neg\varphi$ e quindi abbiamo tutti gli ingredienti per ottenere l'assurdo:

$$\mathrm{I}\neg_1\,\dfrac{\mathrm{E}\neg\,\dfrac{\mathrm{E}\wedge\mathrm{Sx}\,\dfrac{[\varphi \wedge \neg\neg(\psi \wedge \neg\varphi)]^1}{\varphi} \qquad \mathrm{E}\wedge\mathrm{Dx}\,\dfrac{\dfrac{\mathrm{E}\wedge\mathrm{Dx}\,\dfrac{[\varphi \wedge \neg\neg(\psi \wedge \neg\varphi)]^1}{\neg\neg(\psi \wedge \neg\varphi)}}{\psi \wedge \neg\varphi}\,\text{Esempio 2.49}}{\neg\varphi}}{\bot}}{\neg(\varphi \wedge \neg\neg(\psi \wedge \neg\varphi))}\quad .$$

Proposizione 2.51. *Le seguenti osservazioni hanno dimostrazioni immediate:*

1. *Se $\varphi \in \Gamma$ allora $\Gamma \vdash \varphi$.*
2. *Se $\Gamma \vdash \varphi$ e $\Gamma' \vdash \psi$ allora $\Gamma \cup \Gamma' \vdash \varphi \wedge \psi$.*
3. *Se $\Gamma \vdash \bot$ allora $\Gamma \vdash \varphi$, per qualsiasi φ (**ex falsum quodlibet**).*
4. *Se $\Gamma \cup \{\neg\varphi\} \vdash \bot$ allora $\Gamma \vdash \varphi$.*

Esercizio 2.52. Utilizzando tutte le regole presenti nella Tabella 2, produrre derivazioni per i seguenti fatti:

1. $\vdash \varphi \to (\psi \to \varphi)$,
2. $\varphi \to (\neg\varphi \to \psi)$,

3. $(\varphi \to \psi) \to ((\psi \to \sigma) \to (\varphi \to \sigma))$,
4. $(\varphi \to \psi) \leftrightarrow (\neg\psi \to \neg\varphi)$,
5. $\neg\neg\varphi \leftrightarrow \varphi$,
6. $\varphi \to (\psi \to \chi) \leftrightarrow (\varphi \wedge \psi \to \chi)$,
7. $\bot \leftrightarrow (\neg\varphi \leftrightarrow \varphi)$.

Teorema 2.53 (Deduzione, versione sintattica)

Se ψ e φ sono formule e Γ è un insieme di formule allora vale: $\Gamma \cup \{\psi\} \vdash \varphi$ se, e soltanto se, $\Gamma \vdash \psi \to \varphi$.

Dimostrazione. La dimostrazione è un immediata applicazione delle regole $I \to$ e $E \to$. $\square$

Lemma 2.54 (Compattezza, versione sintattica)**.** *Se φ è una formula e Γ è un insieme di formule allora vale: $\Gamma \vdash \varphi$ se, e soltanto se, esiste un sottoinsieme finito $\Delta \subseteq \Gamma$ tale che $\Delta \vdash \varphi$.*

Dimostrazione. Poiché una derivazione è un oggetto finito essa coinvolge solo un numero finito di regole. In ogni regola vengono utilizzate solo un numero finito di formule. Quindi data una derivazione di φ con ipotesi in Γ è sempre possibile ottenere una deduzione con un numero finito di ipotesi, eliminando tutte le formule che non sono necessarie in nessun passo di derivazione. $\square$

Esercizio 2.55. Dimostrare che le regole riassunte nella Tabella 2 per i connettivi $\vee$ e $\to$ sono derivabili dalle altre assumendo che $\varphi \vee \psi$ sia un'abbreviazione per $\neg(\neg\varphi \wedge \neg\psi)$ e $\varphi \to \psi$ sia un'abbreviazione per $\neg(\varphi \wedge \neg\psi)$.

Introduciamo infine un concetto simile alla complessità di una formula per le derivazioni.

Definizione 2.56

Definiamo la **lunghezza** di una derivazione $\begin{array}{c}\Gamma\\ \vdots\\ \varphi\end{array}$ ricorsivamente come segue:

1. Se $\varphi \in \Gamma$ e la derivazione è del tipo $\dfrac{\Gamma}{\varphi}$ allora la lunghezza è 0;

2. Se la derivazione è del tipo

$$\dfrac{\begin{array}{c}\Gamma\\ \vdots\\ \varphi\end{array} \quad \begin{array}{c}\Gamma'\\ \vdots\\ \psi\end{array}}{\varphi \wedge \psi}\ ,$$

allora la lunghezza è definita come il massimo tra le lunghezze di $\begin{array}{c}\Gamma\\ \vdots\\ \varphi\end{array}$ e $\begin{array}{c}\Gamma'\\ \vdots\\ \psi\end{array}$, più 1;

3. Se la derivazione è del tipo

$$E\wedge Sx\ \dfrac{\begin{array}{c}\Gamma\\ \vdots\\ \varphi \wedge \psi\end{array}}{\varphi} \qquad \text{oppure} \qquad E\wedge Dx\ \dfrac{\begin{array}{c}\Gamma\\ \vdots\\ \varphi \wedge \psi\end{array}}{\psi}$$

allora la lunghezza è definita come la lunghezza di $\begin{array}{c}\Gamma\\ \vdots\\ \varphi \wedge \psi\end{array}$ più 1.

4. Se la derivazione è del tipo

$$I\neg_1\ \dfrac{\begin{array}{c}\Gamma, [\varphi]^1\\ \vdots\\ \bot\end{array}}{\neg\varphi}$$

allora la lunghezza è definita come la lunghezza di $\begin{array}{c}\Gamma\\ \vdots\\ \bot\end{array}$, più 1.

5. Se la derivazione è del tipo

$$E\neg\ \dfrac{\begin{array}{c}\Gamma\\ \vdots\\ \varphi\end{array} \quad \begin{array}{c}\Gamma'\\ \vdots\\ \neg\varphi\end{array}}{\bot}$$

allora la lunghezza è definita come il massimo tra le lunghezza di $\begin{array}{c}\Gamma\\ \vdots\\ \varphi\end{array}$ e $\begin{array}{c}\Gamma'\\ \vdots\\ \neg\varphi\end{array}$ più 1.

6. Se la derivazione è del tipo $$\dfrac{\begin{array}{c}\Gamma, [\neg\varphi]^1\\ \vdots \\ \bot\end{array}}{\varphi}\,\text{RA}_1$$ allora la lunghezza è definita come la lunghezza di $\begin{array}{c}\Gamma\\ \vdots\\ \bot\end{array}$ più 1.

2.6.2 *Adeguatezza e completezza della deduzione naturale*

Come sono collegati tra loro teoremi e tautologie? Da un lato ci aspettiamo che ci sia una derivazione di φ da Γ solo se $\Gamma \models \varphi$. D'altro canto, sarebbe utile anche sapere se il viceversa vale: esiste una derivazione di φ da Γ se $\Gamma \models \varphi$? In questa sezione vedremo che entrambe queste implicazioni valgono. La prima implicazione è molto più facile da provare della seconda.

Teorema 2.57 (Adeguatezza)

Se Γ è un insieme di formule φ è una formula tale che $\Gamma \vdash \varphi$, allora $\Gamma \models$ f.

Dimostrazione. Dimostreremo l'enunciato per induzione sulla lunghezza della derivazione $\Gamma \vdash \varphi$. Se $\varphi \in \Gamma$ allora l'enunciato è banale. Supponiamo quindi che l'enunciato sia vero per tutte le derivazioni di lunghezza minori di $n+1$ e dimostriamolo per quelle di lunghezza $n+1$. Supponiamo data una derivazione di lunghezza $n+1$ di φ con ipotesi in Γ e ragioniamo per casi a seconda di quale sia l'ultima regola applicata.

CASO 1 L'ultima regola è I$\wedge$, dunque la derivazione data è della forma:

$$\dfrac{\begin{array}{c}\Gamma_1\\ \vdots\\ \psi_1\end{array} \quad \begin{array}{c}\Gamma_2\\ \vdots\\ \psi_2\end{array}}{\psi_1 \wedge \psi_2}\,\text{I}\wedge\ ,$$

con $\varphi = \psi_1 \wedge \psi_2$ e $\Gamma_1 \cup \Gamma_2 = \Gamma$. Ma allora le derivazioni $\begin{array}{c}\Gamma_1\\ \vdots\\ \psi_1\end{array}$ e $\begin{array}{c}\Gamma_2\\ \vdots\\ \psi_2\end{array}$ hanno lunghezza strettamente minore di $n+1$, quindi per ipotesi induttiva possiamo dedurre $\Gamma_1 \models \psi_1$ e $\Gamma_2 \models \psi_2$. Da ciò segue immediatamente che $\Gamma = \Gamma_1 \cup \Gamma_2 \models \psi_1 \wedge \psi_2$.

caso 2 L'ultima regola è $E\wedge Sx$, dunque la derivazione data è della forma:

$$\begin{matrix}\Gamma\\ \vdots\\ \mathrm{E}\wedge\mathrm{Sx}\,\dfrac{\varphi\wedge\psi}{\varphi}\end{matrix},$$

con ψ formula arbitraria. Ma allora la derivazione $\begin{matrix}\Gamma\\ \vdots\\ \varphi\wedge\psi\end{matrix}$ ha lunghezza strettamente minore di $n+1$, quindi per ipotesi induttiva possiamo dedurre $\Gamma\models\varphi\wedge\psi$. Da ciò segue immediatamente che $\Gamma\models\varphi$. Il caso della regola $E\wedge Sx$ è simmetrico.

caso 3 L'ultima regola è $I\neg$, dunque la derivazione data è della forma:

$$\begin{matrix}\Gamma,[\psi]^1\\ \vdots\\ \mathrm{I}\neg_1\,\dfrac{\bot}{\neg\psi}\end{matrix},$$

con $\varphi=\neg\psi$. Ma allora la derivazione $\begin{matrix}\Gamma\\ \vdots\\ \bot\end{matrix}$ ha lunghezza strettamente minore di $n+1$, quindi per ipotesi induttiva possiamo dedurre $\Gamma\models\bot$. Dunque Γ non è soddisfacibile e dal Punto 1 del Lemma 2.38 segue che $\Gamma\setminus\{\psi\}\models\neg\psi$.

caso 4 L'ultima regola è $E\neg$, dunque la derivazione data è della forma:

$$\mathrm{E}\neg\,\dfrac{\begin{matrix}\Gamma_1\\ \vdots\\ \psi\end{matrix}\quad\begin{matrix}\Gamma_2\\ \vdots\\ \neg\psi\end{matrix}}{\bot},$$

con ψ arbitraria, $\varphi=\bot$ e $\Gamma_1\cup\Gamma_2=\Gamma$. Allora le derivazione $\begin{matrix}\Gamma_1\\ \vdots\\ \psi\end{matrix}$ e $\begin{matrix}\Gamma_2\\ \vdots\\ \neg\psi\end{matrix}$ ha entrambe lunghezza strettamente minore di $n+1$, quindi per ipotesi induttiva possiamo dedurre $\Gamma_1\models\psi$ e $\Gamma_2\models\neg\psi$. Dunque $\Gamma\models\psi_1\wedge\psi_2$, o equivalentemente, $\Gamma\models\bot$

caso 5 Infine, supponiamo che l'ultima regola applicata sia RA, dunque la derivazione data è della forma:

$$\begin{matrix}\Gamma,[\neg\varphi]^1\\ \vdots\\ \mathrm{RA}_1\,\dfrac{\bot}{\varphi}\end{matrix}.$$

Allora la derivazione $\begin{array}{c}\Gamma\\ \vdots\\ \bot\end{array}$ ha lunghezza strettamente minore di $n+1$, quindi per ipotesi induttiva possiamo dedurre $\Gamma \models \bot$. Dunque Γ non è soddisfacibile e dal Punto 1 del Lemma 2.38 segue che $\Gamma \setminus \{\neg\varphi\} \models \varphi$.

□

Definizione 2.58

Un insieme di formule Γ è detto **incoerente** se $\Gamma \vdash \bot$, altrimenti è detto **coerente**.

Esempio 2.59. È facile vedere che l'insieme $\Gamma = \{p, q \wedge p, \neg q\}$ è incoerente, poiché è semplice costruire una derivazione di $\bot$ con ipotesi in Γ. D'altro canto, verificare che l'insieme $\Lambda = \{p, q \vee p, \neg q\}$ è coerente è più laborioso poiché bisognerebbe far vedere che *nessuna* derivazione con ipotesi in Λ può concludersi con $\bot$.

Corollario 2.60. *Se un insieme di formule è soddisfacibile allora è coerente.*

Dimostrazione. Dimostriamo la contronominale. Se un insieme di formule Γ è incoerente allora $\Gamma \vdash \bot$. Dal Teorema 2.57 segue che $\Gamma \models \bot$ e questo significa che Γ è insoddisfacibile. □

Per l'altra implicazione abbiamo bisogno di alcuni risultati preliminari.

Lemma 2.61. *Se Γ è un insieme di formule, le seguenti condizioni sono equivalenti:*

(i) Γ è incoerente,

(ii) per ogni formula φ si ha $\Gamma \vdash \varphi$.

(iii) esiste una formula φ per cui $\Gamma \vdash \varphi$ e $\Gamma \vdash \neg\varphi$,

Dimostrazione. L'implicazione (i) $\to$ (ii) è un'immediata applicazione di *ex falsum quodlibet* (Proposizione 2.51, Punto 3).

L'implicazione (ii) $\to$ (iii) è banale.

Pe dimostrare l'implicazione (iii) $\to$ (i) basta usare la regola di eliminazione della negazione. □

Lemma 2.62. *Se $\Gamma \nvdash \varphi$ allora $\Gamma \cup \{\neg\varphi\}$ è coerente.*

Dimostrazione. Dimostriamo la contronominale. Se $\Gamma \cup \{\neg\varphi\}$ è incoerente, abbiamo $\Gamma \cup \{\neg\varphi\} \vdash \bot$, applicando la regola RA si ottiene che $\Gamma \vdash \varphi$ e il lemma è provato. □

Proposizione 2.63. *Un insieme Σ di formule è incoerente se e soltanto se ha un sottoinsieme finito incoerente.*

Dimostrazione. Per il Lemma 2.54, è possibile derivare una contraddizione da un insieme di formule se e soltanto se è possibile farlo anche da un suo sottoinsieme finito. □

Per ottenere il risultato di completezza abbiamo bisogno di un ulteriore definizione.

Definizione 2.64

Un insieme di formule Σ è **massimalmente coerente** se Σ è coerente ma $\Sigma \cup \{\varphi\}$ è incoerente per ogni $\varphi \notin \Sigma$.

Esercizio 2.65. Sia ν una valutazione. Mostrare che $\Sigma = \{\, \varphi \mid \nu(\varphi) = \mathsf{T} \,\}$ è massimalmente coerente.

Abbiamo bisogno di qualche fatto addizionale sugli insiemi massimalmente coerenti. Le prossime asserzioni sono molto simili a quelle già viste per le teorie massimalmente soddisfacibili nel Lemma 2.41.

Proposizione 2.66. *Se Σ è un insieme di formule massimalmente coerente, allora per ogni coppia di formule φ, ψ valgono le seguenti.*

1. *Se $\Sigma \vdash \varphi$, allora $\varphi \in \Sigma$.*
2. *$\neg\varphi \in \Sigma$ se, e soltanto se, $\varphi \notin \Sigma$.*
3. *$\varphi \wedge \psi \in \Sigma$ se, e soltanto se, $\varphi, \psi \in \Sigma$.*

Esercizio 2.67. Dimostrare che se Σ è un insieme di formule massimalmente coerente, allora per ogni coppia di formule φ, ψ vale che $\varphi \to \psi \in \Sigma$ se, e soltanto se, $\varphi \notin \Sigma$ o $\psi \in \Sigma$.

Come per il risultato di compattezza della sezione precedente, è cruciale sapere che ogni insieme coerente di formule può essere esteso a un insieme di formule massimalmente coerente.

Teorema 2.68 (Lemma di Lindenbaum)

Se Γ è un insieme coerente di formule allora esiste un insieme di formule massimalmente coerente Σ tale che $\Gamma \subseteq \Sigma$.

Dimostrazione. Una dimostrazione generale di questo risultato può essere fatta, riproducendo *mutatis mutandis* quella del Lemma 2.39. Proponiamo una dimostrazione alternativa più costruttiva nel caso in cui l'insieme `Form` è enumerabile. Se `Form` è enumerabile possiamo assumere che le formule siano in una sequenza del tipo $\varphi_1, \varphi_2, \ldots$. Definiamo una sequenza non decrescente di insiemi, tali che la loro unione sia massimalmente coerente.

$$\Gamma_0 := \Gamma,$$
$$\Gamma_{n+1} := \begin{cases} \Gamma_n \cup \{\varphi_n\} & \text{se è coerente} \\ \Gamma_n & \text{altrimenti,} \end{cases}$$
$$\Sigma := \bigcup_{n \in \mathbb{N}} \Gamma_n$$

L'insieme Σ è coerente in base alla Proposizione 2.63, infatti ognuno dei suoi sottoinsiemi finiti è contenuto in qualche Γ_n e questi sono coerenti per costruzione.

L'insieme Σ è massimalmente coerente. Se infatti $\varphi \notin \Sigma$, allora esisterà un n per cui $\varphi = \varphi_n$ e, per costruzione, $\Gamma_n \cup \{\varphi_n\}$ non è coerente. Dunque anche $\Sigma \cup \{\varphi\}$ non è coerente. □

Lemma 2.69. *Un insieme di formule è coerente se, e soltanto se, è soddisfacibile.*

Dimostrazione. Un'implicazione è già stata dimostrata in Corollario 2.60. Per l'altra supponiamo che Γ sia coerente, allora per il Teorema 2.68 esiste Σ massimalmente coerente che estende Γ. Definiamo:

$$v_\Sigma(p_i) = 1 \text{ se, soltanto se, } p_i \in \Sigma.$$

e dimostriamo che

$$\tilde{v}_\Sigma(\varphi) = 1 \text{ se, soltanto se, } \varphi \in \Sigma. \tag{2}$$

Dimostrazione la (2) per induzione sulla complessità di φ. Il passo base è dato direttamente dalla definizione di $v_\Sigma(p)$.

Supponiamo quindi che $\varphi = \varphi_1 \wedge \varphi_2$. Allora si ha $v_\Sigma(\varphi) = 1$ se, e soltanto se, $v_\Sigma(\varphi_1 \wedge \varphi_2) = 1$ se, e soltanto se, $v_\Sigma(\varphi_1) = v_\Sigma(\varphi_2) = 1$ se, e soltanto se, per ipotesi induttiva, $\varphi_1, \varphi_2 \in \Sigma$ se, e soltanto se, per il punto 2 della Proposizione 2.66, $\varphi_1 \wedge \varphi_2 \in \Sigma$. Se invece $\varphi = \neg\varphi_1$. Si ha che $v_\Sigma(\varphi) = 1$ se, e soltanto se, $v_\Sigma(\varphi_1) = 0$. Per ipotesi induttiva quest'ultima è equivalente a $\varphi_1 \notin \Sigma$. A sua volta, per la Proposizione 2.66 ciò è equivalente a $\varphi = \neg\varphi_1 \in \Sigma$. □

Il Lemma 2.69 asserisce implicitamente l'equivalenza $\vdash$ e $\models$, come vedremo nel prossimo teorema.

Teorema 2.70 (Completezza della logica proposizionale)

Se Γ è un insieme di formule e φ è una formula tale che $\Gamma \models \varphi$, allora $\Gamma \vdash \varphi$.

Dimostrazione. Dimostriamo la contronominale, cioè $\Gamma \nvdash \varphi$ implica $\Gamma \not\models \varphi$. Se $\Gamma \nvdash \varphi$ allora, per il Lemma 2.62, $\Gamma \cup \{\neg\varphi\}$ è coerente. Dunque, per il Lemma 2.69, esiste $\tilde{v}$ tale che $\tilde{v}(\beta) = 1$ per ogni $\beta \in \Gamma \cup \{\neg\varphi\}$. Quindi $\tilde{v}(\gamma) = 1$ per ogni $\gamma \in \Gamma$ e $\tilde{v}(\varphi) = 0$. □

2.7 COMPLEMENTI: IL CALCOLO DEI TABLEAUX.

Verificare che una formula proposizionale ben formata sia una tautologia è un compito abbastanza semplice, poiché è necessaria solo un po' di pazienza per scrivere la sua tavola di verità e verificare che nell'ultima colonna siano presenti solo 1. Tuttavia la pazienza necessaria potrebbe essere davvero tanta poiché i casi considerati nella tavola di verità sono 2^n dove n è il numero di variabili proposizionali distinte presenti nella data formula.

In questa breve sezione presenteremo un metodo più efficace per la verifica di tautologie. L'algoritmo, che chiameremo `Tab` costruisce, a partire da una formula, un albero di possibili valutazioni per quella formula. Partendo dalla negazione della formula data, se un ramo dell'albero dovesse arrivare a conclusione positivamente, otterremmo una valutazione che falsifica la formula data; questa non sarebbe dunque una tautologia. Se viceversa l'algoritmo dovesse chiudere tutti i rami negativamente (cioè con qualche contraddizione all'interno di ogni ramo) allora vorrebbe dire che è impossibile falsificare la formula data o, equivalentemente, che essa è una tautologia.

Il primo passo, data la formula φ, è porla falsa, scriveremo dunque:

$$\mathsf{F}(\varphi)$$

I successivi passi da effettuare nell'algoritmo `Tab` dipendono, come sempre, dalla *forma* della formula data.

Se $\varphi = \varphi_1 \wedge \varphi_2$ allora l'albero si prolunga come segue:

$$\begin{array}{ccc} & \mathsf{F}(\varphi_1 \wedge \varphi_2) & \\ / & & \backslash \\ \mathsf{F}(\varphi_1) & & \mathsf{F}(\varphi_2) \end{array}$$

Intuitivamente, se vogliamo falsificare $\varphi_1 \wedge \varphi_2$ basta falsificare o φ_1 o φ_2.

Se $\varphi = \varphi_1 \vee \varphi_2$ allora l'albero si prolunga come segue:

$$\begin{array}{c} \mathsf{F}(\varphi_1 \vee \varphi_2) \\ | \\ \mathsf{F}(\varphi_1) \\ | \\ \mathsf{F}(\varphi_2) \end{array}$$

Intuitivamente, se vogliamo falsificare $\varphi_1 \vee \varphi_2$ bisogna falsificare contemporaneamente (cioè sullo stesso ramo) sia φ_1 che φ_2.

Se $\varphi = \varphi_1 \to \varphi_2$ allora l'albero si prolunga come segue:

$$\begin{array}{c} \mathsf{F}(\varphi_1 \to \varphi_2) \\ | \\ V(\varphi_1) \\ | \\ \mathsf{F}(\varphi_2) \end{array}$$

Intuitivamente, se vogliamo falsificare $\varphi_1 \to \varphi_2$ bisogna contemporaneamente verificare φ_1 e falsificare φ_2.

Se $\varphi = \neg\varphi_1$ allora l'albero si prolunga come segue:

$$\begin{array}{c} \mathsf{F}(\neg\varphi_1) \\ | \\ V(\varphi_1) \end{array}$$

Intuitivamente, se vogliamo falsificare $\neg\varphi_1$ bisogna verificare φ_1.

Abbiamo così visto tutti quattro casi possibile per prolungare una foglia $\mathsf{F}(\varphi)$. Notiamo però che facendo questo, si creano dei nodi dove al posto di F c'è V. Dobbiamo quindi descrivere come procede l'algoritmo nel caso il nodo da prolungare si del tipo $V(\varphi)$. Abbiamo di nuovo quattro casi possibili.

Se $\varphi = \varphi_1 \wedge \varphi_2$ allora l'albero si prolunga come segue:

$$\begin{array}{c} V(\varphi_1 \wedge \varphi_2) \\ | \\ V(\varphi_1) \\ | \\ V(\varphi_2) \end{array}$$

Intuitivamente, se vogliamo verificare $\varphi_1 \wedge \varphi_2$ dobbiamo verificare contemporaneamente φ_1 e φ_2.

Se $\varphi = \varphi_1 \vee \varphi_2$ allora l'albero si prolunga come segue:

$$\begin{array}{ccc} & V(\varphi_1 \vee \varphi_2) & \\ / & & \backslash \\ V(\varphi_1) & & V(\varphi_2) \end{array}$$

Intuitivamente, se vogliamo verificare $\varphi_1 \vee \varphi_2$ bisogna verificare almeno uno tra φ_1 e φ_2.

Se $\varphi = \varphi_1 \to \varphi_2$ allora l'albero si prolunga come segue:

$$
\begin{array}{ccc}
 & V(\varphi_1 \to \varphi_2) & \\
\swarrow & & \searrow \\
F(\varphi_1) & & V(\varphi_2)
\end{array}
$$

Intuitivamente, se vogliamo verificare $\varphi_1 \to \varphi_2$ possiamo o falsificare l'ipotesi, cioè φ_1 o verificare la tesi, cioè φ_2.

Se $\varphi = \neg\varphi_1$ allora l'albero si prolunga come segue:

$$
\begin{array}{c}
V(\neg\varphi_1) \\
| \\
F(\varphi_1)
\end{array}
$$

Intuitivamente, se vogliamo verificare $\neg\varphi_1$ bisogna falsificare φ_1.

Vediamo ora qualche esempio di utilizzo dell'algoritmo `Tab` per controllare che una formula proposizionale sia o no una tautologia.

Esempio 2.71. Utilizzando il metodo degli alberi semantici stabiliamo se la seguente formula è una tautologia:

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

Cominciamo ricordando che vogliamo cercare di falsificare la formula, perciò scriveremo

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

Osservando la formula vedremo che stiamo tentando di falsificare una congiunzione di formule composte. Applichiamo quindi la regola corrispondente, prolungando l'albero come segue:

$$
\begin{array}{ccc}
 & F((A \to (B \vee \neg A)) \wedge B) & \\
\swarrow & & \searrow \\
F(B) & & \\
 & & F((A \to (B \vee \neg A)))
\end{array}
$$

A questo punto il ramo di sinistra è già arrivato a conclusione, poichéé c'è solo una formula atomica. Al contrario, possiamo proseguire con il ramo di destra, notando che questa volta si tratta di falsificare una implicazione.

$$
\begin{tikzcd}
& F((A \to (B \lor \neg A)) \land B) \arrow[dl, dash] \arrow[d, dash] \\
F(B) & F((A \to B \lor \neg A)) \arrow[d, dash] \\
& V(A) \arrow[d, dash] \\
& F(B \lor \neg A)
\end{tikzcd}
$$

Infine applichiamo la regola per falsificare una disgiunzione.

$$
\begin{tikzcd}
& F((A \to (B \lor \neg A)) \land B) \arrow[dl, dash] \arrow[d, dash] \\
F(B) & F((A \to B \lor \neg A)) \arrow[d, dash] \\
& V(A) \arrow[d, dash] \\
& F(B \lor \neg A) \arrow[d, dash] \\
& F(\neg A) \arrow[d, dash] \\
& F(B) \arrow[d, dash] \\
& V(A)
\end{tikzcd}
$$

Concludiamo che la formula data inizialmente non è una tautologia, perché i rami sono rimasti aperti. Infatti, come suggerito dall'albero, basta considerare il caso in cui A è vera e B è falsa per trovare una valutazione che non soddisfa la formula data.

Esempio 2.72. Vediamo un altro esempio.

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

$$F(((A \lor B) \land \neg A) \to B)$$
$$F(B)$$
$$V((A \lor B) \land \neg A)$$
$$V(\neg A)$$
$$V(A \lor B)$$
$$F(A)$$
$$V(B) \qquad V(A)$$
$$= \qquad\quad =$$

È una tautologia perché tutti riami sono chiusi.

Esempio 2.73. Utilizzando il metodo degli alberi semantici controlliamo se la seguente formula è una tautologia:

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

$$F((A \to (B \lor \neg A)) \land B)$$
$$F(B) \qquad\qquad F((A \to B \lor \neg A))$$
$$V(A)$$
$$F(B \lor \neg A)$$
$$F(\neg A)$$
$$F(B)$$
$$V(A)$$

Non è una tautologia, perché i rami sono rimasti aperti.

3 ALGEBRE DI BOOLE.

"La matematica è l'arte di dare lo stesso nome a cose diverse."
Henri Poincaré (1854-1912)

In questo capitolo intraprendiamo un ulteriore studio dei connettivi, seguendo questa volta un approccio assiomatico. Cerchiamo quindi di trovare un piccolo numero di equazioni, soddisfatte dai connettivi, che li caratterizzino completamente.

3.1 ORDINI PARZIALI E RETICOLARI

Osservando le proprietà dell'implicazione si vede facilmente che valgono una sorta di *riflessività* e *transitività*. Le relazioni che godono di queste proprietà prendono il nome di *preordini*.

Dato un insieme X intuitivamente pensiamo a una relazione n-aria su di esso come una legge che lega una n-upla di elementi di X. Una definizione più formale è la seguente.

Definizione 3.1

Dato un insieme X, si dice **relazione** n-aria su X un qualunque sottoinsieme $R \subseteq X^n$. Se $n = 2$, diremo che la relazione è **binaria** e che $x \in X$ è in relazione con $y \in X$ se, e solo se, $(x, y) \in R$ e scriveremo alternativamente xRy.

Definizione 3.2

Dato un insieme X, una relazione binaria $\rho \subseteq X \times X$ è un **preordine** se è una relazione riflessiva e transitiva. La coppia $\langle X, \rho \rangle$ si dirà insieme preordinato.

Alcuni preordini, svolgono un ruolo fondamentale in Matematica e in Logica; sono i preordini in cui vale l'anti-simmetria.

Definizione 3.3

Una **relazione d'ordine** (parziale) su X è una relazione binaria, indicata con $\leqslant$, che soddisfa le seguenti proprietà:

1. **riflessività**: $\forall x \in X$, $x \leqslant x$;
2. **anti-simmetria**: $\forall x, y \in X$, se $x \leqslant y$ e $y \leqslant x$ allora $x = y$;
3. **transitività**: $\forall x, y, z \in X$, se $x \leqslant y$ e $y \leqslant z$ allora $x \leqslant z$.

La coppia $\langle X, \leqslant \rangle$, con $X \neq \emptyset$, è detta **insieme parzialmente ordinato**.

La relazione $\leqslant$ si dirà di **ordine totale** (equivalentemente, diremo che X è una **catena** o X è **totalmente ordinato**) se per ogni coppia di elementi $x, y \in X$ si ha $x \leqslant y$ oppure $y \leqslant x$.

Esempio 3.4.

1. Gli insiemi numerici $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ sono totalmente ordinati dal loro ordine naturale.
2. Sia A insieme non vuoto. L'insieme delle parti di A è parzialmente ordinato dalla relazione di inclusione $\subseteq$. In altre parole, $\langle \wp(A), \subseteq \rangle$ è ordine parziale.
3. La relazione di divisibilità su $\mathbb{N}$ è una relazione di ordine parziale, dove xRy se, e solo se, $x \mid y$ (x divide y).
4. La relazione di divisibilità su $\mathbb{Z}$ non è un ordine parziale. In particolare, non è antisimmetrica: infatti, ad esempio, $5 \mid -5$ e $-5 \mid 5$ ma $5 \neq -5$.

È sempre possibile passare da un preordine a un ordine parziale in maniera canonica.

Proposizione 3.5. *Sia $\langle X, \rho \rangle$ un insieme preordinato e si consideri la relazione $\sim_\rho$ definita come segue:*

$$x \sim_\rho y \text{ se e soltanto se } (x, y) \in \rho \text{ e } (y, x) \in \rho.$$

La relazione $\sim_\rho$ è di equivalenza e l'insieme quoziente $X/\sim_\rho$ è parzialmente ordinato dalla seguente relazione: $[x] \leqslant [y]$ se, e solo se, $(x, y) \in \rho$.

Dimostrazione. Cominciamo dimostrando che $\sim_\rho$ è una relazione di equivalenza. La relazione è riflessiva e transitiva per la riflessività e transitività di ρ. La simmetria di $\sim_\rho$ segue immediatamente dalla definizione, infatti si ha $x \sim_\rho y$ se, e solo se, $(x, y) \in \rho$ e $(y, x) \in \rho$ se, e solo se, $(y, x) \in \rho$ e $(x, y) \in \rho$ se, e solo se, $y \sim_\rho x$.

Possiamo quindi considerare l'insieme quoziente $X/\sim_\rho$ e definire la relazione

$$[x] \leqslant [y] \text{ se, e solo se, } (x, y) \in \rho.$$

Verifichiamo che la definizione è ben posta. Sia $[x] \leqslant [y]$ e siano $x' \in [x]$ e $y' \in [y]$. Allora $x' \sim_\rho x$ e $y' \sim_\rho y$, quindi $(x, y) \in \rho$, $(x', x) \in \rho$ e $(y, y') \in \rho$. Per la transitività di ρ segue che $(x', y') \in \rho$ e di conseguenza $[x'] \leqslant [y']$.

La verifica che $\leqslant$ è un ordine parziale è lasciata al lettore. $\square$

Notazione 3.6. Utilizzeremo il simbolo di ordine **stretto** $<$ per abbreviare "$x \leqslant y$ e $x \neq y$".

Nel caso di insiemi parzialmente ordinati e finiti è possibile rappresentare graficamente l'ordine tramite linee che indicano che l'elemento in basso è minore dell'elemento più in alto (diagrammi di Hasse). Si assume tacitamente la riflessività e transitività di tali collegamenti.

Esempio 3.7. Sia $X = \{a, b, c, d, e\}$, ordinato nel seguente modo: $a \leqslant b, c, d \leqslant e$, dove b, c, d non sono confrontabili. Sia $Y = \{x, y, z, w, t\}$, ordinato nel seguente modo: $w, t \leqslant z \leqslant x, y$ dove le coppie w, t e x, y non sono confrontabili. Le rappresentazioni grafiche di $\langle X, \leqslant \rangle$ e $\langle Y, \leqslant \rangle$ sono in Figura 1.

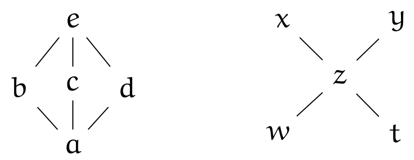


Figura 1: A sinistra l'insieme ordinato $\langle X, \leqslant \rangle$ e a destra $\langle Y, \leqslant \rangle$

Sia $W = \{a, b, c, d, e\}$, ordinato nel seguente modo: $e \geqslant d \geqslant c \geqslant b \geqslant a$. Sia $Z = \{x, y, z, t, w\}$, ordinato nel seguente modo: $x \geqslant y \geqslant z$ e $t \geqslant w$ con i primi tre elementi incomparabili con i secondi. Le rappresentazioni grafiche di $\langle W, \leqslant \rangle$ e $\langle Z, \leqslant \rangle$ sono in Figura 2.

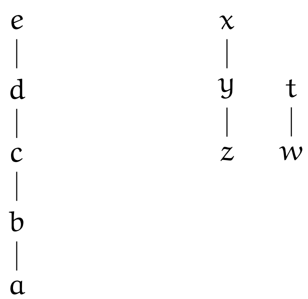


Figura 2: A sinistra l'insieme ordinato $\langle W, \leqslant \rangle$ e a destra $\langle Z, \leqslant \rangle$

Per poter individuare le proprietà fondamentali dei connettivi $\wedge$ e $\vee$ è utile ricordare alcune definizioni nell'ambito delle relazioni d'ordine.

Definizione 3.8

Sia $\langle X, \leqslant \rangle$ un insieme parzialmente ordinato. Diremo che:

- $a \in X$ è elemento **massimale** se $a \leqslant b$ per qualche $b \in X$ implica $a = b$.
- $a \in X$ è elemento **minimale** se $b \leqslant a$ per qualche $b \in X$ implica $a = b$.
- $a \in X$ è **massimo** se $x \leqslant a$ per ogni $x \in X$.
- $a \in X$ è **minimo** se $a \leqslant x$ per ogni $x \in X$.

Osservazione 3.9. Massimo e minimo, quando esistono, sono unici e verranno indicati rispettivamente con 1 e 0, oppure $\top$ e $\bot$. In generale, il massimo e il minimo non esistono sempre, ad esempio $\langle \mathbb{N}, \leqslant \rangle$ non ha massimo.

Esempio 3.10. Nell'insieme X dell'Esempio 3.7 il massimo è e mentre il minimo è a. Nell'insieme Y abbiamo due elementi massimali (x e y) e due elementi minimali (w e z), ma nessun massimo o minimo.

Definizione 3.11

Sia $\langle X, \leqslant \rangle$ un insieme parzialmente ordinato e sia $A \subseteq X$. Diremo che:

- $x \in X$ è un **maggiorante** per A se $a \leqslant x$ per ogni $a \in A$;
- $x \in X$ è un **minorante** per A se $x \leqslant a$ per ogni $a \in A$;
- $x \in X$ è **supremo** per A, e scriveremo $x = \sup(A)$, se è il minimo maggiorante. In altre parole, se $a \leqslant x$ per ogni $a \in A$ e per ogni altro $y \in X$ tale che $a \leqslant y$, si ha $x \leqslant y$;
- $x \in X$ è **infimo** per A, e scriveremo $x = \inf(A)$, se è il massimo minorante. In altre parole, se $x \leqslant a$ per ogni $a \in A$ e per ogni altro $y \in X$ tale che $y \leqslant a$, si ha $y \leqslant x$.

Osservazione 3.12. Si dimostra facilmente, usando la anti-simmetria dell'ordine, che infimo e supremo sono unici (quando esistono).

Esempio 3.13. Nell'insieme X dell'Esempio 3.7 si ha che $\sup(\{b, c, d\}) = e$ e inoltre $\inf(\{b, c, d\}) = a$. Per Y si ha $\inf(\{x, y\}) = z$ e $\sup(\{y, z, w\}) = y$. Infine, non esiste $\inf(\{y, t\})$ in Z.

Definizione 3.14

Diremo che $\langle X, \leqslant \rangle$ è **limitato** se esistono il suo massimo e il suo minimo.

Definizione 3.15

Un insieme $\langle X, \leqslant \rangle$ parzialmente ordinato si dice **reticolare** se per ogni $x, y \in X$

esistono $\inf(x, y)$ e $\sup(x, y)$.

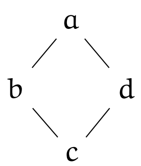
Esercizio 3.16. Dimostrare che ogni ordine totale è un ordine reticolare.

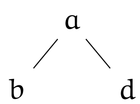
Lemma 3.17. *Se $\langle X, \leqslant \rangle$ è un ordine reticolare e a è un elemento massimale (minimale), allora a è il massimo (minimo).*

Dimostrazione. Sia a massimale. Per ogni $x \in X$ consideriamo il $\sup\{x, a\}$, che esiste poiché X è un reticolo. Si ha che $a \leqslant \sup\{x, a\}$, e quindi, per la massimalità di a, $\sup\{a, x\} = a$ il che implica che $x \leqslant a$ per ogni $x \in X$. □

Si noti che se un ordine reticolare $\langle X, \leqslant \rangle$ è *finito*, allora esistono il massimo e il minimo di X.

Esempio 3.18. È facile verificare che l'insieme parzialmente ordinato qui sotto a sinistra è un ordine reticolare, mentre quello a destra non lo è.





Per quanto detto, per ogni coppia di elementi di un insieme reticolarmente ordinato esistono sempre infimo e supremo. Di conseguenza, ha senso considerarli delle *operazioni binarie*. Vediamo alcune proprietà basilari di infimo e supremo.

Proposizione 3.19. *Sia $\langle X, \leqslant \rangle$ un insieme reticolarmente ordinato. Per ogni $x, y, z \in X$ si ha:*

1. ***Commutatività**: $\inf\{x, y\} = \inf\{y, x\}$, $\sup\{x, y\} = \sup\{y, x\}$.*
2. ***Idempotenza**: $\inf\{x, x\} = x$, $\sup\{x, x\} = x$.*
3. ***Associatività**: $\inf\{x, \inf\{y, z\}\} = \inf\{\inf\{x, y\}, z\}$, $\sup\{x, \sup\{y, z\}\} = \sup\{(\sup\{x, y\}), z\}$.*
4. ***Assorbimento**: $\inf\{x, \sup\{x, y\}\} = x$, $\sup\{x, \inf\{x, y\}\} = x$.*
5. *$\inf\{x, y\} = x$ se, e solo se, $x \leqslant y$ se, e solo se, $\sup\{x, y\} = y$.*
6. ***Monotonia**: se $x \leqslant y$, allora $\inf\{x, z\} \leqslant \inf\{y, z\}$ e $\sup\{x, z\} \leqslant \sup\{y, z\}$.*

Dimostrazione. (1) e (2). Seguono banalmente dalla definizione, infatti è chiaro che $\sup(x, y) = \sup(y, x)$ e $x = \sup(x, x)$; lo stesso vale per l'infimo.

(3). Dimostriamo che $\inf\{x, \inf\{y, z\}\} = \inf\{x, y, z\} = \inf\{\inf\{x, y\}, z\}$. Vediamo la prima uguaglianza. Applicando la definizione di inf si ha

$$\inf\{x, \inf\{y, z\}\} \leqslant x, \tag{3}$$
$$\inf\{x, \inf\{y, z\}\} \leqslant \inf\{y, z\}, \tag{4}$$
$$\inf\{y, z\} \leqslant y \text{ e} \tag{5}$$
$$\inf\{y, z\} \leqslant z. \tag{6}$$

Dalle Equazioni da (3) a (6) e la transitività di $\leqslant$ segue che $\inf\{x, \inf\{y,z\}\} \leqslant x, y, z$, quindi $\inf\{x, \inf\{y,z\}\}$ è un minorante per $\{x,y,z\}$. Sia s un altro minorante e quindi $s \leqslant x, y, z$. Ne segue che $s \leqslant \inf\{y,z\}$. Poiché vale anche $s \leqslant x$ deduciamo $s \leqslant \inf\{x, \inf\{y,z\}\}$. Concludiamo quindi che $\inf\{x, \inf\{y,z\}\} = \inf(\{x,y,z\})$. Analogamente si dimostra che $\inf\{x,y,z\} = \inf\{\inf\{x,y\}, z\}$ e da ciò segue la associatività di inf. La dimostrazione nel caso di sup è analoga.

(4). Poiché $x \leqslant x$ e $x \leqslant \sup\{x,y\}$ si ha $x \leqslant \inf\{x, \sup\{x,y\}\}$. Dall'altro lato si ha $\inf\{x, \sup\{x,y\}\} \leqslant x$ in quanto infimo di x e $\sup\{x,y\}$. Quindi, $x = \inf\{x, \sup\{x,y\}\}$. L'altra legge di assorbimento è analoga.

(5). Vediamo che $x \leqslant y$ se, e solo se, $\inf\{x,y\} = x$. Sia $x \leqslant y$, si ha che $x \leqslant x$ e $x \leqslant y$, quindi $x \leqslant \inf(x,y)$. Inoltre, $\inf(x,y) \leqslant x$ perché infimo di x e y. Quindi $x = \inf(x,y)$. Viceversa, se $\inf\{x,y\} = x$, banalmente $x \leqslant y$ poiché è l'infimo di $\{x,y\}$. L'altra doppia implicazione è analoga.

(6). Sia $x \leqslant y$. Per il Punto 5 si ha $x = \inf\{x,y\}$ e $y = \sup\{x,y\}$. Consideriamo quindi $\inf\{\inf\{x,z\}, \inf\{y,z\}\}$. Per le proprietà precedenti di associatività, commutatività e idempotenza, $\inf\{\inf\{x,z\}, \inf\{y,z\}\} = \inf\{\inf\{z,z\}, \inf\{x,y\}\} = \inf\{z,x\}$, quindi $\inf\{x,z\} \leqslant \inf\{y,z\}$. La dimostrazione per sup è analoga. □

Osservazione 3.20. La dimostrazione della Punto 6 si generalizza al caso in cui abbiamo n relazioni: se $x_1 \leqslant y_1, \ldots, x_n \leqslant y_n$ allora $x_1 \wedge \cdots \wedge x_n \leqslant y_1 \wedge \cdots \wedge y_n$ e $x_1 \vee \cdots \vee x_n \leqslant y_1 \vee \cdots \vee y_n$.

Anticipiamo ora un caso particolare del concetto di *struttura* che vedremo nell'ambito della logica del prim'ordine. Un'**algebra** è una struttura matematica data da un insieme con delle operazioni definite su di esso. A ogni (simbolo di) operazione è associato un numero naturale, detto **arietà**, che specifica il numero di argomenti di quell'operazione. L'insieme delle operazioni con le loro rispettive arietà è detto **segnatura**.

Esempio 3.21.
1. La segnatura dei semigruppi è $\langle +^2 \rangle$.
2. La segnatura dei gruppi è $\langle +^2, -^1, 0 \rangle$.
3. La segnatura degli anelli è $\langle +^2, \cdot^2, -^1, 0, 1 \rangle$.

Quando le arietà delle operazioni sono chiare dal contesto è consueto ometterle. La motivazione per introdurre i reticoli come strutture algebriche risiede nel seguente teorema.

Definizione 3.22

Un **reticolo** è un'algebra $(X, \wedge^2, \vee^2)$ in cui $X \neq \emptyset$ ed entrambe le operazioni sono associative, commutative e verificano le due proprietà di assorbimento $(x \wedge (x \vee y) = x$, $x \vee (x \wedge y) = x)$.

Lemma 3.23. *Se* $(X, \wedge^2, \vee^2)$ *è un reticolo allora le operazioni* $\wedge$ *e* $\vee$ *sono idempotenti.*

Dimostrazione. Per le leggi di assorbimento possiamo scrivere $x = x \vee (x \wedge x)$ e $x = x \wedge (x \vee (x \wedge x))$. Quindi, sostituendo la prima uguaglianza nella seconda, $x = x \wedge x$. Analogamente, $x = x \wedge (x \vee x)$ e $x = x \vee (x \wedge (x \vee x))$ e di conseguenza $x = x \vee x$. □

Lemma 3.24. *Ogni reticolo* $(X, \wedge, \vee)$ *risulta reticolarmente ordinato dalla seguente relazione:*

$$x \leqslant y \Leftrightarrow x \wedge y = x \Leftrightarrow x \vee y = y. \tag{7}$$

Inoltre l'infimo e il supremo rispetto a questo ordine sono rispettivamente $\wedge$ *e* $\vee$.

Dimostrazione. Verifichiamo inizialmente che $x \wedge y = x$ se, e solo se, $x \vee y = y$, ciò semplificherà la dimostrazione più avanti. Infatti, se $x = x \wedge y$, si ha che $x \vee y = (x \wedge y) \vee y = y$ per l'assorbimento. Dall'altro lato, se $y = x \vee y$, si ha $x \wedge y = x \wedge (x \vee y) = x$, ancora per la legge di assorbimento.

Dimostriamo ora che la relazione definita in Equazione (7) è un ordine reticolare. Vediamo prima di tutto che è un ordine parziale. Si vede facilmente che la riflessività di $\leqslant$ segue dall'idempotenza di $\wedge$, la anti-simmetria di $\leqslant$ segue dalla commutatività di $\wedge$, mentre la transitività di $\leqslant$ segue dall'associatività di $\wedge$.

Proviamo ora che infimo e supremo esistono per ogni coppia di elementi e sono proprio dati dalle due operazioni. In simboli, vediamo che $\sup(x, y) = x \vee y$ e $\inf(x, y) = x \wedge y$. Verifichiamo che $x \wedge y$ è un minorante per $\{x, y\}$. Infatti, $(x \wedge y) \wedge x = (y \wedge x) \wedge x = y \wedge (x \wedge x) = y \wedge x = x \wedge y$, che implica $x \wedge y \leqslant x$. Analogamente $(x \wedge y) \wedge y = x \wedge y$ e $x \wedge y \leqslant y$. Sia ora w un minorante arbitrario per $\{x, y\}$. Di conseguenza si ha $w \leqslant x$ e $w \leqslant y$, che per definizione dell'ordine diventano $w \wedge y = w$ e $w \wedge x = w$. Allora, $w \wedge (x \wedge y) = (w \wedge x) \wedge y = w \wedge y = w$, che implica $w \leqslant x \wedge y$. Quindi $x \wedge y$ è il massimo minorante (cioè l'infimo) per $\{x, y\}$.

La dimostrazione che $x \vee y = \sup(x, y)$ è analoga, usando il fatto che $x \vee y = y$ se, e solo se, $x \wedge y = x$. □

Definizione 3.25

Un reticolo $\langle X, \wedge, \vee \rangle$ si dice **distributivo** se $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ per ogni $x, y, z \in X$.

Lemma 3.26. *In ogni reticolo* X*, per ogni* $x, y, z \in X$ *le seguenti sono equivalenti*

1. $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$,
2. $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$.

Dimostrazione. Punto 1 implica Punto 2:

$$
\begin{aligned}
(x \vee y) \wedge (x \vee z) &= ((x \vee y) \wedge x) \vee ((x \vee y) \wedge z) = && \text{per il Punto 1,}\\
&= x \vee ((x \vee y) \wedge z) = && \text{per l'assorbimento,}\\
&= x \vee ((x \wedge z) \vee (y \wedge z)) = && \text{per il Punto 1,}\\
&= (x \vee (x \wedge z)) \vee (y \wedge z) = && \text{per l'associatività,}\\
&= x \vee (y \wedge z) = && \text{per l'assorbimento.}
\end{aligned}
$$

Punto 2 implica Punto 1:

$$
\begin{aligned}
(x \wedge y) \vee (x \wedge z) &= ((x \wedge y) \vee x) \wedge ((x \wedge y) \vee z) = && \text{per il Punto 2,}\\
&= x \wedge ((x \wedge y) \vee z) = && \text{per l'assorbimento,}\\
&= x \wedge ((x \vee z) \wedge (y \vee z)) = && \text{per il Punto 2,}\\
&= (x \wedge (x \vee z)) \wedge (y \vee z) = && \text{per l'associatività,}\\
&= x \wedge (y \vee z) && \text{per l'assoribimento.}
\end{aligned}
$$

□

Nei reticoli distributivi vale una sorta di *cancellatività*:

Lemma 3.27. *Sia* $(X, \wedge, \vee)$ *un reticolo distributivo e* $x, y, z \in X$. *Se* $x \wedge y = x \wedge z$ *e* $x \vee y = x \vee z$, *allora* $y = z$.

Dimostrazione. Si ha

$$
\begin{aligned}
y &= y \wedge (y \vee x) = && \text{per l'assorbimento,}\\
&= y \wedge (x \vee z) = && \text{per ipotesi,}\\
&= (y \wedge x) \vee (y \wedge z) = && \text{per la distributività,}\\
&= (z \wedge x) \vee (y \wedge z) = && \text{per ipotesi,}\\
&= z \wedge (x \vee y) = && \text{per la distributività,}\\
&= z \wedge (x \vee z) = && \text{per ipotesi,}\\
&= z && \text{per l'assorbimento.}
\end{aligned}
$$

□

Definizione 3.28

Un reticolo limitato $\langle X, \wedge, \vee \rangle$ si dice **complementato** se per ogni $x \in X$ esiste $y \in X$ tale che $x \vee y = 1$ e $x \wedge y = 0$, dove 0 e 1 sono il minimo e il massimo del reticolo. L'elemento y è detto **complemento** di x.

Lemma 3.29. *Sia* $\langle X, \wedge, \vee \rangle$ *un reticolo limitato, complementato e distributivo. Allora il complemento di ogni elemento è unico.*

Dimostrazione. Sia $x \in X$ e supponiamo che y, z siano due complementi di x, cioè $x \wedge y = 0 = x \wedge z$ e $x \vee y = 1 = x \vee z$ allora per il Lemma 3.27, si ha $y = z$. □

3.2 ALGEBRE DI BOOLE

Definizione 3.30

Un'**algebra di Boole** è un reticolo complementato, limitato e distributivo. Alternativamente, possiamo definire un'algebra di Boole come una struttura del tipo $\langle A, \wedge^2, \vee^2, \neg^1, 0, 1\rangle$, che soddisfi i seguenti assiomi:

$$(x \vee y) \vee z = x \vee (y \vee z) \quad \text{e} \quad (x \wedge y) \wedge z = x \wedge (y \wedge z), \tag{BA1}$$

$$x \vee y = y \vee x \quad \text{e} \quad x \wedge y = y \wedge x, \tag{BA2}$$

$$(x \wedge y) \vee y = y \quad \text{e} \quad (x \vee y) \wedge y = y, \tag{BA3}$$

$$(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z) \quad \text{e} \quad (x \wedge y) \vee z = (x \vee z) \wedge (y \vee z), \tag{BA4}$$

$$x \wedge \neg x = 0 \quad \text{e} \quad x \vee \neg x = 1 \tag{BA5}$$

Si noti, che sebbene nessuna delle equazioni qui sopra dica esplicitamente che 0 e 1 sono rispettivamente il minimo e il massimo dell'algebra, come vedremo nella Proposizione 3.33, ciò è una conseguenza di questi assiomi.

Osserviamo che dalle Equazioni da (BA1) a (BA3) e Lemma 3.23 segue l'idempotenza di $\vee$ e $\wedge$.

Esempio 3.31. Forniamo qui sotto alcuni esempi di algebre di Boole. Il primo e il secondo si riveleranno importantissimi.

1. Se S è un insieme, allora $\langle \wp(S), \cap, \cup, ^c, \emptyset, S\rangle$ è un algebra di Boole, dove $A^c = S \setminus A$, per ogni $A \in \wp(S)$.
2. L'algebra $\langle \{0, 1\}, \min, \max, 1 - x, 0, 1\rangle$ è un algebra di Boole. Useremo il simbolo $\mathbb{2}$ per indicare quest'algebra.
3. Grazie alla simmetria degli assiomi di algebra di Boole, è facile vedere che scambiando le operazioni $\wedge$ e $\vee$ in un'algebra di Boole si ottiene un'altra algebra di Boole. In altre parole se $\langle A, \wedge, \vee, \neg, 0, 1\rangle$ è un'algebra di Boole, allora anche $\langle A, \vee, \wedge, \neg, 1, 0\rangle$ lo è.
4. Sia $m > 1$ un intero e sia A l'insieme dei divisori di m (incluso 1). Definiamo per ogni $a, b \in A$

$$a \wedge b := \mathsf{MCD}\{a, b\}$$
$$a \vee b := \mathsf{mcm}\{a, b\}$$
$$\neg a := m/a.$$

Se m non è divisibile per il quadrato di nessun numero diverso da 1, allora A è un'algebra di Boole. Infatti in questo caso c'è una corrispondenza biunivoca tra divisori di m e i sottoinsiemi dei numeri primi che dividono m. Sotto questa corrispondenza, l'operazione $\wedge$ diventa l'intersezione, il $\vee$ diventa l'unione, il $\neg$ diventa il complemento insiemistico e $\emptyset$ e $\{p \mid p \text{ primo}, p \text{divide } m\}$ diventano il minimo e il massimo dell'algebra. In altre parole è possibile rappresentare l'algebra A come un'algebra di sottoinsiemi. Nella Sezione 3.3.2 il Teorema di rappresentazione di Stone rivelerà che in effetti ciò è possibile per *qualunque* algebra di Boole.

5. Il reticolo $X = \{a, b, c, d\}$ dato da

$$\begin{tikzcd}[column sep=small] & a \arrow[dl, dash] \arrow[dr, dash] & \\ b \arrow[dr, dash] & & d \arrow[dl, dash] \\ & c & \end{tikzcd}$$

è un'algebra di Boole dove $1 = a$, $0 = c$, $\neg b = d$ e $\neg d = b$.

Osservazione 3.32. Segue dal Lemma 3.24 che ogni algebra di Boole ha un ordine parziale naturale, definito da

$a \leqslant b$ se, e soltanto se, $a \vee b = b$ o, equivalentemente se, e soltanto se, $a \wedge b = a$.

Vediamo alcune proprietà basilari che valgono in ogni algebra di Boole.

Proposizione 3.33. *Sia $\langle A, \wedge, \vee, \neg, 0, 1\rangle$ un'algebra di Boole. Per ogni $x, y \in A$ si ha:*

1. $0 \leqslant x \leqslant 1$;
2. $0 = \neg 1$, $1 = \neg 0$;
3. $\neg(\neg x) = x$ *(legge della **doppia negazione**)*;
4. $x = y$ *se, e solo se,* $\neg x = \neg y$
5. $\neg(x \vee y) = \neg x \wedge \neg y$, $\neg(x \wedge y) = \neg x \vee \neg y$ *(leggi di **De Morgan**)*;
6. $x \leqslant y$ *se, e solo se,* $\neg y \leqslant \neg x$;

Dimostrazione. (1). Per mostrare che per ogni $x \in A$, $0 \leqslant x$ calcoliamo:

$$\begin{aligned} 0 \wedge x &= (x \wedge \neg x) \wedge x && \text{per Equazione (BA5)}, \\ &= (\neg x \wedge x) \wedge x && \text{per Equazione (BA2)}, \\ &= \neg x \wedge (x \wedge x) && \text{per Equazione (BA1)}, \\ &= \neg x \wedge x && \text{per il Lemma 3.23}, \\ &= 0 && \text{per Equazione (BA5)}. \end{aligned}$$

Il fatto che $x \leqslant 1$ si dimostra similmente.

(2). Poiché 0 è il minimo dell'algebra, $0 \wedge 1 = 0$ e poiché 1 è il massimo $0 \vee 1 = 1$. L'asserzione segue dunque immediatamente dall'unicità del complemento.

(3). Per definizione di complemento e commutatività delle operazioni è facile verificare che $\neg x \vee x = 1 = \neg x \vee \neg(\neg x)$ e $\neg x \wedge x = 0 = \neg x \wedge \neg(\neg x)$. Per l'unicità del complemento, Lemma 3.29, si ha $x = \neg(\neg x)$.

(4). Segue immediatamente dall'unicità del complemento e dal Punto 3.

(5). Verifichiamo che $(x \vee y) \wedge (\neg x \wedge \neg y) = 0$ e $(x \vee y) \vee (\neg x \wedge \neg y) = 1$. Si ha

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

La dimostrazione dell'altra legge è analoga.

(6). Si ha $x \leqslant y$ se, e solo se, $x \vee y = y$ se, e solo se, $\neg(x \vee y) = \neg y$ se, e solo se, $\neg x \wedge \neg y = \neg y$ se, e solo se, $\neg y \leqslant \neg x$. □

La caratterizzazione dell'ordine seguente è di fondamentale importanza e verrà sistematicamente usata nel resto del capitolo.

Lemma 3.34. *Sia $\langle A, \wedge, \vee, \neg, 0, 1 \rangle$ un'algebra di Boole. Per ogni $x, y \in A$ si ha:*

$$x \leqslant y \text{ se, e solo se, } x \wedge \neg y = 0 \text{ se, e solo se, } \neg x \vee y = 1.$$

Dimostrazione. Se $x \leqslant y$, allora $y = x \vee y$. Quindi $0 = y \wedge \neg y = (x \vee y) \wedge \neg y = (x \wedge \neg y) \vee (y \wedge \neg y) = (x \wedge \neg y) \vee 0 = x \wedge \neg y$. Viceversa, se $x \wedge \neg y = 0$, $y = y \vee 0 = y \vee (x \wedge \neg y) = (y \vee x) \wedge (y \vee \neg y) = (y \vee x) \wedge 1 = y \vee x$. La seconda equivalenza nell'enunciato segue dalla prima e dal Punto 4 della Proposizione 3.33. □

3.2.1 *Omomorfismi e quozienti*

La maggior parte delle informazioni riguardanti un'algebra di Boole possono essere ottenute studiando le "deformazioni" dell'algebra. Ovviamente la nozione di deformazione a cui siamo interessati è quella che preserva la struttura di algebra di Boole, cioè le sue operazioni.

Definizione 3.35

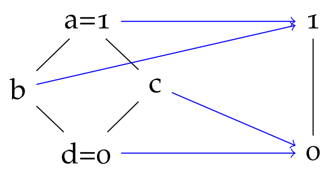
Siano A e B due algebre di Boole. Un **omomorfismo** di algebre di Boole è una funzione $f\colon A \to B$ tale che $\forall a, b \in A$:

$$\begin{aligned} f(a \wedge b) &= f(a) \wedge f(b) \\ f(a \vee b) &= f(a) \vee f(b) \\ f(\neg a) &= \neg f(a). \end{aligned}$$

Osservazione 3.36. Le tre condizioni date nella definizione di omomorfismo implicano che $f(1) = 1$ e $f(0) = 0$. Infatti si ha $f(1) = f(a \vee \neg a) = f(a) \vee \neg f(a) = 1$ e analogamente per 0.

Un omomorfismo iniettivo è detto **monomorfismo**, un omomorfismo suriettivo è detto **epimorfismo** e un omomorfismo biettivo è detto **isomorfismo**.

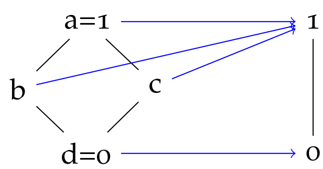
Esempio 3.37. La funzione descritta dal seguente diagramma



è un epimorfismo, verifichiamo ad esempio le seguenti condizioni:

$$b \wedge c = 0 \qquad \text{e} \qquad f(b \wedge c) = 0 = 1 \wedge 0 = f(b) \wedge f(c).$$

Mentre,



non è un omomorfismo, perché

$$b \wedge c = 0 \qquad \text{ma} \qquad f(b) \wedge f(c) = 1 \wedge 1 = 1$$

Esempio 3.38. Sia S un insieme non vuoto e $\langle \wp(S), \cap, \cup, {}^c, \emptyset, S \rangle$ l'algebra di Boole associata. Fissato $s \in S$, definiamo per ogni $X \in \wp(S)$

$$\chi_s(X) := \begin{cases} 1 & \text{se } s \in X \\ 0 & \text{se } s \notin X. \end{cases}$$

Allora χ_s è un omomorfismo da $\wp(S)$ in $\mathbb{2}$. Verifichiamo come esempio che χ_s rispetta il $\wedge$. Siano X, Y sottoinsiemi di S, allora per definizione

$$\chi_s(X \cap Y) = \begin{cases} 1 & \text{se } s \in X \cap Y \\ 0 & \text{se } s \notin X \cap Y. \end{cases}$$

D'altro canto,

$$\chi_s(X) \wedge \chi_s(Y) = \min\{\chi_s(X), \chi_s(Y)\} = 1 \text{ se, e soltanto se, } s \in X \text{ e } s \in Y.$$

Dunque si ha $\chi_s(X \cap Y) = \chi_s(X) \wedge \chi_s(Y)$.

La seguente proposizione mostra che un omomorfismo, oltre alle operazioni, preserva anche l'ordine.

Proposizione 3.39. *Siano* A *e* B *due algebre di Boole e* $f \colon A \to B$ *un omomorfismo tra esse. Per ogni* $x, y \in A$, *se* $x \leqslant y$ *allora* $f(x) \leqslant f(y)$.

Dimostrazione. Poiché $x \leqslant y$ se, e solo se, $x \wedge y = x$, abbiamo che $f(x) = f(x \wedge y) = f(x) \wedge f(y)$ e quindi $f(x) \leqslant f(y)$. □

Sebbene le funzioni siano oggetti fondamentali in matematica, a volte è più semplice ragionare su un sottoinsieme di A^2 piuttosto che su una funzione $f \colon A \to B$. Sorprendentemente, se la funzione oggetto di studio è un epimorfismo ciò è possibile. Vedremo adesso che a ogni epimorfismo $f \colon A \to B$ è associabile un sottoinsieme di A^2 che permette di ricostruire interamente f. I sottoinsiemi di A^2 che corrispondono in questo senso a epimorfismi sono detti *congruenze*.

Definizione 3.40

Se $\mathcal{B} = \langle B, \wedge, \vee, \neg, 0, 1 \rangle$ è un'algebra di Boole, una **congruenza** su $\mathcal{B}$ è una relazione di equivalenza $\sim$ (riflessiva, simmetrica e transitiva) tale che, per ogni $x_1, x_2, y_1, y_2 \in B$, se $x_1 \sim x_2$ e $y_1 \sim y_2$ allora

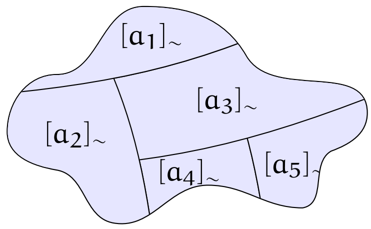
1. $x_1 \wedge y_1 \sim x_2 \wedge y_2$,
2. $x_1 \vee y_1 \sim x_2 \vee y_2$,
3. $\neg x_1 \sim \neg x_2$.

Definizione 3.41

Data un'algebra di Boole A, una congruenza $\sim$ su A induce una **struttura quoziente**, sull'insieme delle classi di equivalenza in $A/\sim$ definita come segue:

- $1 := [1]_\sim$,
- $0 := [0]_\sim$,

- $[a]_\sim \wedge [b]_\sim := [a \wedge b]_\sim$,
- $[a]_\sim \vee [b]_\sim := [a \vee b]_\sim$,
- $\neg[a]_\sim := [\neg a]_\sim$.



Esercizio 3.42. Dimostrare che le operazioni definite qui sopra sono ben poste e che se $\mathcal{A}$ è un'algebra di Boole, allora anche $A/\sim$ con le operazioni definite qui sopra lo è.

Esempio 3.43. L'insieme $\mathtt{Form}$ della Definizione 2.2 può essere dotato naturalmente di operazioni simili a quelle delle algebre di Boole:

- $\varphi \wedge^{\mathtt{Form}} \psi := \varphi \wedge \psi$,
- $\varphi \vee^{\mathtt{Form}} \psi := \varphi \vee \psi$,
- $\neg^{\mathtt{Form}} \varphi := \neg\varphi$.

L'algebra $\langle \mathtt{Form}, \wedge^{\mathtt{Form}}, \vee^{\mathtt{Form}}, \neg^{\mathtt{Form}}, \bot, \top \rangle$ è detta l'algebra **assolutamente libera** per il linguaggio $\langle \wedge^2, \vee^2, \neg^1, 0, 1 \rangle$. L'algebra $\langle \mathtt{Form}, \wedge^{\mathtt{Form}}, \vee^{\mathtt{Form}}, \neg^{\mathtt{Form}}, \bot, \top \rangle$ *non è* però un'algebra di Boole. Per esempio l'equazione $\varphi \wedge^{\mathtt{Form}} \psi = \psi \wedge^{\mathtt{Form}} \varphi$ non è valida in $\mathtt{Form}$, perché le formule $\varphi \wedge^{\mathtt{Form}} \psi$ e $\psi \wedge^{\mathtt{Form}} \varphi$ sono sintatticamente diverse!

Per ottenere un'algebra di Boole a partire da $\langle \mathtt{Form}, \wedge^{\mathtt{Form}}, \vee^{\mathtt{Form}}, \neg^{\mathtt{Form}}, \bot, \top \rangle$ è necessario considerare il quoziente rispetto alla relazione $\equiv$ che sussiste tra due formule se, e soltanto se, esse sono logicamente equivalenti. Questo porterà al concetto di algebra di Lindenbaum-Tarski, vedi Teorema 3.98 e definizioni precedenti.

Dunque, se A è una qualsiasi algebra di Boole, ogni congruenza $\sim$ su A induce un epimorfismo da A in $A/\sim$, detto **epimorfismo canonico** e dato da

$$\pi_\sim(a) := [a]_\sim.$$

Esercizio 3.44. Dimostrare che la funzione $\pi_\sim$ è un epimorfismo di algebre di Boole.

Viceversa, ogni epimorfismo induce una congruenza, come segue.

Definizione 3.45

Sia $f\colon A \to B$ un epimorfismo di algebre di Boole. Definiamo la seguente relazione su A
$$a \equiv_f b \text{ se, soltanto se, } f(a) = f(b).$$

Proposizione 3.46. *La relazione definita in Definizione 3.45 è una congruenza.*

Dimostrazione. Cominciamo con il verificare che $\equiv_f$ è una relazione di equivalenza. La riflessività e la simmetria sono immediate. Per verificare la transitività siano $a, b, c \in A$ tali che $f(a) = f(b)$ e $f(b) = f(c)$, allora segue immediatamente che $f(a) = f(c)$ e quindi $a \equiv_f c$. Mostriamo ora che $\equiv_f$ è compatibile con le operazioni booleane, vediamo solo il caso di $\wedge$ poiché gli altri sono molto simili. Siano $a_1, b_1, a_2, b_2 \in A$ tali che $a_1 \equiv_f a_2$ e $b_1 \equiv_f b_2$. Quindi si ha $f(a_1) = f(a_2)$ e $f(b_1) = f(b_2)$. Poiché f è un omomorfismo si ha $f(a_1 \wedge b_1) = f(a_1) \wedge f(b_1)$ e per quanto detto prima $f(a_1) \wedge f(b_1) = f(a_2) \wedge f(b_2) = f(a_2 \wedge b_2)$, dunque $(a_1 \wedge b_1) \equiv_f a_2 \wedge b_2$. □

Inoltre, le corrispondenze $f \mapsto \equiv_f$ e $\sim \mapsto \pi_\sim$ sono l'una l'inversa dell'altra. In altre parole si hanno i seguenti due risultati.

Lemma 3.47. *Sia $\sim$ una congruenza su A. Per ogni $a, b \in A$ si ha $a \sim b$ se, e soltanto se, $a \equiv_{\pi_\sim} b$.*

Dimostrazione. Si ha che $a \sim b$ se, e soltanto se, $[a]_\sim = [b]_\sim$, per definizione ciò è equivalente a $\pi_\sim(a) = \pi_\sim(b)$. Infine, ancora per definizione, quest'ultima condizione è equivalente a $a \equiv_{\pi_\sim} b$. □

Lemma 3.48. *Sia $f\colon A \to B$ un epimorfismo. La funzione $\iota\colon A/\equiv_f \to B$ definita da $\iota([a]_{\equiv_f}) := f(a)$ è un isomorfismo e per ogni $a \in A$ si ha $f(a) = \iota(\pi_{\equiv_f}(a))$ (cioè $\pi_{\equiv_f}$ e f sono uguali a meno di un isomorfismo).*

Dimostrazione. Innanzitutto verifichiamo che ι è un isomorfismo. La funzione ι è ben definita: se $a \equiv_f b$, per la definizione di $\equiv_f$ si ha $f(a) = f(b)$ quindi $\iota([a]_{\equiv_f}) = \iota([b]_{\equiv_f})$. Viceversa, se $\iota([a]_{\equiv_f}) = \iota([b]_{\equiv_f})$, allora $f(a) = f(b)$ quindi $[a]_{\equiv_f} = [b]_{\equiv_f}$ e dunque la funzione è iniettiva. La suriettività di ι è un'immediata conseguenza della suriettività di f. Infine, ι è un omomorfismo perché f lo è. Verifichiamo a titolo di esempio che ι commuta con $\wedge$. Siano $a, b \in A$, calcoliamo

$$\begin{aligned}
\iota([a]_{\equiv_f} \wedge [b]_{\equiv_f}) &= \iota([a \wedge b]_{\equiv_f}) && \text{applicando la Definizione 3.41} \\
&= f(a \wedge b) && \text{per definizione di } \iota \\
&= f(a) \wedge f(b) && \text{perché } f \text{ è un omomorfismo} \\
&= \iota([a]_{\equiv_f}) \wedge \iota([b]_{\equiv_f}) && \text{per definizione di } \iota.
\end{aligned}$$

Concludiamo la dimostrazione verificando che $\iota(\pi_{\equiv_f}(a)) = \iota([a]_{\equiv_f}) = f(a)$. □

Un'ispezione della dimostrazione appena conclusa mostra che la condizione di suriettività su f può essere in qualche modo evitata:

Corollario 3.49 (Primo Teorema di isomorfismo). *Siano A e B due algebre di Boole e sia $f\colon A \to B$ è un qualsiasi omomorfismo di algebre di Boole, allora f si fattorizza in un omomorfismo suriettivo $\pi_{\equiv_f}\colon A \to A/\equiv_f$ e un unico omomorfismo iniettivo $\iota\colon A/\equiv_f \to B$ tale che $f = \iota \circ \pi_{\equiv}$.*

$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr, "\pi_{\equiv_f}"'] & & B \\ & A/\equiv_f \arrow[ur, "\iota"'] & \end{tikzcd}$$

Abbiamo quindi stabilito che epimorfismi e congruenze sono in biezione e dunque lo studio dei primi si può riportare a quello delle seconde.

3.2.2 *Sottalgebre*

Il Lemma 3.48 visto in precedenza ci permette di studiare omomorfismi tramite le congruenze (o i filtri, in virtù del Lemma 3.66), a patto però che questi siano suriettivi. Nel caso di un omomorfismo generale $f\colon A \to B$ invece, il quoziente è solo *contenuto* nell'algebra codominio. In quest'ultimo caso si può notare che l'immagine $f[A]$ è chiusa rispetto alle operazioni di B. Infatti se $a, b \in A$ $f(a) \wedge^B f(b) = f(a \wedge b) \in f[A]$, poiché $a \wedge b \in A$.

Definizione 3.50

Sia A un'algebra di Boole. Un sottoinsieme non vuoto $S \subseteq A$ chiuso rispetto alle operazioni di algebra di Boole è detto **sottalgebra**. In altre parole S è tale che $\forall s, t \in S$

$$s \wedge t, s \vee t, \neg s, 0, 1 \in S$$

Alla luce di questa definizione il Corollario 3.49 permette di ridurre, a meno di un isomorfismo, lo studio di omomorfismi qualsiasi a quello di *epimorfismi* e *sottalgebre*.

Esempio 3.51. Sia S un insieme e $A = \langle \wp(S), \cap, \cup, {}^c, \emptyset, S \rangle$ l'algebra di Boole dei suoi sottoinsiemi. L'insieme B di tutti i sottoinsiemi di S *finiti o cofiniti* (=insieme il cui complemento è finito) forma una sottalgebra di A. Infatti:

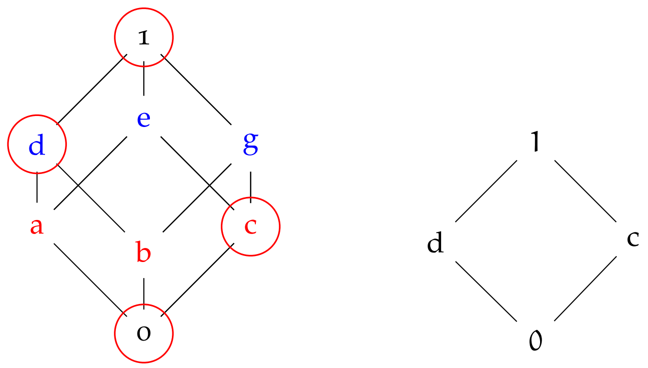
- complemento di finito = cofinito,
- finito $\cup$ finito = finito,
- finito $\cup$ cofinito = cofinito,
- finito $\cap$ finito = finito,
- finito $\cap$ cofinito = finito,

Le sottalgebre sono evidentemente chiuse per intersezione. Ciò ci permette di definire la più piccola sottalgebra contenente un dato insieme.

Definizione 3.52

Dato un sottoinsieme S di un'algebra di Boole B, definiamo la **sottalgebra generata** da S come l'intersezione di tutte le sottalgebre di B contenenti S. Indicheremo la sottalgebra generata da S con $\langle S \rangle$. Essa è dunque la più piccola sottalgebra di B che contiene S Diremo che un sottoinsieme S **genera** B se $\langle S \rangle = B$.

Esempio 3.53. Vediamo un esempio di sottalgebra generata. Consideriamo l'algebra B rappresentata a sinistra e vediamo qual è la sottalgebra generata da c. Si nota facilmente che l'unica sottalgebra diversa da B e che contiene c è quella data da $\{0, c, d, 1\}$, in quanto contiene esattamente $d = \neg c$, massimo e minimo di B.



3.3 KERNEL E FILTRI

Ciò che ci apprestiamo a dimostrare adesso permette un'ulteriore semplificazione: infatti vedremo ora che la congruenza $\equiv_f$ può essere completamente ricostruita a partire dalla sola classe di equivalenza dell'elemento 1, e cioè: $[1]_f = \{a \in A \mid f(a) = f(1) = 1\}$.

Definizione 3.54

Siano A e B due algebre di Boole e $f\colon A \to B$ un omomorfismo tra esse. Definiamo il **nucleo** di f (denotato con **ker**(f)) come l'insieme

$$\ker(f) := \{a \in A \mid f(a) = 1\}.$$

Per ricostruire $\equiv_f$ a partire da $\ker(f)$ definiamo

$$a \equiv_{\ker(f)} b \text{ se, soltanto se, } \text{ se, soltanto se, } a \vee \neg b \in \ker(f) \text{ e } b \vee \neg a \in \ker(f) \tag{8}$$

Lemma 3.55. *Se* f *è un omomorfismo le relazioni* $\equiv_f$ *e* $\equiv_{\mathsf{ker}(f)}$ *sono uguali.*

Dimostrazione. Supponiamo $a \equiv_f b$, cioè $f(a) = f(b)$. Dobbiamo verificare che $a \vee \neg b \in \mathsf{ker}(f)$ e $b \vee \neg a \in \mathsf{ker}(f)$. Per (BA5) nella Definizione 3.30 si ha che $f(a) \vee \neg f(b) = f(a) \vee \neg f(a) = 1$, quindi $f(a \vee \neg b) = f(1) = 1$. Ne segue che $a \vee \neg b \in \mathsf{ker}(f)$. Similmente si prova che anche $b \vee \neg a \in \mathsf{ker}(f)$ da cui segue $a \equiv_{\mathsf{ker}(f)} b$.

Supponiamo ora che $a \equiv_{\mathsf{ker}(f)} b$, quindi $a \vee \neg b, b \vee \neg a \in \mathsf{ker}(f)$. In altre parole $f(a \vee \neg b) = f(b \vee \neg a) = 1$. Poiché f è un omomorfismo abbiamo anche $1 = f(a \vee \neg b) = f(a) \vee \neg f(b)$, inoltre $\neg f(b \vee \neg a) = \neg 1 = 0$ e dunque $\neg f(b) \wedge f(a) = 0$, avendo usato le leggi di De Morgan e la legge della doppia negazione (cfr. Proposizione 3.33, Punti 3 e 5). Si è dunque stabilito che $f(a) \vee \neg f(b) = 1$ e $\neg f(b) \wedge f(a) = 0$, utilizzando l'unicità del complemento (Lemma 3.29) si ha $f(a) = f(b)$ e dunque $a \equiv_f b$. □

Lemma 3.56. *Siano* A *e* B *due algebre di Boole e sia* $f \colon A \to B$ *un qualsiasi omomorfismo di algebre di Boole. Si ha che* f *è iniettivo se, e solo se,* $\mathsf{ker}(f) = \{1\}$.

Dimostrazione. Se f è iniettiva, poiché $1 \in \mathsf{ker}(f) = \{a \in A \mid f(a) = 1\}$, si ha $\mathsf{ker}(f) = \{1\}$. Viceversa, se $f(a) = f(b)$, per il Lemma 3.34 e la anti-simmetria dell'ordine si ha $\neg f(a) \vee f(b) = 1 = \neg f(b) \vee f(a)$. Poiché f è omomorfismo ricaviamo $f(\neg a \vee b) = f(\neg b \vee a) = 1$, e quindi $\neg a \vee b, \neg b \vee a \in \mathsf{ker}(f)$. Siccome $\mathsf{ker}(f) = \{1\}$ segue $\neg a \vee b = \neg b \vee a = 1$ e $a = b$ ancora per il Lemma 3.34 e la anti-simmetria dell'ordine. □

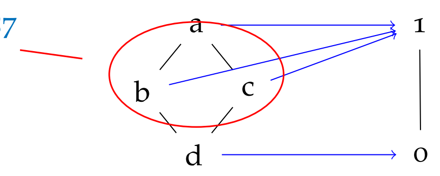
Lemma 3.57. *Siano* A *e* B *due algebre di Boole e* $f \colon A \to B$ *un omomorfismo tra di esse. Allora* $\mathsf{ker}(f)$ *soddisfa le seguenti proprietà:*

- $1 \in \mathsf{ker}(f)$,
- *per ogni* $x, y \in \mathsf{ker}(f)$, $x \wedge y \in \mathsf{ker}(f)$,
- *dati* $x \in \mathsf{ker}(f)$ *e* $y \in A$ *tali che* $x \leqslant y$, *allora* $y \in \mathsf{ker}(f)$.

Dimostrazione. Poiché $f(1) = 1$, si ha che $1 \in \mathsf{ker}(f)$. Siano $x, y \in \mathsf{ker}(f)$, allora $f(x \wedge y) = f(x) \wedge f(y) = 1 \wedge 1 = 1$ che implica $x \wedge y \in \mathsf{ker}(f)$. Sia $x \in \mathsf{ker}(f)$ e $y \in A$ tale che $x \leqslant y$. Per la Proposizione 3.39 si ha $f(x) \leqslant f(y)$. Siccome $f(x) = 1$ segue che $f(y) = 1$ e $y \in \mathsf{ker}(f)$. □

Esempio 3.58. Ricordando la funzione dell'Esempio 3.37, che non era un omomorfismo, notiamo che il suo ker non è chiuso per $\wedge$.

Non rispetta il Lemma 3.57



Abbiamo appena visto che i nuclei degli omomorfismi permettono di ricostruire la congruenza associata a questi ultimi. È naturale domandarsi quali siano le proprietà che individuano sottoinsiemi delle algebre di Boole che permettono di costruire congruenze nella stessa maniera. La risposta è che queste proprietà sono esattamente quelle elencate nel Lemma 3.57.

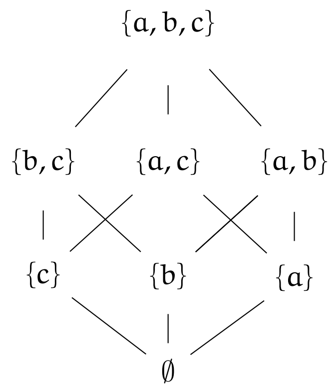
Definizione 3.59

Sia B un'algebra di Boole. Un sottoinsieme non vuoto F è detto **filtro** se:

1. per ogni $x, y \in F$, $x \wedge y \in F$,
2. dati $x \in F$ e $y \in B$ tali che $x \leqslant y$, allora $y \in F$.

In altre parole, un filtro è un sottoinsieme non vuoto che risulta chiuso per $\wedge$ e chiuso *verso l'alto*. Diremo che F è un filtro **proprio** se $F \neq B$. Indicheremo la collezione dei filtri di B con $\mathcal{F}(B)$. Notiamo che $1 \in F$ per ogni filtro F.

Esempio 3.60. Sia $X = \{a, b, c\}$. Consideriamo l'algebra di Boole $\langle \wp(X), \cap, \cup, {}^c, \emptyset, X \rangle$. Avremo la seguente rappresentazione grafica.



I filtri propri di $\wp(X)$ sono i seguenti:

- $F_1 = \{X\}$;
- $F_2 = \{X, \{a, b\}\}$, $F_3 = \{X, \{b, c\}\}$, $F_4 = \{X, \{a, c\}\}$;
- $F_5 = \{X, \{a, b\}, \{a, c\}, \{a\}\}$, $F_6 = \{X, \{b, c\}, \{a, c\}, \{c\}\}$, $F_7 = \{X, \{a, b\}, \{b, c\}, \{b\}\}$.

Osservazione 3.61. Un filtro F è proprio se, e solo se, $0 \notin F$.

Proposizione 3.62. *Sia A un'algebra di Boole e sia $F \in \mathcal{F}(A)$. Sia $\equiv_F$ la relazione definita da*

$$a \equiv_F b \textit{ se, e solo se, } \neg a \vee b \in F \textit{ e } \neg b \vee a \in F.$$

Si ha che $\equiv_F$ è una congruenza.

Dimostrazione. Sia $a \in A$. Poiché $\neg a \vee a = 1$, si ha $\neg a \vee a \in F$ e di conseguenza $a \equiv_F a$. Siano $a, b \in A$ tali che $a \equiv_F b$. Allora $a \vee \neg b \in F$ e $b \vee \neg a \in F$, che implicano, per la commutatività di $\vee$ che $b \equiv_F a$.

Verifichiamo ora la transitività. Siano $a \equiv_F b$ e $b \equiv_F c$. Di conseguenza, $a \vee \neg b, \neg a \vee b, b \vee \neg c, c \vee \neg b \in F$. Poiché F è un filtro, basta verificare che esiste $d \in F$ tale che $(a \vee \neg c) \wedge (\neg a \vee c) \geqslant d$. Si ha

$$\begin{aligned}(a \vee \neg c) \wedge (\neg a \vee c) &= ((a \vee \neg c) \wedge (\neg a \vee c)) \vee (b \wedge \neg b) = \\ &= ((a \vee \neg c) \vee (b \wedge \neg b)) \wedge ((\neg a \vee c) \vee (b \wedge \neg b)) = \\ &= ((a \vee \neg c) \vee b) \wedge ((a \vee \neg c) \vee \neg b) \wedge ((\neg a \vee c) \vee b) \wedge ((\neg a \vee c) \vee \neg b) \geqslant \\ &\geqslant (\neg c \vee b) \wedge (a \vee \neg b) \wedge (\neg a \vee b) \wedge (c \vee \neg b) \in F.\end{aligned}$$

Quindi $(a \vee \neg c) \in F$ e $(\neg a \vee c) \in F$ e $\equiv_F$ è transitiva.

Resta da verificare che $\equiv_F$ è una congruenza. Siano $a_1 \equiv_F a_2$ e $b_1 \equiv_F b_2$. Si ha che

$$\begin{aligned}(a_1 \wedge b_1) \vee \neg(a_2 \wedge b_2) &= (a_1 \wedge b_1) \vee (\neg a_2 \vee \neg b_2) = \\ &= ((a_1 \vee \neg a_2) \wedge (b_1 \vee \neg a_2)) \vee \neg b_2 = \\ &= ((a_1 \vee \neg a_2) \vee \neg b_2) \wedge ((b_1 \vee \neg a_2) \vee \neg b_2) \\ &\geqslant (a_1 \vee \neg a_2) \wedge (b_1 \vee \neg b_2) \in F.\end{aligned}$$

Si dimostra analogamente che anche $(a_2 \wedge b_2) \vee \neg(a_1 \wedge b_1) \in F$.

Quindi $(a_1 \wedge b_1) \vee \neg(a_2 \wedge b_2) \in F$ e $(a_2 \wedge b_2) \vee \neg(a_1 \wedge b_1) \in F$ e, per definizione, $a_1 \wedge b_1 \equiv_F a_2 \wedge b_2$. Allo stesso modo possiamo vedere che $a_1 \vee b_1 \equiv_F a_2 \vee b_2$:

$$\begin{aligned}(a_1 \vee b_1) \vee \neg(a_2 \vee b_2) &= (a_1 \vee b_1) \vee (\neg a_2 \wedge \neg b_2) = \\ &= a_1 \vee ((\neg a_2 \vee b_1) \wedge (b_1 \vee \neg b_2)) = \\ &= (a_1 \vee (\neg a_2 \vee b_1)) \wedge (a_1 \vee (b_1 \vee \neg b_2)) \geqslant (a_1 \vee \neg a_2) \wedge (b_1 \vee \neg b_2) \in F.\end{aligned}$$

Si dimostra analogamente che anche $(a_2 \vee b_2) \vee \neg(a_1 \vee b_1) \in F$. Quindi $(a_1 \vee b_1) \vee \neg(a_2 \vee b_2) \in F$ e $(a_2 \vee b_2) \vee \neg(a_1 \vee b_1) \in F$, così $a_1 \vee b_1 \equiv_F a_2 \vee b_2$. Per concludere, osserviamo che $(\neg a_1 \vee \neg\neg a_2) \wedge (\neg\neg a_1 \vee \neg a_2) = (\neg a_1 \vee a_2) \wedge (a_1 \vee \neg a_2) \in F$ per ipotesi e $\neg a_1 \equiv_F \neg a_2$. □

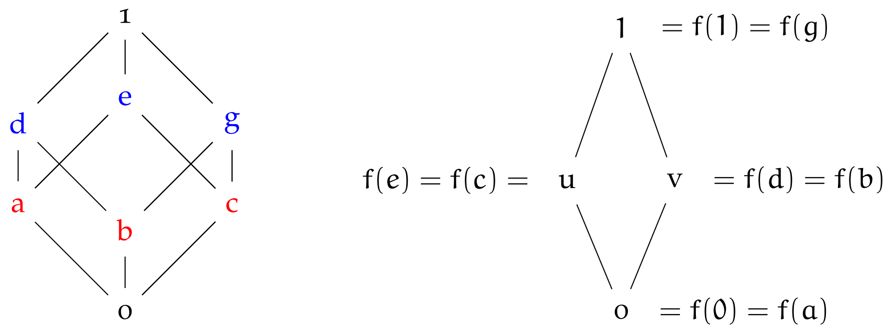
Notazione 3.63. In virtù della proposizione precedente, se A è un'algebra di Boole e F è un suo filtro, scriveremo semplicemente A/F per indicare il quoziente $A/\equiv_F$.

Osservazione 3.64. La classe di equivalenza $[1]_F \in A/F$ coincide con F. Infatti, $x \in [1]_F$ se, e soltanto se, $x \equiv_F 1$ se, e soltanto se, $\neg x \vee 1 \in F$ e $x \vee \neg 1 \in F$, ma il primo elemento è proprio 1 e appartiene sempre a F e il secondo è proprio x. Ne deriva che $x \in F$ se, e soltanto se, $x \equiv_F 1$.

Esempio 3.65. Consideriamo l'algebra di Boole B rappresentata nella figura a sinistra e sia $A = \{0, u, v, 1\}$ l'algebra rappresentata a destra. Sia $f\colon B \to A$ l'omomorfismo definito da $0 = f(0) = f(a)$, $f(d) = f(b) = v$, $f(e) = f(c) = u$, $1 = f(1) = f(g)$.

L'insieme $F = \{1, g\}$, che coincide con $\ker(f)$, è un filtro e l'algebra quoziente B/F è isomorfa ad A.

L'insieme $F = \{e, g, c, 1\}$ è ancora un filtro e in questo caso si ha $B/F = \mathbb{2}$.



Vediamo come la Proposizione 3.62 ci consente di riscrivere una delle conseguenze del Corollario 3.49 usando il concetto di filtro.

Lemma 3.66. *Sia A un'algebra di Boole. A meno di isomorfismi, c'è una corrispondenza biunivoca tra gli omomorfismi suriettivi di A, con codominio una qualsiasi algebra di Boole, e i filtri di A.*

Dimostrazione. Sia $f : A \to B$ un omomorfismo suriettivo ed $F \in \mathcal{F}(A)$. Ricordando che $\mathsf{ker}(f)$ è un filtro di A, mostriamo che le mappe $F \mapsto \pi_{\equiv_F}$ e $f \mapsto \mathsf{ker}(f)$ forniscono una biezione tra l'insieme degli epimorfismi con dominio $\mathcal{A}$ e i filtri di $\mathcal{A}$. In altre parole mostriamo che le due composizioni delle precedenti mappe producono entrambe l'identità. Iniziamo osservando che $F = \mathsf{ker}(\pi_{\equiv_F})$. Infatti, si ha che $x \in F$ se, e solo se, $x \in [1]_F$ se, e solo se, $\pi_{\equiv_F}(x) = [x]_F = [1]_F$ se, e solo se, $x \in \mathsf{ker}(\pi_{\equiv_F})$.

Per mostrare che anche l'altra composizione dà l'identità, in altre parole che f e $\pi_{\equiv_{\mathsf{Ker}(f)}}$ differiscono solo per un isomorfismo, notiamo preliminarmente che per il Lemma 3.55 $\equiv_f$ coincide con $\equiv_{\mathsf{ker}(f)}$. A questo punto basta ricordare che il Lemma 3.48 asserisce proprio che $\pi_{\equiv_f}$ differisce da f per un isomorfismo. $\square$

Lemma 3.67. *Sia B un'algebra di Boole, sia $A \subseteq B$ un sottoinsieme qualsiasi di B e sia $\mathcal{F}_A \subseteq \mathcal{F}(B)$ la collezione dei filtri di B che contengono A (incluso il filtro improprio). Allora $\bigcap_{F \in \mathcal{F}_A} F$ è un filtro.*

Dimostrazione. La dimostrazione è una semplice applicazione della definizione di filtro ed è lasciata per esercizio al lettore. Osserviamo solo che $\bigcap_{F \in \mathcal{F}_A} F$ è non vuoto in quanto contiene B. $\square$

Definizione 3.68

Per ogni sottoinsieme A di un'algebra di Boole B, diremo che il filtro $F_A = \bigcap_{F \in \mathcal{F}_A} F$ definito come nel Lemma 3.67 è il **filtro generato** da A.

Se $A = \{a\}$ chiameremo $F_{\{a\}} = F_a$ **filtro principale** generato da a.

Proposizione 3.69. *Sia* B *un'algebra di Boole e sia* $A \subseteq B$ *non vuoto. Allora*

$$F_A = \{x \in B \mid \textit{esiste } n \in \mathbb{N} \textit{ ed esistono } y_1, \dots, y_n \in A \textit{ tali che } x \geqslant y_1 \wedge \cdots \wedge y_n\}.$$

Dimostrazione. Sia $C = \{x \in B \mid \exists n \in \mathbb{N}\ \exists y_1, \dots, y_n \in A \text{ tali che } x \geqslant y_1 \wedge \cdots \wedge y_n\}$. Vediamo che C è un filtro che contiene A, e cioè che $C \in \mathcal{F}_A$.

Per ogni $a \in A$, poiché $a \geqslant a$ segue che $a \in C$. Quindi $A \subseteq C$ e C contiene sicuramente 1. Mostriamo che C è un filtro. Siano $u, v \in C$. Esistono due naturali n, m ed elementi $y_1, \dots, y_n, z_1, \dots z_m \in A$ tali che $u \geqslant y_1 \wedge \cdots \wedge y_n$ e $v \geqslant z_1 \wedge \cdots \wedge z_m$. Dalla Proposizione 3.19 Punto 6 segue che $u \wedge v \geqslant y_1 \wedge \cdots \wedge y_n \wedge z_1 \wedge \cdots \wedge z_m$, che è ancora sequenza finita di elementi di A. Quindi $u \wedge v \in C$. Analogamente, se $u \in C$ e $v \in B$ con $u \leqslant v$ esistono $y_1, \dots, y_n \in A$ tali che $u \geqslant y_1 \wedge \cdots \wedge y_n$. Di conseguenza $v \geqslant u \geqslant y_1 \wedge \cdots \wedge y_n$ e $y \in C$. Abbiamo così dimostrato che $C \in \mathcal{F}_A$ e quindi $F_A \subseteq C$. Per dimostrare l'altra inclusione, vediamo che per ogni $F \in \mathcal{F}_A$ si ha $C \subseteq F$. Sia $x \in C$ e sia $F \in \mathcal{F}_A$. Esistono $y_1, \dots, y_n \in A$ tali che $x \geqslant y_1 \wedge \cdots \wedge y_n$. Poiché $A \subseteq F$, che è filtro, $y_1 \wedge \cdots \wedge y_n \in F$ e $x \in F$. Di conseguenza $C \subseteq F$ per ogni F in $\mathcal{F}_A$, il che implica che $C \subseteq \bigcap_{F \in \mathcal{F}_A} F = F_A$. □

Definizione 3.70

Sia B un'algebra di Boole e sia A un suo sottoinsieme. Diremo che A ha la **proprietà delle intersezioni finite**, in breve **FIP**, se per ogni suo sottoinsieme finito $\{c_1, \dots, c_n\} \subseteq A$ si ha $c_1 \wedge \cdots \wedge c_n \neq 0$.

Esempio 3.71. Consideriamo l'algebra dell'Esempio 3.60. Il sottoinsieme

$$\{\{a, b\}, \{a, c\}, \{b, c\}\}$$

non ha la FIP in quanto $\{a, b\} \cap \{a, c\} \cap \{b, c\} = \emptyset$.

Lemma 3.72. *Sia* B *un'algebra di Boole e sia* $A \subseteq B$*. Il filtro* F_A *è proprio se, e solo se,* A *ha la FIP.*

Dimostrazione. Se A non ha la FIP allora esistono $y_1, \dots, y_n \in A$ tali che $0 = y_1 \wedge \cdots \wedge y_n$. Quindi $0 \geqslant 0 = y_1 \wedge \cdots \wedge y_n$ e $0 \in F_A$, dunque ogni filtro che contiene A deve contenere anche 0 e quindi non è proprio.

Viceversa, supponiamo che F_A non sia proprio, in altre parole $0 \in F_A$ quindi, per la Proposizione 3.69, esistono $y_1, \dots, y_n \in A$ tali che $0 \geqslant y_1 \wedge \cdots \wedge y_n$. Poiché 0 è il minino di B, possiamo dedurre che $0 = y_1 \wedge \cdots \wedge y_n$ e dunque A non ha la FIP. □

Esercizio 3.73. Sia B un'algebra di Boole e sia $F \in \mathcal{F}(B)$. Definiamo

$$a \sim_F b \text{ se, e solo se, } \exists f \in F \text{ tale che } a \wedge f = b \wedge f.$$

Dimostrare che $\sim_F$ è una congruenza e che $\equiv_F = \sim_F$, cioè $a \equiv_F b$ se, e solo se, $a \sim_F b$.

Concludiamo questa sezione ricordando che è possibile dare una definizione *duale* a quella di filtro. Come i filtri corrispondono alle controimmagini di 1 attraverso un omomorfismo, così gli ideali corrispondono alle contorimmagini di 0. In effetti, come vedremo nella Proposizione 3.76 è facilmente possibile passare da un filtro a un ideale e viceversa.

Definizione 3.74

Sia A un'algebra di Boole. Un sottoinsieme non vuoto $I \subseteq A$ è detto **ideale** se:

1. per ogni $a, b \in I$, $a \vee b \in I$,
2. dati $a \in I$ e $b \in A$ tali che $b \leqslant a$, allora $b \in I$.

In altre parole, un ideale è un sottoinsieme non vuoto che risulta chiuso per $\vee$ e chiuso *verso il basso*. Diremo che I è **ideale proprio** se $I \neq A$. Notiamo che $0 \in I$ per ogni ideale I e che un ideale I è proprio se, e solo se, $1 \notin I$.

Esempio 3.75.

1. In ogni algebra di Boole $\{1\}$ è un filtro e $\{0\}$ è ideale.
2. Nell'esempio Esempio 3.31 Punto 5, il sottoinsieme $\{a, b\}$ è un filtro, mentre il sottoinsieme $\{b, c\}$ è un ideale.

Proposizione 3.76. *Sia B un'algebra di Boole e sia F un filtro di B. L'insieme $\neg F = \{\neg x \mid x \in F\}$ è un ideale. Viceversa, per ogni ideale I, l'insieme $\neg I$ è un filtro.*

Dimostrazione. Sia F un filtro e siano $\neg x, \neg y \in \neg F$. Usando il Punto 5 della Proposizione 3.33 si ha $\neg x \vee \neg y = \neg(x \wedge y)$. Poiché $x, y \in F$, che è filtro, si ha $x \wedge y \in F$ e $\neg(x \wedge y) \in \neg F$, quindi $\neg F$ è chiuso per $\vee$. Siano $\neg x \in F$ e $y \in B$, con $y \leqslant \neg x$. Dalle Punti 3 e 6 della Proposizione 3.33, si ha $x \leqslant \neg y$. Poiché $x \in F$ ricaviamo che $\neg y \in F$ e $\neg(\neg y) = y \in \neg F$. La seconda parte della proposizione è analoga. □

Osservazione 3.77. Si noti che quanto visto nella Proposizione 3.62 si può adattare al caso in cui viene definita una congruenza a partire da un ideale. Infatti, per ogni ideale I di B è possibile definire la relazione $\equiv_I$ come $a \equiv_I b$ se, e solo se, $a \wedge \neg b \in I$ e $\neg a \wedge b \in I$. Inoltre il Proposizione 3.69 ha una versione duale per gli ideali: se B è un'algebra di Boole e $A \subseteq B$ non vuoto. Allora l'ideale generato da A è dato da $\{x \in B \mid \text{esiste } n \in \mathbb{N} \text{ ed esistono } y_1, \dots, y_n \in A \text{ tali che } x \leqslant y_1 \vee \dots \vee y_n\}$.

3.3.1 *Ultrafiltri*

Nella prossima sezione dimostreremo il teorema di rappresentazione di Stone che permette di vedere ogni algebra di Boole come una sottalgebra di $\wp(X)$ per un appropriato insieme X. Il concetto fondamentale per provare tale rappresentazione è quello di *ultrafiltro*.

Consideriamo l'algebra di Boole dell'Esempio 3.60. Poiché $\mathcal{F}(\wp(X)) \subseteq \wp(\wp(X))$, $\mathcal{F}(\wp(X))$ è parzialmente ordinato dall'ordine indotto da $\langle \wp(\wp(X)), \subseteq \rangle$. Ricordando che $\mathcal{F}(\wp(X))$ è dato da:

- $F_1 = \{X\}$;
- $F_2 = \{X, \{a, b\}\}$, $F_3 = \{X, \{b, c\}\}$, $F_4 = \{X, \{a, c\}\}$;
- $F_5 = \{X, \{a, b\}, \{a, c\}, \{a\}\}$, $F_6 = \{X, \{b, c\}, \{a, c\}, \{c\}\}$, $F_7 = \{X, \{a, b\}, \{b, c\}, \{b\}\}$,

otteniamo la seguente rappresentazione:

$$\begin{tikzcd}
F_7 \arrow[d, dash] \arrow[dr, dash] & F_5 \arrow[dl, dash] \arrow[dr, dash] & F_6 \arrow[dl, dash] \arrow[d, dash] \\
F_2 \arrow[dr, dash] & F_3 \arrow[d, dash] & F_4 \arrow[dl, dash] \\
& F_1 &
\end{tikzcd}$$

Gli elementi F_5, F_6 ed F_7 sono *massimali* rispetto a $\subseteq$.

Definizione 3.78

Sia B un'algebra di Boole. Un filtro *proprio* di B si dice **ultrafiltro** (o filtro **massimale**) se è massimale rispetto all'inclusione. La collezione degli ultrafiltri verrà indicata con $\mathcal{U}(B)$.

Lemma 3.79. *Sia A un'algebra di Boole e sia $U \subseteq A$ un filtro proprio di A, le seguenti sono equivalenti.*

1. *U è un ultrafiltro*
2. *se $x \vee y \in U$ allora $x \in U$ oppure $y \in U$ (filtro **primo**).*
3. *per ogni $x \in A$, si ha $x \in U$ o $\neg x \in U$ (filtro **completo**).*
4. *$A/U \cong \{0, 1\}$.*

Dimostrazione. Punto 1 $\Rightarrow$ Punto 2. Sia U un ultrafiltro tale che $x \notin U$ e $y \notin U$. Consideriamo allora i filtri generati $F_{U \cup \{x\}}$ e $F_{U \cup \{y\}}$, poiché U è massimale, devono essere entrambi uguali a B. Per la Proposizione 3.69 esistono $u_1, \ldots, u_n \in U$ e $v_1, \ldots, v_m \in U$ tali che $0 = u_1 \wedge \cdots \wedge u_n \wedge x = v_1 \wedge \cdots \wedge v_m \wedge y$, avendo usato il fatto che U ha la FIP. Per ogni $i \leqslant k = \max\{m, n\}$ sia $w_i := u_i \wedge v_i$ se esistono entrambi u_i e v_i, altrimenti poniamo w_i uguale all'unico che esiste tra u_i e v_i. Per la monotonia di $\wedge$ (Punto 6 della Proposizione 3.19) abbiamo che $0 = w_1 \wedge \cdots \wedge w_k \wedge x = w_1 \wedge \cdots \wedge w_k \wedge y$ e dunque

$$\begin{aligned} 0 &= (w_1 \wedge \cdots \wedge w_k \wedge x) \vee (w_1 \wedge \cdots \wedge w_k \wedge y) = \\ &= (w_1 \wedge \cdots \wedge w_k) \wedge (x \vee y) \end{aligned}$$

Poiché U ha la FIP se ne deduce che $x \vee y \notin U$ e la condizione Punto 2 è dimostrata.

Punto 2 $\Rightarrow$ Punto 3. Poiché U è un filtro $1 \in U$, ma per ogni $x \in A$, $1 = \neg x \vee x$. Dunque il Punto 2 implica $x \in U$ oppure $\neg x \in U$.

Punto 3 $\Rightarrow$ Punto 4. L'insieme A/U è dato dalle classi di equivalenza di $\equiv_U$. Per l'Osservazione 3.64, $[1]_U = U$, quindi $a \in [1]_{\equiv_U}$ sse $a \in U$ e $a \in [0]_{\equiv_U}$ sse $\neg a \in U$. Ma per il Punto 3 questi sono gli unici casi possibili, dunque A/U è formato da due elementi e necessariamente isomorfo a l'algebra di Boole $\{0, 1\}$.

Punto 4 $\Rightarrow$ Punto 1. Sia $A/U \cong \mathbb{2}$, supponiamo che esista un filtro proprio F tale che $U \subseteq F$ e sia $x \in F \setminus U$. Allora (sempre per l'Osservazione 3.64) $[x]_U \neq [1]_U$ e quindi $[x]_U = [0]_U$, o equivalentemente $[\neg x]_U = [1]_U$. Dunque $\neg x \in U \subseteq F$, da cui $0 = x \wedge \neg x \in F$ e quindi F non è proprio. Dunque U è massimale, come volevasi dimostrare. $\square$

Osservazione 3.80. Osserviamo che, poiché un ultrafiltro U, per definizione, è proprio si ha che $x \in U$ oppure $\neg x \in U$ ma non entrambe.

Proposizione 3.81. *Sia $X \neq \emptyset$ e consideriamo l'algebra $\langle \wp(X), \cap, \cup, {}^c, \emptyset, X \rangle$. Per ogni $x \in X$ si ha che $F_{\{x\}}$ è un ultrafiltro.*

Dimostrazione. Osserviamo che $F_{\{x\}} = \{A \in \wp(X) \mid \{x\} \subseteq A\} = \{A \in \wp(X) \mid x \in A\}$. Quindi $F_{\{x\}}$ ha la FIP: per ogni $A_1, \dots, A_k \in F_{\{x\}}$ si ha che $x \in A_1 \cap \dots \cap A_k$. Sia ora $A \notin F_{\{x\}}$. Allora $x \notin A$ e quindi $x \in X \setminus A$, che implica $X \setminus A \in F_{\{x\}}$. La tesi segue ora dal Lemma 3.79. $\square$

Vediamo ora che ogni filtro si può estendere a un ultrafiltro.

Teorema 3.82 (dell'ultrafiltro)

Sia B un'algebra di Boole. Ogni filtro proprio di B si estende ad un ultrafiltro.

Dimostrazione. Sia F un filtro proprio di B e sia $\mathcal{A}$ l'insieme dei filtri propri di B che estendono F. Ovviamente $\mathcal{A}$ è non vuoto, perché $F \in \mathcal{A}$. Mostriamo che ogni catena $\mathcal{C}$ in $\mathcal{A}$ ha un maggiorante in $\mathcal{A}$: $\bigcup \mathcal{C}$. Ovviamente $\bigcup \mathcal{C}$ *è non vuoto* ed *estende* F. Mostriamo che $\cup \mathcal{C}$ è un filtro. Se $a, b \in \bigcup \mathcal{C}$ allora esistono $H, K \in \mathcal{C}$ tali che $a \in H$ e $b \in K$. Poiché $\mathcal{C}$ è una catena, possiamo assumere $H \subseteq K$, quindi $a, b \in K$ e dunque $a \wedge b \in K \subseteq \bigcup \mathcal{C}$. Similmente se $a \in \bigcup \mathcal{C}$ e $b \geqslant a$, allora $b \in \bigcup \mathcal{C}$. Infine, ovviamente $0 \notin \bigcup \mathcal{C}$ perché non appartiene a nessuno degli elementi di $\mathcal{C}$. Quindi $\bigcup \mathcal{C}$, che è un filtro proprio che contiene F, è il maggiorante cercato.

Applicando ora il lemma di Zorn, ottenendo un filtro $\mathcal{U}$ massimale *tra quelli che estendono* F. Resta da verificare che $\mathcal{U}$ è un ultrafiltro di B. Ciò segue dal fatto che se un filtro estende $\mathcal{U}$ allora contiene anche F. $\square$

Corollario 3.83. *Sia* B *un'algebra di Boole e sia* $\emptyset \neq A \subseteq B$ *un sottoinsieme con la FIP. Allora* A *si estende a un ultrafiltro.*

Dimostrazione. Se A ha la FIP, allora per il Lemma 3.72 si può estendere a un filtro proprio F. Per il Teorema 3.82 il filtro F si può estendere a un ultrafiltro. Quindi abbiamo $A \subseteq F \subseteq U$ e la dimostrazione è conclusa. □

Corollario 3.84. *Sia* B *un'algebra di Boole,* $c \in B$ *e* F *un filtro proprio di* B *tale che* $c \notin F$. *Allora esiste un ultrafiltro* U *di* B *che estende* F, *cioè* $F \subseteq U$, *ma non contiene* c.

Dimostrazione. L'insieme $F \cup \{\neg c\}$ ha la FIP. Infatti, se esistessero $f_1, \ldots, f_k \in F$ tali che $f_1 \wedge \cdots \wedge f_k \wedge \neg c = 0$ si avrebbe $f_1 \wedge \cdots \wedge f_k \leqslant c$ e quindi $c \in F$, contro l'ipotesi. Per il Corollario 3.83 l'insieme $F \cup \{\neg c\}$ è estendibile a un ultrafiltro U. Si noti che U non può contenere c, perché se così fosse avremmo che $0 = c \wedge \neg c \in U$ e ciò non è possibile perché U è proprio per definizione. □

Corollario 3.85. *Dati due elementi* x, y *di un'algebra di Boole, con* $x \neq y$, *esiste sempre un ultrafiltro che contiene un elemento ma non l'altro.*

Dimostrazione. Poiché $x \neq y$ sicuramente almeno una tra $x \leqslant y$ e $y \leqslant x$ non vale. Supponiamo che $x \nleqslant y$. Per il Lemma 3.34, $x \wedge \neg y \neq 0$ e quindi $\{x, \neg y\}$ ha la FIP. Per il Corollario 3.83 esiste un ultrafiltro U che estende $\{x, \neg y\}$. Inoltre, $y \notin U$ altrimenti si avrebbe $0 = y \wedge \neg y \in U$. □

3.3.2 *Il teorema di rappresentazione di Stone*

I teoremi di rappresentazione sono di cruciale importanza perché consentono di trasferire informazioni da aree diverse della matematica. Anche se presentato in maniera semplificata, il seguente teorema è un ponte tra algebra e topologia.

Teorema 3.86 (Rappresentazione di Stone)

Sia $\langle A, \wedge, \vee, \neg, 0, 1 \rangle$ *una algebra di Boole. Esiste un insieme* X *tale che* A *è isomorfa a una sottalgebra di* $\langle \wp(X), \cup, \cap, {}^c, \emptyset, X \rangle$.

Dimostrazione. Sia $X = \mathcal{U}(A)$, l'insieme dei filtri massimali di A, e sia $e : A \to \wp(X)$ definita da

$$a \in A \longmapsto \{F \in \mathcal{U}(A) \mid a \in F\}.$$

La funzione e *è iniettiva*: infatti se $a \neq b$, per Corollario 3.85 esiste un ultrafiltro che contiene a e non b. Di conseguenza, $e(a) \neq e(b)$.

La funzione e *è un omomorfismo.* Si osserva che $1 \in F$ per ogni $F \in \mathcal{U}(A)$, quindi $e(1) = \mathcal{U}(A)$, mentre $0 \notin F$ per ogni $F \in \mathcal{U}(A)$, quindi $e(0) = \emptyset$.

$$\begin{aligned}
e(a \vee b) &= \{F \in \mathcal{U}(A) \mid a \vee b \in F\} = \\
&= \{F \in \mathcal{U}(A) \mid a \in F \text{ o } b \in F\} = \\
&= \{F \in \mathcal{U}(A) \mid a \in F\} \cup \{F \in \mathcal{U}(A) \mid b \in F\} = e(a) \cup e(b). \\
e(a \wedge b) &= \{F \in \mathcal{U}(A) \mid a \wedge b \in F\} = \\
&= \{F \in \mathcal{U}(A) \mid a \in F \text{ e } b \in F\} = \\
&= \{F \in \mathcal{U}(A) \mid a \in F\} \cap \{F \in \mathcal{U}(A) \mid b \in F\} = e(a) \cap e(b).
\end{aligned}$$

Per concludere, $e(\neg x) = \{F \in \mathcal{U}(A) \mid \neg x \in F\}$. Essendo ogni ultrafiltro proprio si ha che $\neg x \in F$ se, e solo se, $x \notin F$ e di conseguenza $U \in e(\neg x)$ se, e solo se, $U \notin e(x)$ se, e solo se, $U \in \mathcal{U}(A) \setminus e(x)$. Notiamo infine che, per quanto detto all'inizio della Sezione 3.2.2, l'immagine $e[A]$ di A tramite e è una sottalgebra di $\wp(X)$. Quindi, in base a quanto detto sopra, e è un isomorfismo tra A e $e[A]$. □

Si noti che in generale i sottoinsiemi di un insieme X sono in corrispondenza biunivoca con le funzioni da X in $\{0, 1\}$. Infatti a un insieme $S \subseteq X$ possiamo associare una funzione $\chi_S \colon X \to \{0, 1\}$ tale che $\chi_S(x) = 1$ se, e soltanto se, $x \in S$. Viceversa, a ogni funzione $f \colon X \to \{0, 1\}$ possiamo associare il sottoinsieme di X definito come $\{x \in X \mid f(x) = 1\}$. La funzione χ_S è detta la **funzione caratteristica** di S. Dunque il Teorema di Stone può essere equivalentemente enunciato come segue

Corollario 3.87 (Formulazione equivalente del Teorema di rappresentazione di Stone)**.** *Per ogni algebra di Boole A esiste un insieme X tale che A è isomorfa a una sottalgebra di $\Pi_{x \in X} A_x$ dove tutte le A_x sono copie isomorfe dell'algebra di Boole $\{0, 1\}$ e $\Pi_{x \in X}$ rappresenta il prodotto diretto.*

Dimostrazione. Basta dimostrare che per ogni insieme X, l'algebra $\langle \wp(X), \cup, \cap, \neg, \emptyset, X \rangle$ è isomorfa al prodotto diretto $\mathbb{2}^X$. Notiamo preliminarmente che l'algebra $\mathbb{2}^X$ può essere vista sia come l'algebra delle tuple 0 e 1, indiciate da X, con le operazioni definite componente per componente sia come l'algebra delle funzioni da X in $\{0, 1\}$, dove le operazioni sono definite punto per punto. Definiamo dunque un isomorfismo i da $\wp(X)$ in $\mathbb{2}^X$ ponendo, per ogni $S \subseteq X$, $i(S) := \chi_S$. Per quanto detto nel paragrafo precedente al Corollario 3.87, i è una funzione biettiva. Resta da verificare che i preserva le operazioni. Calcoliamo, per $S, T \subseteq X$:

$$\begin{aligned}
i(S \cap T) &= \chi_{S \cap T} = \min\{\chi_S, \chi_T\}, \\
i(S \cup T) &= \chi_{S \cup T} = \max\{\chi_S, \chi_T\}, \\
i(\neg T) &= \chi_{\neg T} = 1 - T.
\end{aligned}$$

□

3.4 completezza algebrica

3.4.1 *Termini ed equazioni booleane*

È giunto il momento di fare un po' di chiarezza sulla notazione, abbastanza rilassata, usata in questo capitolo. Abbiamo infatti usato gli stessi simboli $\wedge, \vee, \neg$, etc. per denotare sia i connettivi logici che le operazioni nelle algebre di Boole (e a volte anche le operazioni concrete!). Di per sé ciò non rappresenta un grande problema, visto che di solito è semplice capire dal contesto se ci stiamo riferendo a un'operazione booleana o a un connettivo logico. Inoltre in questa sezione vedremo che tale confusione di notazione è in qualche modo giustificata da risultati matematici. Ma proprio perché intendiamo collegare la validità di equazioni nelle algebre di Boole con la validità di formule nella logica proposizionale, conviene fare un po' di chiarezza sulla notazione prima di intraprendere questo lavoro.

Per poter fare chiarezza è necessario distinguere i diversi usi dei simboli. Quindi, d'ora in avanti e fino alla fine di questo capitolo, indichiamo i connettivi con $\wedge, \vee, \neg$, i simboli di operazioni booleane con $\underline{\wedge}, \underline{\vee}, \underline{\neg}$ e le loro interpretazioni in un'algebra A con $\underline{\wedge}^A, \underline{\vee}^A, \underline{\neg}^A$.

Seguendo il parallelo con la logica proposizionale, data una qualsiasi algebra di Boole, ha senso definire le operazioni:

$$
\begin{aligned}
x \mathbin{\underline{\rightarrow}} y &:= \underline{\neg} x \mathbin{\underline{\vee}} y, \\
x \mathbin{\underline{\leftrightarrow}} y &:= (x \mathbin{\underline{\rightarrow}} y) \mathbin{\underline{\wedge}} (y \mathbin{\underline{\rightarrow}} x).
\end{aligned}
$$

Ma ovviamente ci sono tante altre operazioni definibili a partire da quelle di base di algebra di Boole. La seguente definizione descrive l'insieme di tutte le operazioni definibili.

Sia $\mathtt{VarX} := \{x, y, z, \dots x_1, x_2, \dots\}$ un insieme numerabile di simboli, che chiameremo variabili **individuali**.

Definizione 3.88

Definiamo l'insieme `Term` dei **termini** (o **funzioni definibili**) in analogia con `Form`:

- ogni elemento di `VarX` appartiene a `Term`,
- se $t \in \mathtt{Term}$, allora anche $(\underline{\neg} t) \in \mathtt{Term}$,
- se $t, s \in \mathtt{Term}$, allora anche
  - $(t \mathbin{\underline{\wedge}} s) \in \mathtt{Term}$,
  - $(t \mathbin{\underline{\vee}} s) \in \mathtt{Term}$,

Scriveremo $t(x_1, ..., x_n)$ per evidenziare il fatto che le variabili individuali in t sono *comprese* tra le variabili $x_1, \dots, x_n$.

Il concetto di termine ci permette di dare una nuova caratterizzazione della sottalgebra generata da un insieme definita nella Definizione 3.52.

Lemma 3.89. *Sia* A *un'algebra di Boole e* $\emptyset \neq S \subseteq A$. *La sottalgebra generata da* S *è data dalla* chiusura algebrica *di* S. *In altre parole,*

$$\langle S \rangle = \{a \in A \mid \exists t(x_1, \dots, x_n) \in \mathtt{Term},\ \exists s_1, \dots, s_n \in S,\ a = t(s_1 \dots, s_n)\}$$

Dimostrazione. Iniziamo con il notare che l'insieme $B := \{a \in A \mid \exists t(x_1, \dots, x_n) \in \mathtt{Term}, \exists s_1, \dots, s_n \in S,\ a = t(s_1 \dots, s_n)\}$ è una sottalgebra di A contenente S. Se infatti b_1, b_2 sono elementi di B allora esistono due termini $t_1(x_1, \dots, x_n), t_2(y_1, \dots, y_m)$ e $r_1, \dots, r_n, s_1, \dots, s_m \in S$ tali che $b_1 = t_1(r_1, \dots, r_n)$ e $b_2 = t_2(s_1, \dots, s_m)$. Se $\star \in \{\triangle, \veebar\}$, allora $b_1 \star b_2 = (t_1(r_1, \dots, r_n)) \star (t_2(s_1, \dots, s_m))$ ma $(t_1(x_1, \dots, x_n)) \star (t_2(y_1, \dots, y_m))$ è ancora un termine, che possiamo denotare con $u(x_1, \dots x_n, y_1, \dots, y_m)$ e dunque $b_1 \star b_2$ appartiene a B perché $b_1 \star b_2 = u(r_1, \dots, r_n, s_1, \dots, s_m)$. Un simile ragionalmento mostra che B è anche chiuso rispetto a $\underline{\neg}$. Inoltre è immediato vedere che $S \subseteq B$. Dunque, poiché $\langle S \rangle$ è la più piccola sottalgebra di A contenente S, segue che $\langle S \rangle \subseteq B$. Per vedere che vale anche l'inclusione opposta, si noti per ogni termine $t(x_1, \dots, x_n)$ e per ogni tupla $s_1, \dots, s_n \in S$ deve valere che $t(s_1, \dots, s_n) \in \langle S \rangle$ poiché quest'ultimo è chiuso rispetto alle operazioni booleane e ogni termine è una combinazione di esse. Ciò conclude la dimostrazione. □

Definizione 3.90

Un'**equazione** nel linguaggio delle algebre di Boole è una coppia di termini (s, t). Per rendere più chiara la lettura indicheremo un'equazione (s, t) con $s \approx t$.

Definizione 3.91

Se $A = \langle A, \triangle^A, \veebar^A, \underline{\neg}^A, 0^A, 1^A \rangle$ è un algebra di Boole, chiamiamo **interpretazione** in A una qualsiasi funzione $e\colon \mathtt{VarX} \to A$. In analogia con le valutazioni, un'interpretazione e si *estende univocamente* a una funzione $\hat{e}\colon \mathtt{Term} \to A$ come segue: per ogni $t \in \mathtt{Term}$

- se $t \in \mathtt{VarX}$ allora $\hat{e}(t) = e(t)$,
- se $t = (t_1 \triangle t_2)$ allora $\hat{e}(t) = \hat{e}(t_1) \triangle^A \hat{e}(t_2)$,
- se $t = (t_1 \veebar t_2)$ allora $\hat{e}(t) = \hat{e}(t_1) \veebar^A \hat{e}(t_2)$,
- se $t = (\underline{\neg} t_1)$ allora $\hat{e}(t) = \underline{\neg}^A \hat{e}(t_1)$.

Quando l'interpretazione è chiara dal contesto, scriveremo t^A per indicare l'interpretazione del termine t in A.

Un'interpretazione $e\colon \mathtt{VarX} \to A$, verifica un'equazione $s(x_1, \ldots, x_n) \approx t(x_1, \ldots, x_n)$, se l'identità

$$\hat{e}\,(s(x_1, \ldots, x_n)) = \hat{e}\,(t(x_1, \ldots, x_n))$$

o, equivalentemente,

$$s^A(e(x_1), \ldots, e(x_n)) = t^A(e(x_1), \ldots, e(x_n))$$

è vera in A.

L'equazione $s(x_1, \ldots, x_n) \approx t(x_1, \ldots, x_n)$ è **valida** (o è verificata) in A se ogni interpretazione e a valori in A verifica l'equazione. Cioè, se per ogni $e\colon \mathtt{VarX} \to A$, l'uguaglianza

$$s^A(e(x_1), \ldots, e(x_n)) = t^A(e(x_1), \ldots, e(x_n))$$

vale in A. Per indicare ciò useremo il simbolo $\models_{BA}$, in altre parole se l'equazione $s(x_1, \ldots, x_n) \approx t(x_1, \ldots, x_n)$ è valida in A scriveremo

$$A \models_{BA} s(x_1, \ldots, x_n) \approx t(x_1, \ldots, x_n).$$

Se Γ è un insieme di equazioni, scriveremo

$$\Gamma \models_{BA} s(x_1, \ldots, x_n) \approx t(x_1, \ldots, x_n)$$

se per ogni algebra di Boole A, ogni interpretazione in A che rende valide tutte le equazioni in Γ, rende valida anche $s(x_1, \ldots, x_n) \approx t(x_1, \ldots, x_n)$.

Aver definito formalmente l'equazioni nel linguaggio delle algebre di Boole, ci permette di dimostrare un'importante conseguenza del teorema di Stone.

Corollario 3.92. *Un'equazione nel linguaggio delle algebre di Boole è vera in tutte le algebre di Boole se, e soltanto se, è vera nell'algebra di Boole $\mathbb{2}$.*

Dimostrazione. Un verso è banale. Per l'altro ragioniamo sulla contronominale. Supponiamo che un equazione $s(x_1, \ldots, x_n) \approx t(x_1, \ldots, x_n)$ fallisca in qualche algebra di Boole A, dunque esiste un'interpretazione e in A tale che $\tilde{e}(s(x_1, \ldots, x_n)) \neq \tilde{e}(t(x_1, \ldots, x_n))$. Per il teorema di Stone (Corollario 3.87), A è isomorfa a una sottalgebra di $\Pi_{x \in X} A_x$ dove tutte le A_x sono copie isomorfe dell'algebra di Boole $\mathbb{2}$. Inoltre, l'interpretazione e può essere vista come un interpretazione a valori in $\Pi_{x \in X} A_x$ e dunque anche in quest'ultima algebra abbiamo che $\tilde{e}(s(x_1, \ldots, x_n)) \neq \tilde{e}(t(x_1, \ldots, x_n))$. Ciò vuol dire gli elementi $\tilde{e}(s(x_1, \ldots, x_n))$ e $\tilde{e}(t(x_1, \ldots, x_n))$ differiscono per qualche componente, in altre parole, deve esistere una proiezione $\pi\colon \Pi_{x \in X} A_x \to A_x$ tale che $\pi(\tilde{e}(s(x_1, \ldots, x_n))) \neq \pi(\tilde{e}(t(x_1, \ldots, x_n)))$. Ovviamente $\pi \circ e$ è un'interpretazione in $\mathbb{2}$ e si vede facilmente che $\widetilde{\pi \circ e} = \pi \circ \tilde{e}$, dunque l'interpretazione $\pi \circ e$ fa fallire l'equazione $s(x_1, \ldots, x_n) \approx t(x_1, \ldots, x_n)$ in $\mathbb{2}$, come volevasi dimostrare. $\square$

3.4.2 *Algebre libere*

Definizione 3.93

Sia A un'algebra di Boole e sia $X \subseteq A$ un suo sottoinsieme che la genera. L'algebra A è detta **liberamente generata** da X (gli elementi di X sono detti **generatori liberi**) se,

per ogni algebra di Boole B, ogni *funzione* da X in B si estende a un *omomorfismo* da A in B.

Esempio 3.94. È possibile mostrare che l'algebra a sinistra in Figura 3 è liberamente generata da $\{x\}$, una dimostrazione rigorosa richiederebbe un argomento più generale, ma per familiarizzare con il concetto di algebra liberamente generata è utile prendere come algebra B quella a destra in Figura 3 e convincersi che ogni assegnazione di x a un elemento di B si estende univocamente a un omomorfismo di algebre di Boole. Tale riflessione è lasciata al lettore.

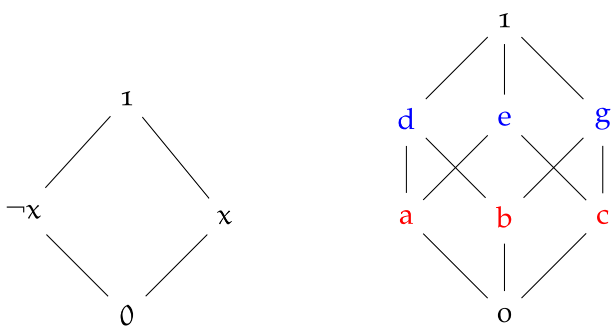


Figura 3: Le algebre nell'Esempio 3.94.

Indicheremo con $\mathtt{Free}(X)$ l'algebra liberamente generata da X.

Teorema 3.95 (Unicità delle algebre libere)

Se X e Y sono due insiemi della stessa cardinalità, allora $\mathtt{Free}(X) \cong \mathtt{Free}(Y)$.

Dimostrazione. poiché X e Y hanno la stessa cardinalità, esiste una biezione $f : X \to Y$. Se $g : Y \to X$ denota l'inversa di f, siano $\overline{f} : X \to \mathtt{Free}(Y)$ e $\overline{g} : Y \to \mathtt{Free}(X)$ le funzioni definite da $\overline{f}(x) = f(x)$ e $\overline{g}(y) = g(y)$. Per la definizione di algebra libera, entrambe $\overline{f}$ e $\overline{g}$ si estendono a $\widetilde{f} : \mathtt{Free}(X) \to \mathtt{Free}(Y)$ e $\widetilde{g} : \mathtt{Free}(Y) \to \mathtt{Free}(X)$, omomorfismi di algebre di Boole. Vediamo che $\widetilde{f} \circ \widetilde{g}$ e $\widetilde{g} \circ \widetilde{f}$ sono rispettivamente le funzioni identità su $\mathtt{Free}(Y)$ e $\mathtt{Free}(X)$. Essendo omomorfismi di algebre di Boole ed essendo $\mathtt{Free}(X)$ e $\mathtt{Free}(Y)$ generate da X e Y, dal Lemma 3.89, è sufficiente notare che, per ogni $x \in X$ e per ogni $y \in Y$, $\widetilde{g}(\widetilde{f}(x)) = \widetilde{g}(f(x)) = g(f(x)) = x$ e $\widetilde{f}(\widetilde{g}(y)) = \widetilde{f}(g(y)) = f(g(y)) = y$. □

Le algebre libere hanno la seguente importante proprietà.

Lemma 3.96. *L'equazione nel linguaggio delle algebre di Boole*

$$t(x_1, \dots, x_n) \approx s(x_1, \dots, x_n)$$

è valida nell'algebra libera generata da $X = \{x_1, \dots, x_n\}$ se, e soltanto se, è valida in tutte le algebre di Boole.

Dimostrazione. Un'implicazione è ovvia. Per l'altra, ragioniamo sulla contronominale. Supponiamo quindi che $t(x_1, \dots, x_n) \approx s(x_1, \dots, x_n)$ fallisca in qualche algebra di Boole A. Questo vuol dire che esistono $a_1, \dots, a_n \in A$ tali che in A si ha $t^A(a_1, \dots, a_n) \neq s^A(a_1, \dots, a_n)$.

Consideriamo l'assegnazione $x_i \mapsto a_i$ per ogni $1 \leqslant i \leqslant n$. Per la definizione stessa di algebra libera, essa si estende a un omomorfismo $\tilde{f}\colon \mathtt{Free}(X) \to A$. A questo punto si ha

$$\begin{aligned} \tilde{f}\big(t^{\mathtt{Free}(X)}(x_1, \dots, x_n)\big) &= t^A(f(x_1), \dots, f(x_n)) = \\ &= t^A(a_1, \dots, a_n) \neq s^A(a_1, \dots, a_n) = \\ &= s^A(f(x_1), \dots, f(x_n)) = \\ &= \tilde{f}\big(s^{\mathtt{Free}(X)}(x_1, \dots, x_n)\big) \end{aligned}$$

Quindi $t^{\mathtt{Free}(X)}(x_1, \dots, x_n)$ e $s^{\mathtt{Free}(X)}(x_1, \dots, x_n)$ sono diversi anche in $\mathtt{Free}(X)$ e la dimostrazione è conclusa. □

Vediamo ora come "costruire" algebre di Boole libere utilizzando le formule della logica proposizionale.

Fissiamo un arbitrario $P \subseteq \mathrm{Var}$ e indichiamo con $\mathtt{Form}(P)$ l'insieme delle formule proposizionali (Definizione 2.2) le cui variabili appartengono a P. Sia Γ un suo sottoinsieme coerente. Nella Definizione 2.18 abbiamo definito la relazione $\equiv$. Definiamo ora una relazione più generale $\equiv_\Gamma$ come segue:

$$\varphi \equiv_\Gamma \psi \text{ se, soltanto se, } \Gamma \vdash \varphi \leftrightarrow \psi.$$

Se $\Gamma = \emptyset$, le relazioni $\equiv_\Gamma$ e $\equiv$ coincidono.

Esercizio 3.97. Dimostrare che la relazione d'equivalenza $\equiv_\Gamma$ è una congruenza.

Questa osservazione ci consente di dotare il quoziente $\mathtt{Form}(P)/\equiv_\Gamma$ della struttura di algebra di Boole definendo

$$
\begin{aligned}
0 := [\bot]_{\equiv_\Gamma} &\qquad 1 := [\top]_{\equiv_\Gamma} \\
[\varphi]_{\equiv_\Gamma} \underline{\wedge} [\psi]_{\equiv_\Gamma} &:= [\varphi \wedge \psi]_{\equiv_\Gamma}, \\
[\varphi]_{\equiv_\Gamma} \underline{\vee} [\psi]_{\equiv_\Gamma} &:= [\varphi \vee \psi]_{\equiv_\Gamma}, \\
\underline{\neg} [\varphi]_{\equiv_\Gamma} &:= [\neg\varphi]_{\equiv_\Gamma}.
\end{aligned}
$$

Le algebre di questo tipo sono anche note come algebre di **Lindenbaum-Tarski**. Indicheremo con $\mathtt{LT}_\Gamma(P)$ l'algebra qui definita. Dalla definizione delle operazioni e il Lemma 3.34, possiamo osservare che $[\varphi]_\Gamma \leqslant [\psi]_\Gamma$ se, e solo se $[\neg\varphi \vee \psi]_\Gamma = [\top]_\Gamma$. Di conseguenza, l'ordine è dato da:

$$[\varphi]_\Gamma \leqslant [\psi]_\Gamma \text{ se, soltanto se, } \Gamma \vdash \varphi \to \psi. \tag{9}$$

Il prossimo risultato ha il duplice effetto di chiarire il ruolo di rilievo giocato da $\mathtt{LT}_\emptyset(P)$ e contemporaneamente dimostrare che le algebre libere esistono.

Teorema 3.98 (Birkhoff)

Sia $P \subseteq \mathsf{Var}$, l'algebra di Lindenbaum-Tarski $\mathtt{LT}_\emptyset(P)$ è l'algebra libera generata da (le classi di equivalenza di elementi di) P.

Dimostrazione. Iniziamo notando che con una semplice induzione è possibile dimostrare che in effetti l'insieme $[P] := \{[p]_{\equiv_\emptyset} \mid p \in P\}$ genera $\mathtt{LT}_\emptyset(P)$, sfruttando il Lemma 3.89. In questa dimostrazione usiamo semplicemente le parentesi quadre per denotare le classi di equivalenza modulo $\equiv$.

Sia ora f un'assegnazione da $[P]$ in un'algebra di Boole A. Definiamo per induzione una funzione $\tilde{f}\colon \mathtt{LT}_\emptyset(P) \to A$:

$$
\begin{aligned}
\tilde{f}([p]) &:= f([p]) \text{ per ogni } p \in P, \\
\tilde{f}([\varphi \wedge \psi]) &:= \tilde{f}([\varphi]) \mathbin{\underline{\wedge}^A} \tilde{f}([\psi]) \\
\tilde{f}([\neg\varphi]) &:= \underline{\neg}\tilde{f}([\varphi])^A.
\end{aligned}
$$

Si dimostra facilmente che, in base a questa definizione, valgono anche:

$$
\begin{aligned}
\tilde{f}([\varphi \vee \psi]) &= \tilde{f}([\varphi]) \mathbin{\underline{\vee}^A} \tilde{f}([\psi]), \\
\tilde{f}([\bot]) = 0^A &\text{ e } \tilde{f}([\top]) = 1^A.
\end{aligned}
$$

Dunque $\tilde{f}$ è un omomorfismo che estende f. Inoltre è unico, perché qualsiasi omomorfismo che estenda f deve verificare le equazioni che definiscono $\tilde{f}$ e perciò coincide con $\tilde{f}$. □

3.4.3 *Connettivi logici e operazioni booleane*

Se assumiamo che esista una biezione $\mathtt{b}\colon \mathsf{Var} \to \mathtt{VarX}$ (in altre parole, se assumiamo che Var e $\mathtt{VarX}$ abbiano la stessa cardinalità) le formule in $\mathtt{Form}$ possono essere trasformate in termini in $\mathtt{Term}$.. Supponiamo per semplicità che $\mathtt{b}(p_i) = x_i$ e definiamo la traduzione come segue:

$$\begin{array}{cccc} \text{Se} & p_i \in \mathsf{Var}, & \text{allora} & p_i^T := x_i, \\ \text{Se} & \varphi = \varphi_1 \wedge \varphi_2, & \text{allora} & \varphi^T := \varphi_1^T \triangle \varphi_2^T \\ \text{Se} & \varphi = \varphi_1 \vee \varphi_2, & \text{allora} & \varphi^T := \varphi_1^T \veebar \varphi_2^T \\ \text{Se} & \varphi = \neg\varphi_1, & \text{allora} & \varphi^T := \underline{\neg}\varphi_1^T. \end{array}$$

Viceversa, termini booleani possono essere trasformati in formule:

$$\begin{array}{cccc} \text{Se} & x_i \in \mathtt{VarX}, & \text{allora} & x_i^L := p_i, \\ \text{Se} & t = t_1 \triangle t_2, & \text{allora} & t^L := t_1^L \wedge t_2^L \\ \text{Se} & t = t_1 \veebar t_2, & \text{allora} & t^L := t_1^L \vee t_2^L \\ \text{Se} & t = \underline{\neg} t_1, & \text{allora} & t^L := \neg t_1^L. \end{array}$$

Le precedenti traduzioni permettono di trasformare formule proposizionali in equazioni e viceversa:

$$\text{Se } \varphi \text{ è una formula, definiamo } \varphi^= \text{ come } \varphi^T \approx 1,$$
$$\text{Se } s \approx t \text{ è un'equazione, definiamo } (s \approx t)^{\leftrightarrow} \text{ come } s^L \leftrightarrow t^L.$$

Queste traduzioni permettono di aggiungere al teorema di completezza visto all'inizio (Teorema 2.70) un passo intermedio:

$$\Gamma \vdash \varphi \text{ se, soltanto se, } \Gamma^= \models_{BA} \varphi^= \text{ se, soltanto se, } \Gamma \models \varphi$$

Prima di dimostrare tale risultato, è però necessario approfondire ancora un po' lo studio delle algebre di Lindenbaum-Tarski.

Lemma 3.99. *Sia $\mathsf{P} \subseteq \mathsf{Var}$ e Γ un insieme di formule le cui variabili proposizionali appartengono tutte a P, scriviamo $[\Gamma] := \{[\gamma]_\equiv \mid \gamma \in \Gamma\}$. Allora si ha che il filtro generato da $[\Gamma]$ in $\mathsf{LT}_\emptyset(\mathsf{P})$ è dato da $\mathcal{F}_{[\Gamma]} = \{[\varphi] \mid \varphi \in \mathsf{Var}(\mathsf{P})$ e $\Gamma \vdash \varphi\}$.*

Dimostrazione. Per la Proposizione 3.69,

$$\mathcal{F}_{[\Gamma]} = \{[\varphi] \in \mathsf{LT}_\emptyset(\mathsf{P}) \mid \exists n \in \mathbb{N} \text{ e } \exists \psi_1, \dots, \psi_n \in \Gamma \text{ tali che } [\varphi] \geqslant [\psi_1] \triangle \dots \triangle [\psi_n]\}. \quad (10)$$

Ricordando che per la Equazione (9) in $\mathsf{LT}_\emptyset(\mathsf{P})$ vale $[\psi] \leqslant [\varphi]$ se e soltanto se $\vdash \psi \to \varphi$ possiamo riscrivere Equazione (10) come

$$\mathcal{F}_{[\Gamma]} = \{[\varphi] \in \mathsf{LT}_\emptyset(\mathsf{P}) \mid \exists n \in \mathbb{N} \text{ e } \exists \psi_1, \dots, \psi_n \in \Gamma \text{ tali che } \vdash (\psi_1 \wedge \dots \wedge \psi_n) \to \varphi\}.$$

Poiché le derivazioni sono oggetti finiti e quindi usano un numero finito di ipotesi dire per qualche $n \in \mathbb{N}$ esistono $\psi_1, \dots, \psi_n \in \Gamma$ tali che $\vdash (\psi_1 \wedge \dots \wedge \psi_n) \to \varphi$ è equivalente a dire $\Gamma \vdash \varphi$, da cui l'asserto. $\square$

Lemma 3.100. *Sia* $\mathsf{P} \subseteq \mathsf{Var}$ *e* Γ *un insieme di formule le cui variabili proposizionali appartengono tutte a* P, *scriviamo* $[\Gamma] := \{[\gamma]_\equiv \mid \gamma \in \Gamma\}$. *Allora si ha* $\mathsf{LT}_\Gamma(\mathsf{P}) \cong \mathsf{LT}_\emptyset(\mathsf{P})/\mathcal{F}([\Gamma])$.

Dimostrazione. Si noti che gli elementi di $\mathsf{LT}_\Gamma(\mathsf{P})$ sono tutti della forma $[\varphi]_{\equiv_\Gamma}$ e quelli di $\mathsf{LT}_\emptyset(\mathsf{P})/\mathcal{F}([\Gamma])$ sono della forma $[[\varphi]_\equiv]_{\equiv_{\mathcal{F}_{[\Gamma]}}}$, per φ che varia in $\mathtt{Form}(\mathsf{P})$. Mostriamo innanzitutto che la corrispondenza che associa, per ogni variabile $\varphi \in \mathsf{Var}(\mathsf{P})$,

$$f\colon \mathsf{LT}_\Gamma(\mathsf{P}) \to \frac{\mathsf{LT}_\emptyset(\mathsf{P})}{\mathcal{F}_{([\Gamma])}} \qquad f([\varphi]_{\equiv_\Gamma}) := [[\varphi]_\equiv]_{\equiv_{\mathcal{F}_{[\Gamma]}}} \tag{11}$$

è una biezione tra $\mathsf{LT}_\Gamma(\mathsf{P})$ e $\mathsf{LT}_\emptyset(\mathsf{P})/\mathcal{F}([\Gamma])$. Infatti è ben definita e iniettiva perché

$$\begin{aligned}
[\varphi]_{\equiv_\Gamma} = [\psi]_{\equiv_\Gamma} \quad &\Leftrightarrow && \text{(per definizione di } \equiv_\Gamma) \\
\Gamma \vdash \varphi \leftrightarrow \psi \quad &\Leftrightarrow && \text{(per il Lemma 3.99)} \\
[\varphi \leftrightarrow \psi]_\equiv \in \mathcal{F}_{[\Gamma]} \quad &\Leftrightarrow && \text{(per definizione di } \equiv_{\mathcal{F}_{[\Gamma]}}) \\
[[\varphi]_\equiv]_{\equiv_{\mathcal{F}_{[\Gamma]}}} = [[\psi]_\equiv]_{\equiv_{\mathcal{F}_{[\Gamma]}}}. &
\end{aligned}$$

Inoltre la Equazione (11) è ovviamente suriettiva. Il fatto che la biezione in Equazione (11) è un omomorfismo segue banalmente da come sono definite le operazioni sulle relazioni di equivlalenza. A titolo di esempio osserviamo che $f([\varphi]_{\equiv_\Gamma} \wedge [\psi]_{\equiv_\Gamma}) = f([\varphi \wedge \psi]_{\equiv_\Gamma}) = [[\varphi \wedge \psi]_\equiv]_{\equiv_{\mathcal{F}_{[\Gamma]}}} = [[\varphi]_\equiv]_{\equiv_{\mathcal{F}_{[\Gamma]}}} \wedge [\psi]_\equiv]_{\equiv_{\mathcal{F}_{[\Gamma]}}} = f([\varphi]_{\equiv_\Gamma}) \wedge f([\psi]_{\equiv_\Gamma})$. □

Lemma 3.101. *Sia* $\mathsf{P} \subseteq \mathsf{Var}$ *e* $\Gamma \cup \{\varphi\}$ *un insieme di formule le cui variabili proposizionali appartengono tutte a* P. *Se* $\Gamma \nvdash \varphi$ *e* v *è l'interpretazione a valori in* $\mathsf{LT}_\Gamma(\mathsf{P})$ *che manda ogni variabile individuale* x_i *nella classe di equivalenza della corrispondente variabile proposizionale* $[p_i]_{\equiv_\Gamma}$ *allora si ha* $\mathsf{LT}_\Gamma(\mathsf{P}), v \models_{\mathrm{BA}} \Gamma^=$ *e* $\mathsf{LT}_\Gamma(\mathsf{P}), v \not\models_{\mathrm{BA}} \varphi^=$.

Dimostrazione. Sia v come nell'enunciato e $\psi(p_1, \ldots, p_n)$ una arbitraria formula in $\mathtt{Form}(\mathsf{P})$. Cominciamo osservando che $\tilde{v}((\psi(p_1, \ldots, p_n))^\mathsf{T}) = [\psi(v(x_1), \ldots, v(x_n))]_{\equiv_\Gamma} = [\psi(p_1, \ldots, p_n)]_{\equiv_\Gamma}$. In base al Lemma 3.100 $\mathsf{LT}_\Gamma(\mathsf{P})$ è isomorfa a $\mathsf{LT}_\emptyset(\mathsf{P})/\mathcal{F}_{[\Gamma]}$ e sotto questo isomorfismo $[\psi(p_1, \ldots, p_n)]_{\equiv_\Gamma}$ corrisponde a $[\psi(p_1, \ldots, p_n)]_\equiv]_{\equiv_{\mathcal{F}_\Gamma}}$. Ora, per l'Osservazione 3.64, gli elementi di $[[1]_\equiv]_{\equiv_{\mathcal{F}_\Gamma}}$ sono esattamente gli elementi di $\mathcal{F}_{[\Gamma]}$. Dunque si ha che $[[\gamma]_\equiv]_{\equiv_{\mathcal{F}_\Gamma}} = [[1]_\equiv]_{\equiv_{\mathcal{F}_\Gamma}}$ per ogni $\gamma \in \Gamma$ e, poiché $\Gamma \nvdash \varphi$, per il Lemma 3.99, $[[\varphi]_\equiv]_{\equiv_{\mathcal{F}_\Gamma}} \neq [[1]_\equiv]_{\equiv_{\mathcal{F}_\Gamma}}$. Ne segue che $\mathsf{LT}_\Gamma(\mathsf{P}), v \models_{\mathrm{BA}} \Gamma^=$ e $\mathsf{LT}_\Gamma(\mathsf{P}), v \not\models_{\mathrm{BA}} \varphi^=$. □

Teorema 3.102 (Completezza algebrica I)

Sia $\Gamma \cup \{\varphi\}$ *un insieme di formule proposizionali.*

$$\Gamma \vdash \varphi \textit{ se, soltanto se, } \Gamma^= \models_{\mathrm{BA}} \varphi^=.$$

Dimostrazione. $\boxed{\Rightarrow}$ Per induzione sulla lunghezza della derivazione di φ.

- Se la derivazione ha lunghezza 1, allora $\varphi \in \Gamma$, quindi banalmente $\Gamma^= \models_{\mathrm{BA}} \varphi^=$.

- Per il passo induttivo, bisogna verificare che ogni regola del calcolo $\vdash$ è valida nella teoria delle algebre di Boole. A titolo di esempio riportiamo il caso della regola (RA). Se una deduzione di lunghezza $n+1$ a partire da Γ con conclusione φ si conclude con un'applicazione della regola (RA), allora abbiamo una deduzione

$$\dfrac{\begin{array}{c}\Gamma, [\neg\varphi]^1 \\ \vdots \\ \bot\end{array}}{\varphi}\,\mathrm{RA}_1$$

Dunque sappiamo che esiste una deduzione

$$\dfrac{\begin{array}{c}\Gamma \\ \vdots \\ \end{array}}{\bot}$$

e che essa ha lunghezza n. Possiamo dunque applicare l'ipotesi induttiva e ottenere che $\Gamma^= \models_{BA} \bot^=$. Poiché $\bot^=$ corrisponde a $0 = 1$, essa vale solo nell'algebra di Boole banale composta da un solo elemento. Dunque le equazioni in $\Gamma^=$ valgono contemporaneamente solo nell'algebra banale. Supponiamo per assurdo che la tesi non valga, quindi che si abbia $\Gamma^= \not\models_{BA} \varphi^=$, in altre parole esiste un'algebra di Boole A e un'interpretazione f in A tali che $A \models_{BA} f[\Gamma^T] = 1$ e $A \models_{BA} f[\varphi^T] \neq 1$. Usando il teorema di rappresentazione di Stone (Corollario 3.87) si ottiene un insieme X tale che A è una sottalgebra del prodotto diretto $\Pi_{x \in X} A_x$ dove $A_x \cong \mathbb{2}$ per ogni $x \in X$. Poiché $f[\gamma^T] = 1$, per ogni $\gamma \in \Gamma$, ogni proiezione π_i con $i \in X$ è tale che $\pi_i(f[\gamma^T]) = 1$. Ma la composizione $\pi_i \circ f$ è un'interpretazione in $\mathbb{2}$ che rende vere tutte le equazioni in $\Gamma^=$. Poiché l'algebra $\mathbb{2}$ non è banale, abbiamo raggiunto una contraddizione e questo caso del passo induttivo è verificato. I rimanenti casi sono più semplici.

$\boxed{\Leftarrow}$ Proviamo la contronominale. Supponiamo che $\Gamma \nvdash \varphi$ e mostriamo che esiste un'algebra di Boole A e un'interpretazione e in A tale che $e[\Gamma] = 1$ e $e[\varphi] \neq 1$. Basta prendere per A l'algebra $\mathsf{LT}_\Gamma(\mathsf{Var})$ e l'interpretazione che manda ogni x_i in $[p_i]_\Gamma$. Per il Lemma 3.101 $\mathsf{LT}_\Gamma(\mathsf{Var}), e \models_{BA} \Gamma^=$ e $\mathsf{LT}_\Gamma, e \not\models_{BA} \varphi^=$, perché φ non appartiene al filtro generato da $[\Gamma]$. $\square$

Prima di vedere l'altra equivalenza nel teorema di completezza algebrica è utile approfondire il rapporto tra valutazioni e interpretazioni nelle algebre di Boole.

Lemma 3.103. *Ogni biezione* $b\colon \mathsf{Var} \to \mathtt{VarX}$ *si estende a una biezione tra valutazioni (Definizione 2.10) e interpretazioni nell'algebra* $\mathbb{2}$ *(Definizione 3.91) tale che:*

- *se* $v\colon \mathsf{Var} \to \{0, 1\}$ *è una valutazione allora per ogni formula* φ *si ha*

$$\tilde{v}(\varphi) = \widehat{v \circ b^{-1}}(\varphi^T),$$

- *se* $e\colon \texttt{VarX} \to \mathbb{2}$ *è una interpretazione allora per ogni termine* t *si ha*

$$\hat{e}(t) = \widehat{e \circ b}(t^L).$$

Dimostrazione. Dimostriamo solo il primo punto poiché il secondo è simile. Sia φ una formula in cui compaiono le variabili proposizionali $p_1, \dots, p_n$ e siano $x_1, \dots, x_n$ tali che $b(p_i) = x_i$, per $1 \leqslant i \leqslant n$.

$$\begin{aligned}\tilde{v}(\varphi(p_1, \dots, p_n)) = (\varphi^T)^{\mathbb{2}}(v(p_1), \dots, v(p_n)) = \\ = (\varphi^T)^{\mathbb{2}}(v(b^{-1}(x_1)), \dots, v(b^{-1}(x_n))) = \widehat{v \circ b^{-1}}(\varphi^T)\end{aligned}$$

□

Teorema 3.104 (Completezza algebrica II)

Sia $\Gamma \cup \{\varphi\}$ *un insieme di formule.*

$$\Gamma^{=} \models_{BA} \varphi^{=} \text{ se, soltanto se, } \Gamma \models \varphi.$$

Dimostrazione. $\boxed{\Rightarrow}$ L'ipotesi afferma che per ogni algebra di Boole A, ogni interpretazione in A che mandi tutte le i termini in Γ^T in 1, deve mandare φ^T in 1. Quindi in particolare ogni interpretazione in $\mathbb{2}$ che mandi tutti i termini Γ^T in 1, deve mandare anche φ^T in 1. Per il Lemma 3.103, questo è lo stesso che dire che ogni valutazione che mandi tutte le formule in Γ in 1 deve mandare anche φ in 1. In altre parole $\Gamma \models \varphi$.

$\boxed{\Leftarrow}$ Sia A un'algebra di Boole qualsiasi e supponiamo che $f\colon \texttt{Form} \to A$ sia un'interpretazione che manda $[\Gamma]$ in 1. Per il teorema di rappresentazione di Stone (Corollario 3.87), l'algebra A è sottalgebra del prodotto diretto di X copie di $\mathbb{2}$, per un insieme X opportuno. Quindi componendo f con ogni proiezione, otteniamo una valutazionef_i per ogni $i \in X$ con $f_i\colon \texttt{Form} \to \mathbb{2}$. Poiché $f([\Gamma]) = 1$, per ogni $i \in X$, $f_i([\Gamma]) = 1$, dunque per ipotesi, anche $f_i([\varphi]) = 1$ per ogni $i \in X$. Ma allora $f[\varphi] = 1$, cioè: l'interpretazione f in A, manda φ in 1. Poiché sia f che A sono arbitrarie, abbiamo stabilito che $\Gamma^{=} \models_{BA} \varphi^{=}$. □

Si noti che è possibile dimostrare anche degli analoghi dei Teoremi 3.102 e 3.104 riguardanti le equazioni nel linguaggio delle algebre di Boole. In altre parole, vale il seguente risultato.

Proposizione 3.105. *Sia* $\Lambda \cup \{s \approx t\}$ *un insieme di equazioni nel linguaggio delle algebre di Boole. Allora valgono:*

$$\Lambda \models_{BA} s \approx t \text{ se, soltanto se, } \Lambda^{\leftrightarrow} \models (s \approx t)^{\leftrightarrow}.$$

e

$$\Lambda \models_{BA} s \approx t \text{ se, soltanto se, } \Lambda^{\leftrightarrow} \vdash (s \approx t)^{\leftrightarrow}.$$

La dimostrazione è lasciata per esercizio al lettore.

3.5 COMPLEMENTI: ALGEBRE DI BOOLE ATOMICHE

Si consideri l'algebra di Boole $\wp(X)$, dove X è un insieme finito. Si osserva facilmente che ci sono degli elementi, i singoletti degli elementi di X, che sono *immediatamente sopra* $\emptyset$ e, per ogni altro $A \in \wp(X)$, A è unione dei singoletti che lo compongono. Generalizzando a un algebra qualsiasi, si ottiene la seguente definizione.

Definizione 3.106

Sia B un'algebra di Boole. Un elemento $a \in B$, $a \neq 0$, si dice **atomo** di B se per ogni $y \in B$ tale che $0 \leqslant y \leqslant a$ si ha $y = a$ oppure $y = 0$. Nel seguito $\mathcal{A}(B)$ denoterà l'insieme degli atomi di B.

L'algebra B si dice **atomica** se per ogni $y \in B$, $y \neq 0$, esiste $a \in \mathcal{A}(B)$ tale che $a \leqslant y$.

Esempio 3.107. Ogni insieme delle parti di un insieme è un'algebra atomica e ogni algebra di Boole finita è atomica. Ci sono però algebre che hanno atomi ma non sono atomiche, ci sono algebra senza atomi.

Proposizione 3.108. *Sia* B *un'algebra di Boole e sia* $a \in B$, $a \neq 0$. *Sono equivalenti:*

1. $a \in \mathcal{A}(B)$;
2. *Per ogni* $y \in B$, $a \wedge y = 0$ *oppure* $a \wedge y = a$;
3. *Il filtro generato da* a, F_a, *è un ultrafiltro;*
4. *Esiste un unico ultrafiltro che contiene* a.

Dimostrazione. 1 $\Rightarrow$ 2. Segue dalla definizione di atomo, poiché per ogni $y \in B$ si ha $0 \leqslant y \wedge a \leqslant a$.

2 $\Rightarrow$ 3. Poiché $a \neq 0$, si ha che F_a è proprio ed ha la FIP. Resta da verificare che F_a è completo: sia $x \notin F_a$, siccome $x \geqslant a \wedge x$, segue che $x \wedge a \neq a$, altrimenti $x \in F_a$. Di conseguenza, $x \wedge a = 0$, che implica $a \wedge \neg\neg x = 0$ e $a \leqslant \neg x$, da cui segue $\neg x \in F_a$.

3 $\Rightarrow$ 4. Sia $U \in \mathcal{U}(B)$ tale che $a \in U$. Segue che $F_a \subseteq U$, e per l'ipotesi $F_a = U$.

4 $\Rightarrow$ 1. Sia, per assurdo, $y \in B$ tale che $0 < y < a$. I filtri generati da y e da $a \wedge \neg y$ sono entrambi propri, infatti $y \neq 0$ per ipotesi, mentre $a \wedge \neg y \neq 0$ deriva dal fatto che $y < a$. Per dimostrare quest'ultimo fatto basta notare che se $a \wedge \neg y$ fosse uguale a 0 allora per il Lemma 3.34, $a \leqslant y$ e ciò contraddice $y < a$. Quindi per il Corollario 3.84 esistono $U, V \in \mathcal{U}(B)$ tali che $F_{\{a \wedge \neg y\}} \subseteq U$ e $F_y \subseteq V$. Poiché a appartiene ad entrambi gli ultrafiltri, dall'ipotesi ipotesi si ha $V = U$. Ma $y \in V$ e $\neg y \in U$, dunque $0 = y \wedge \neg y \in U = V$. Tale contraddizione deriva dall'aver supposto l'esistenza di un tale y, dunque a è un atomo. □

Il seguente risultato caratterizza le algebra di Boole atomiche.

Proposizione 3.109. *Un'algebra di Boole* B *è atomica se, e solo se,* $\sup(\mathcal{A}(B)) = 1$.

Dimostrazione. Sia B atomica e sia $z = \sup(\mathcal{A}(B)) \neq 1$. Di conseguenza, $\neg z \neq 0$ e per ipotesi esiste $a \in \mathcal{A}(B)$ tale che $a \leqslant \neg z$, e quindi $a \wedge \neg z = a$. Ma $a \leqslant \sup(\mathcal{A}(B)) = z$ implica $a = a \wedge \neg z = 0$, un assurdo.

Viceversa, sia $y \in B$ tale che $a \nleqslant y$ per ogni $a \in \mathcal{A}(B)$. Allora $a \neq y \wedge a$ implica $y \wedge a =$o e $a \leqslant \neg y$. Quindi $1 = \sup(\mathcal{A}(B)) \leqslant \neg y$ e $\neg y = 1$, che implica $y = 0$. □

Nei seguenti risultati il risultato viene ristretto al caso delle algebre finite.

Proposizione 3.110. *Sia* B *un'algebra di Boole finita. Sia* $A_x = \{a \in \mathcal{A}(B) \mid a \leqslant x\}$. *Allora* x *si scrive in maniera univoca come* $\sup(A_x)$.

Dimostrazione. Poiché B è finita, allora è atomica e $\sup(\mathcal{A}(B)) = 1$ e siano $a_1, \dots, a_n$ gli atomi di B. Si ha $x = x \wedge 1 = x \wedge (a_1 \vee \dots \vee a_n) = (x \wedge a_1) \vee \dots (x \wedge a_n)$. Per ogni $i = 1, \dots, n$ si ha che $0 \leqslant a_i \wedge x \leqslant a_i$. Quindi $a_i \wedge x = a_i$ oppure $a_i \wedge x = 0$. Nel primo caso si ha $a_i \leqslant x$. Siano $a_{i_1}, \dots, a_{i_k}$ gli atomi minori o uguali a x. Segue che $x = a_{i_1} \vee \dots \vee a_{i_k}$.

Sia $x = a_{j_1} \vee \dots \vee a_{j_l}$ con $\{a_{j_1}, \dots, a_{j_l}\} \neq \{a_{i_1}, \dots, a_{i_k}\}$. Esiste quindi almeno un indice j_t tale che $a_{j_t} \notin \{a_{i_1}, \dots, a_{i_k}\}$. Di conseguenza $a_{j_t} \wedge (a_{j_1} \vee \dots \vee a_{j_l}) = a_{j_t} \wedge (a_{i_1} \vee \dots \vee a_{i_k})$. Ancora per la Proposizione 3.108, atomi distinti hanno 0 come infimo. Di conseguenza, per la proprietà distributiva, il primo membro sarà proprio uguale a a_{j_t}, mentre il secondo a 0. Segue l'unicità della rappresentazione. □

Proposizione 3.111. *Sia* $\mathcal{B}$ *una algebra di Boole finita e sia* $|\mathcal{A}(B)| = n$. *Allora* B *è atomica,* B *è isomorfa a* $\wp(\mathcal{A}(B))$ *e* $|B| = 2^n$.

Dimostrazione. Il fatto che B sia atomica segue dalla sua finitezza. Sia $e : B \to \wp(\mathcal{A}(B))$ la mappa definita come segue

$$e \colon y \in B \mapsto \{a \in \mathcal{A}(B) \mid a \leqslant y\}.$$

Dalla Proposizione 3.110, se $e(x) = \{a_{i_1}, \dots, a_{i_k}\}$, si ha $\sup(e(x)) = a_{i_1} \vee \dots \vee a_{i_k} = x$.

La mappa e è iniettiva: infatti, siano $x, y \in B$ tali che $e(x) = e(y) = \{a_{i_1}, \dots a_{i_k}\}$. Segue che $\sup(e(x)) = \sup(e(y))$ e di conseguenza $x = y$.

La mappa e è suriettiva: per ogni $A \in \wp(\mathcal{A}(B))$, $A \subseteq B$ e $e(\sup(A)) = A$.

Resta da vedere che e è omomorfismo di algebre di Boole. Siano $C = \{a_{i_1}, \dots, a_{i_k}\}$ con $x = a_{i_1} \vee \dots \vee a_{i_k}$ e $D = \{b_{j_1}, \dots, b_{j_l}\}$ con $y = b_{j_1} \vee \dots \vee b_{j_l}$. Allora $e(x \vee y) = e((a_{i_1} \vee \dots \vee a_{i_k}) \vee (b_{j_1} \vee \dots \vee b_{j_l})) = \{a_{i_1}, \dots, a_{i_k}, b_{j_1}, \dots, b_{j_l}\} = C \cup D = e(x) \cup e(y)$.

Siano $C = \{a_{i_1}, \dots, a_{i_k}\}$ con $x = a_{i_1} \vee \dots \vee a_{i_k}$ e $C^c = \{b_{j_1}, \dots, b_{j_l}\}$. Vediamo che $\sup(C^c) = \neg x$. Sia $z = b_{j_1} \vee \dots \vee b_{j_l}$. Usando le proprietà distributiva e associativa si vede facilmente che $x \vee z = (a_{i_1} \vee \dots \vee a_{i_k}) \vee (b_{j_1} \vee \dots \vee b_{j_l}) = 1$ e $x \wedge z = (a_{i_1} \vee \dots \vee a_{i_k}) \wedge (b_{j_1} \vee \dots \vee b_{j_l}) = 0$. Quindi $z = \neg x$ e $e(\neg x) = e(x)^c$.

Inoltre, $e(1) = e(\sup(\mathcal{A}(B)) = \mathcal{A}(B)$ e $e(0) = \{a \in \mathcal{A}(B) \mid a \leqslant 0\} = \emptyset$. Infine, per le leggi di De Morgan, segue che $e(x \wedge y) = e(e) \cap e(y)$ ed e è omomorfismo di algebre di Boole. □

Corollario 3.112. *Tutte le algebre di Boole di una fissata cardinalità finita* $n \in \mathbb{N}$ *sono isomorfe. Inoltre,* n *è necessariamente una potenza di* 2*.*

Dimostrazione. Siano B_1 e B_2 due algebre di Boole di cardinalità finita $n \in \mathbb{N}$ fissata. Per il Proposizione 3.111 si ha che $B_1 \simeq \wp(\mathcal{A}(B_1))$ e $B_2 \simeq \wp(\mathcal{A}(B_2))$. Di conseguenza $n = 2^{|\mathcal{A}(B_1)|} = 2^{|\mathcal{A}(B_2)|}$ e la tesi segue banalmente. □

4 SINTASSI E SEMANTICA DELLA LOGICA DEL PRIMO ORDINE.

"Anyone can prove true theorems"
William Feller (1906-1970)

Il calcolo proposizionale che abbiamo presentato è poco espressivo. Manca la possibilità di esprimere che una certa proprietà P vale per tutti gli elementi di un certo insieme, oppure che esiste almeno un elemento che gode della proprietà P. Se x e y sono elementi di un dato insieme, scriveremo $P(x)$ per indicare che la proprietà P vale per l'elemento x o $R(x, y)$ per indicare che l'elemento x è in relazione R con l'elemento y. Ad esempio, $P(x)$ potrebbe essere l'asserzione seguente: "x è rosso," dove x denota un qualsiasi oggetto, oppure la relazione $R(x, y)$ potrebbe indicare che x è più vecchio di y, dove x e y sono elementi nell'insieme degli esseri umani. Grazie a questo linguaggio più espressivo, possiamo ora studiare ragionamenti come il seguente, che non sono affrontabili con la logica proposizionale.

$$\frac{\begin{array}{l}\text{Anna è moglie di Nicola,}\\ \text{Se una qualsiasi persona è moglie di un qualsiasi altro,}\\ \text{allora quell'altro è marito di questa persona,}\end{array}}{\text{Nicola è marito di Anna.}}$$

Con la nostra nuova notazione potremmo indicare con $R(x, y)$ che x è marito di y e con $Q(x, y)$ che x è moglie di y, dunque avremmo:

$$\frac{\begin{array}{c}\text{Q(Anna, Nicola),}\\ Q(x, y) \to R(y, x)\end{array}}{\text{R(Nicola, Anna).}}$$

La struttura logica del ragionamento comincia a diventare più evidente. Quello che ancora manca è il poter esprimere la parola *qualsiasi* del ragionamento iniziale. Introdurremo due nuovi simboli, che indicheremo con $\forall$ e $\exists$, a cui attribuiremo i seguenti significati:

1. $\forall x \varphi(x)$ servirà ad indicare che la proprietà φ vale per ogni elemento x (di un qualche insieme prefissato),
2. $\exists x \varphi(x)$ servirà ad indicare che la proprietà φ vale per qualche x, cioè che esiste almeno un elemento x per cui $\varphi(x)$ è vera.

I due simboli $\forall$ e $\exists$ si chiamano, rispettivamente, **quantificatore universale** e **quantificatore esistenziale**. Si tratterà quindi di estendere il linguaggio del calcolo proposizionale aggiungendo questi due nuovi simboli, assieme a tutta una serie di altri "oggetti" di cui avremo bisogno.

4.1 IL LINGUAGGIO DEL CALCOLO DEI PREDICATI

Definiamo ora l'alfabeto che ci servirà a creare espressioni logiche del tipo visto sopra. A differenza della logica proposizionale, il linguaggio non è totalmente fissato all'inizio, ma è composto da un insieme di simboli fissati e uno variabile. I simboli che appartengono sempre al linguaggio del prim'ordine sono i seguenti:

1. un insieme infinito di simboli di variabile:

$$\texttt{VarX} = \{x, x_1, x_2, x_3, \ldots y, y_1, y_2, x_3, z, \ldots\};$$

2. i connettivi proposizionali: $\neg, \wedge, \vee, \rightarrow, \perp$;
3. i simboli per i quantificatori: $\forall, \exists$;
4. i simboli ausiliari: le parentesi.

I simboli che possono variare a seconda del contesto sono quelli della seguente definizione.

Definizione 4.1

Un **linguaggio del primo ordine** è un insieme $\mathcal{L}$ composto da:

5. un insieme (anche vuoto) di **simboli di costante**: $\{c_1, c_2, c_3 \ldots\}$;
6. un insieme (anche vuoto) di **simboli di predicato** (detti anche **simboli relazione**): $\{P_1, P_2, P_3, \ldots\}$;
7. un insieme (anche vuoto) di **simboli di funzione**: $\{f_1, f_2, f_3, \ldots\}$;
8. una funzione a che assegna a ogni simbolo di predicato e di funzione un numero naturale, detta **arietà** del simbolo.

L'arietà dei simboli di predicato sta a indicare il corretto numero di argomenti da associare ad ogni predicato. I predicati a due argomenti sono detti binari, ma possono esserci predicati che richiedono un solo argomento o altri che ne richiedono più di due. Ad esempio, nella frase "5 è un numero primo", il predicato "essere un numero primo" ha un solo argomento, il numero 5; nella frase "8 è compreso tra 6 e 12", il predicato "essere compreso" ha tre argomenti: i numeri 8, 6, 12. L'arietà permetterà più avanti di definire i termini e le formule ben formate. Inoltre nella valutazione semantica, ogni simbolo di predicato P tale che $a(P) = m$ sarà associato a un predicato con m argomenti. Similmente, ogni simbolo di funzione f tale che $a(f) = n$ sarà associato a una funzione n-aria.

Osservazione 4.2. Data l'importanza dell'uguaglianza in matematica, considereremo il simbolo $=$ presente in ogni linguaggio e lo interpreteremo sempre nell'uguaglianza tra elementi.

A differenza della logica proposizionale, in questo linguaggio abbiamo due tipi di costrutti: quelli che rappresentano individui, che chiameremo termini e quelli che rappresentano asserzioni su questi individui, che chiameremo formule.

Cominciamo con il definire i termini del linguaggio, la seguente definizione si specializza, nel caso in cui $\mathcal{L}$ sia il linguaggio delle algebre di Boole, alla Definizione 3.88

Definizione 4.3

Sia $\mathcal{L}$ un linguaggio del prim'ordine, definiamo l'insieme $\mathtt{Term}_{\mathcal{L}}$ dei **termini** nel linguaggio $\mathcal{L}$ come il più piccolo insieme chiuso rispetto alle seguenti regole:

- ogni elemento di $\mathtt{VarX}$ appartiene a $\mathtt{Term}$,
- se c è un simbolo di costante in $\mathcal{L}$ allora $c \in \mathtt{Term}$,
- se f è un simbolo di funzione in $\mathcal{L}$ tale che $a(f) = n$ e $t_1, \dots, t_n \in \mathtt{Term}$, allora anche $f(t_1, \dots, t_n) \in \mathtt{Term}$.

Scriveremo $t(x_1, \dots, x_n)$ per evidenziare il fatto che le variabili individuali in t sono *comprese* tra le variabili $x_1, \dots, x_n$.

Definizione 4.4

Sia $\mathcal{L}$ un linguaggio del prim'ordine, definiamo l'insieme $\mathtt{Form}\forall_{\mathcal{L}}$ delle **formule ben formate** (del prim'ordine, nel linguaggio $\mathcal{L}$) come il più piccolo insieme chiuso rispetto alle seguenti regole:

1. se $t_1, t_2, \dots, t_n \in \mathtt{Term}_{\mathcal{L}}$ e P è un simbolo di predicato in $\mathcal{L}$ tale che $a(P) = n$, allora $P(t_1, \dots, t_n) \in \mathtt{Form}\forall$ (tale formula è detta **formula atomica**).
2. se $\varphi_1, \varphi_2 \in \mathtt{Form}\forall$ allora
   a) $(\neg\varphi_1) \in \mathtt{Form}\forall$;
   b) $(\varphi_1 \wedge \varphi_2) \in \mathtt{Form}\forall$;
   c) $\exists x(\varphi_1) \in \mathtt{Form}\forall$ con $x \in \mathtt{VarX}$.

Notazione 4.5. Come per la logica proposizionale definiremo gli altri connettivi come le seguenti abbreviazioni:

$$\varphi \vee \psi := \neg(\neg\varphi \wedge \neg\psi), \qquad \varphi \to \psi := \neg\varphi \vee \psi$$
$$\varphi \leftrightarrow \psi := (\varphi \to \psi) \wedge (\psi \to \varphi), \qquad \forall x(\varphi) := \neg\exists x(\neg\varphi).$$

Esempio 4.6. Se il linguaggio $\mathcal{L}$ ha due simboli di relazione binari P ed R, un simbolo di funzione binario f e una costante c allora le seguenti sono in $\mathtt{Form}\forall_{\mathcal{L}}$:

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

$$(\forall x(\exists y(R(x,f(c,y)) \vee Q(y,c))))$$

Al contrario, la seguente sequenza di simboli non è in $\mathtt{Form}\forall$:

$$\forall x \exists \to (\wedge Q \forall$$

Notazione 4.7. Le regole che abbiamo stabilito conducono a un uso eccessivo delle parentesi. Come nel calcolo proposizionale, conviene dunque stabilire delle priorità tra i vari simboli:

priorità più alta	$\forall, \exists,$
	$\neg,$
	$\wedge,$
	$\vee,$
priorità più bassa	$\to .$

La generica formula

$$(\forall x(\varphi(x) \to ((\exists y \psi(x,y)) \vee (\neg\varphi(x)))))$$

si potrà dunque scrivere come segue:

$$\forall x(\varphi(x) \to \exists y \psi(x,y) \vee \neg\varphi(x)) .$$

Notazione 4.8. D'ora in avanti supporremo, salvo se diversamente specificato, che $\mathcal{L}$ sia un linguaggio del prim'ordine fissato e arbitrario. Dunque per alleggerire la notazione scriveremo solo $\mathtt{Term}$ per $\mathtt{Term}_{\mathcal{L}}$ e $\mathtt{Form}\forall$ per $\mathtt{Form}\forall_{\mathcal{L}}$.

Diversamente dalla logica proposizionale, nel primo ordine non è sempre possibile assegnare un valore di verità a una formula ben formata. Questo non è un limite del nostro sistema formale, cose del genere succedono anche nel linguaggio quotidiano, infatti finché tutti i termini delle espressione non sono stati univocamente determinati, in generale non è possibile asserire niente sul valore di verità della frase. Le frasi

"il numero naturale x è il doppio di 7"

"il signor x è il Preside dell'Istituto"

sono esempi di frasi ben formate, di cui però non possiamo stabilire se siano vere o false. Dipende, infatti, da ciò che la variabile x rappresenta. In questi casi, parliamo di formule aperte. In altre parole, una variabile si dice *libera* in una formula φ quando non è sottoposta a nessuna quantificazione all'interno della formula φ, mentre una variabile quantificata si dice *legata* (o *vincolata*). Diamo ora una definizione più formale.

Definizione 4.9

Per ogni termine $t \in \texttt{Term}$ definiamo per ricorsione l'insieme delle sue **variabili libere** $\texttt{FV}(t)$:

- se $t \in \texttt{VarX}$ allora $\texttt{FV}(t) = \{t\}$,
- se t è una costante allora $\texttt{FV}(t) = \emptyset$,
- se $t = f(t_1, \dots, t_n)$ allora $\texttt{FV}(t) = \texttt{FV}(t_1) \cup \dots \cup \texttt{FV}(t_n)$.

Per ogni formula $\varphi \in \texttt{Form}\forall$ definiamo per ricorsione l'insieme delle sue variabili libere $\texttt{FV}(\varphi)$.

1. se $\varphi = P(t_1, \dots, t_n)$ allora $\texttt{FV}(\varphi) = \texttt{FV}(t_1) \cup \dots \cup \texttt{FV}(t_n)$,
2. se $\varphi = (\neg\varphi_1)$ allora $\texttt{FV}(\varphi) = \texttt{FV}(\varphi_1)$;
3. se $\varphi = (\varphi_1 \wedge \varphi_2)$ allora $\texttt{FV}(\varphi) = \texttt{FV}(\varphi_1) \cup \texttt{FV}(\varphi_2)$;
4. se $\varphi = \exists x(\varphi_1)$ allora $\texttt{FV}(\varphi) = \texttt{FV}(\varphi_1) \setminus \{x\}$;

L'unico passaggio a cui fare particolare attenzione nella precedente definizione è quello dei quantificatori. Come per i termini, scriveremo $\varphi(x_1, ..., x_n)$ per evidenziare il fatto che le variabili libere in φ sono *comprese* tra le variabili $x_1, \dots, x_n$.

Definizione 4.10

Una formula ben formata φ è detta **aperta** se essa contiene almeno una variabile libera ($\texttt{FV}(\varphi) \neq \emptyset$). In caso contrario essa è detta **enunciato** (o **formula chiusa**). Le variabili che occorrono in φ, ma non appartengono a $\texttt{FV}(\varphi)$ si dicono **vincolate**.

Definizione 4.11

Siano t, s due termini e x una variabile. Il termine $s[t/x]$ ottenuto da s con una **sostituzione** di tutte le occorrenze di x con t è definito ricorsivamente come segue:

1. se $s \in \texttt{VarX}$ allora $s[t/x] = \begin{cases} s \text{ se } s \neq x \\ t \text{ se } s = x \end{cases}$;
2. se s è un simbolo di costante allora $s[t/x] = s$;
3. se $s = f(s_1, \dots, s_n)$ allora $s[t/x] = f(s_1[t/x], \dots, s_n[t/x])$;

Ora che è chiaro come operare una sostituzione in un termine, si può definire cosa si intende per una sostituzione all'interno di una formula.

Definizione 4.12

Siano φ una formula, t un termine e x una variabile. La formula $\varphi[t/x]$ è definita ricorsivamente come segue:

1. se $\varphi = P(t_1, \dots, t_n)$, allora $P(t_1, \dots, t_n)[t/x] = P(t_1[t/x], \dots, t_n[t/x])$;
2. se $\varphi = \varphi_1 \wedge \varphi_2$ allora $(\varphi_1 \wedge \varphi_2)[t/x] = (\varphi_1[t/x] \wedge \varphi_2[t/x])$;
3. se $\varphi = (\neg\varphi_1)$ allora $\varphi[t/x] = \neg(\varphi_1[t/x])$;
4. se $\varphi = \exists y(\varphi_1)$ allora

$$\exists y(\varphi_1)[t/x] = \begin{cases} \exists y(\varphi_1[t/x]) & \text{se } x \neq y, \\ \exists y(\varphi_1) & \text{se } x = y, \end{cases}$$

Notazione 4.13. Quando la sostituzione è chiara dal contesto cercheremo di alleggerire la notazione. Quindi, se $\varphi(x)$ è una formula scriveremo $\varphi(t)$ per $\varphi(x)[t/x]$.

Dal punto di vista sintattico l'unica attenzione che bisogna prestare, dopo aver posto la Definizione 4.12, è che il risultato sia ancora una formula ben formata. Questa verifica è immediata. Quando però daremo *significato* alle stringhe di simboli chiamate formule, dovremo fare attenzione che queste sostituzioni non stravolgano tale significato. Anticipiamo a ancora una volta a livello intuitivo il significato delle formule e consideriamo il seguente esempio:

Esempio 4.14. Consideriamo la formula $\varphi = \exists y(x < y)$, in cui x compare come variabile libera e y come variabile legata. Se consideriamo il termine $t = z$, in cui non compare la variabile y, non incontriamo nessun problema: la formula ottenuta sostituendo z ad x, che indicheremo con $\varphi[z/x]$, è $\exists y(z < y)$ ed esprime la stessa asserzione della formula φ. Al contrario, se consideriamo il termine $t = y$, in cui compare proprio la y come variabile libera, si ottiene la formula $\varphi[y/x] = \exists y(y < y)$, la quale ha un significato logico diverso: è sempre falsa.

Il problema presentato nell'Esempio 4.14 può essere risolto in due maniere praticamente equivalenti. La prima, che è quella che utilizzeremo in seguito, è non permettere sostituzioni del tipo $\varphi[t/x]$ in cui le variabili di t vengono vincolate dai quantificatori di φ dopo la sostituzione.

Definizione 4.15

Diremo che un temine t è **sostituibile** per x in φ se le variabili di t non diventano vincolate all'interno di φ dopo la sostituzione.

I seguito assumeremo sempre (a volte tacitamente) che t sia sostituibile per x in φ quando operiamo la sostituzione $\varphi[t/x]$.

Un metodo alternativo per evitare il problema dell'Esempio 4.14 sfrutta una proprietà che dimostreremo in seguito, cioè che *rinominare le variabili vincolate non cambia il significato di una formula*. Dunque è possibile evitare il problema della cattura delle variabili di t nella sostituzione $\varphi[t/x]$ ridefinendo il passo $\exists$ nella Definizione 4.12 come segue

$$\exists y(\varphi)[t/x] = \begin{cases} \exists y(\varphi[t/x]) & \text{se } x \neq y \text{ e } y \notin \mathtt{FV}(t), \\ \exists w(\varphi[w/y][t/x]) & \text{se } x \neq y \text{ e } y \in \mathtt{FV}(t), \\ \exists y(\varphi) & \text{se } x = y, \end{cases}$$

dove w è una variabile *nuova*, cioè che non compare né in φ né in t. La seconda soluzione prevede dunque di rinominare opportunamente la variabile legata y all'interno della formula φ prima di operare la sostituzione del termine t al posto della variabile x. In questo modo nell'Esempio 4.14 si avrebbe:

$$\begin{aligned} \varphi[y/x] =& (\exists y(x < y))[z/y][y/x] = \\ =& (\exists z(x < z))[y/x] = \\ =& (\exists z(y < z)) \,, \end{aligned}$$

la quale ha, intuitivamente, lo stesso significato della formula φ.

Il seguente lemma illustra le condizioni in cui si possono scambiare sostituzioni consecutive senza cambiare il risultato finale.

Lemma 4.16. *Siano* $r, s, t \in \mathtt{Term}$ *e supponiamo che* x *e* y *siano variabili distinte tali che* $x \notin \mathtt{FV}[r]$, *allora valgono le seguenti uguaglianze.*

1.
$$(t[s/x])[r/y] = (t[r/y])[s[r/y]/x].$$

2. Se r *ed* s *sono sostituibili per* x *e* y *rispettivamente in* φ, *allora*
$$(\varphi[s/x])[r/y] = (\varphi[r/y])[s[r/y]/x].$$

Dimostrazione. Punto 1. Per induzione su t.

- Se $t = c$ allora le sostituzioni non hanno effetto, quindi l'asserto vale banalmente.
- Se $t \in \mathtt{VarX}$ e $t \neq x, y$ allora nuovamente le sostituzioni non hanno effetto.
- Se $t = x$ allora da un lato si ha $(t[s/x])[r/y] = s[r/y]$ e dall'altro $(t[r/y])[s[r/y]/x] = x[s[r/y]/x] = s[r/y]$. Quindi l'asserto è vero.
- Se $t = y$ allora da un lato si ha $(t[s/x])[r/y] = t[r/y] = r$ mentre dall'altro lato si ha $(t[r/y])[s[r/y]/x] = r[s[r/y]/x] = r$, dove l'ultima uguaglianza vale perché per ipotesi $x \notin \mathtt{FV}(r)$. Quindi l'asserto è vero anche in questo caso.

- Infine, se $t = f(t_1, \dots, t_n)$ allora

$$
\begin{aligned}
&(t[s/x])[r/y] = \\
&\quad = f((t_1[s/x])[r/y], \dots, (t_n[s/x])[r/y] && \text{per la def. di sost.} \\
&\quad = f(t_1[r/y])[s[r/y]/x], \dots, (t_n[r/y])[s[r/y]/x]) && \text{per ip. induttiva} \\
&\quad = f(t_1, \dots, t_n)[r/y][s[r/y]/x] = (t[r/y])[s[r/y]/x] && \text{per la def. di sost.}
\end{aligned}
$$

La dimostrazione del Punto 2 è simile.

□

Corollario 4.17. *Sia* $t \in \mathtt{Term}$. *Se* $y \notin \mathtt{FV}(t)$ *allora* $t[c/x] = (t[y/x])[c/y]$. *Similmente, se* $\varphi \in \mathtt{Form}\forall$, $y \notin \mathtt{FV}(\varphi)$ *e* y *è sostituibile per* x *in* φ, *allora* $\varphi[c/x] = (\varphi[y/x])[c/y]$.

4.2 LA SEMANTICA DELLA LOGICA DEL PRIM'ORDINE

Ci poniamo ora il problema di attribuire un significato a tutte le formule ben formate di un dato linguaggio del prim'ordine. Se nel caso del Calcolo Proposizionale ciò era piuttosto facile (ricordiamo che si trattava solo di stabilire le tavole di verità dei connettivi proposizionali), nel caso del Calcolo dei Predicati (al primo ordine) l'attribuzione di un valore di verità a una formula ben formata risulta complicata a causa della presenza di costanti, variabili, ecc.

Innanzitutto dovremo fissare un dominio, cioè un insieme A, nel quale assumeranno i loro valori i simboli di costante e i simboli di variabile. Poi ad ogni simbolo di predicato P, con $a(P) = n$ dovremo far corrispondere una relazione n-aria sull'insieme A, cioè una funzione definita su A^n a valori nell'insieme $\{0, 1\}$ (vero o falso). Cominciamo quindi con il dare la seguente definizione.

Definizione 4.18

Dato un linguaggio del prim'ordine $\mathcal{L}$, una **struttura** del prim'ordine A per $\mathcal{L}$ è data da un insieme non vuoto A, detto **dominio** (o **supporto** della struttura) e da un assegnamento che associa:

1. a ogni simbolo di costante c in $\mathcal{L}$ un elemento $c^A \in A$;
2. a ogni simbolo di predicato Q in $\mathcal{L}$, tale che $a(Q) = n$, una relazione n-aria $Q^A \colon A^n \to \{0, 1\}$ o in altre parole, un sottoinsieme $Q^A \subseteq A^n$.
3. a ogni simbolo di funzione f in $\mathcal{L}$, tale che $a(f) = m$, una funzione m-aria $f^A \colon A^m \to A$.

In generale, non è possibile assegnare un valore di verità a una formula che contenga delle variabili libere; sarà prima necessario assegnare a tali variabili degli elementi del dominio. Di conseguenza il valore di verità di una formula dipenderà, in generale, dalla specifica interpretazione scelta. Diamo dunque la seguente definizione:

Definizione 4.19

Data una struttura A con dominio A, chiameremo **interpretazione** in A una qualunque funzione $v\colon \mathtt{VarX} \to A$.

Con un leggero abuso di notazione, è possibile estendere la definizione di sostituzione anche alle interpretazioni. Se v è un'interpretazione in A e $a \in A$, indicheremo con $v[a/x]$ l'interpretazione v modificata in modo da associare alla variabile x l'elemento a. Più precisamente, si ha:

$$v[a/x](y) = \begin{cases} v(y) & \text{se } y \neq x \\ a & \text{se } y = x \end{cases}$$

Definiamo ora il valore di un termine sotto una data interpretazione:

Definizione 4.20

Data un'interpretazione v definiamo $\tilde{v}$ come l'estensione di v a tutto l'insieme dei termini $Term$ come segue: se t è un qualsiasi termine allora

1. se $t = x$ per qualche variabile x, si ha $\tilde{v}(t) = v(x)$;
2. se $t = c$ per qualche costante c, si ha $\tilde{v}(t) = c^A$;
3. se $t = f(t_1, \ldots, t_n)$, si ha $\tilde{v}(t) = f^A(\tilde{v}(t_1), \ldots, \tilde{v}(t_n))$.

È immediato verificare che una tale estensione è unica.

Possiamo ora definire formalmente il valore di verità di una formula ben formata φ sotto l'interpretazione v. Indicheremo con il simbolo $A, v \models \varphi$ che la formula φ è valida in A sotto l'interpretazione v.

Definizione 4.21

[**Semantica del prim'ordine**] Sia φ una formula nel linguaggio $\mathcal{L}$, A una struttura per il linguaggio $\mathcal{L}$ e v un'interpretazione in A. La relazione $A, v \models \varphi$ è definita ricorsivamente come segue:

1. $A, v \models P(t_1, \ldots, t_n)$ vale se, e soltanto se, $P^A(v(t_1), \ldots, v(t_n))$ è vera in A;
2. $A, v \models (\neg\varphi)$ se, e soltanto se, $A, v \not\models \varphi$ (cioè non vale che $A, v \models \varphi$);
3. $A, v \models (\varphi \wedge \psi)$ se, e soltanto se, $A, v \models \varphi$ e $A, v \models \psi$;

4. $A, v \models (\exists x \varphi)$ se, e soltanto se, esiste un a in A tale che $A, v[a/x] \models \varphi$.

Se $A, v \models \varphi$, diremo che la formula φ è **valida sotto l'interpretazione v** in A. Diremo semplicemente che la formula φ è **valida** in A se per ogni interpretazione v in A si ha $A, v \models \varphi$. In questo caso scriveremo $A \models \varphi$ e diremo che A è un **modello** di φ.

Si noti che le definizioni date ai Punti 2 e 3 della semantica di $\neg$ e $\wedge$, sono equivalenti a quelle date nel Calcolo Proposizionale mediante l'uso delle tavole di verità. Osserviamo inoltre che ha senso definire $A, v \models \varphi$ solo nel caso in cui φ è una formula nel linguaggio $\mathcal{L}$, A è una struttura per lo stesso linguaggio $\mathcal{L}$ e v è una interpretazione a valori in A. Nel seguito assumeremo che sia così ogni volta che scriveremo $A, v \models \varphi$.

Esempio 4.22. Si consideri la formula

$$\exists x\,(P(x) \wedge \neg P(x))\,.$$

Stabiliamo se la formula è vera o falsa nella struttura

$$A = \mathbb{N}, \quad P^A(n) \Leftrightarrow n \text{ è pari}$$

sotto l'interpretazione

$$v(x) = 1.$$

$$\begin{array}{lll}
\mathbb{N}, v \models (\exists x P(x) \wedge \neg P(x)) & & \text{sse} \\
\text{Esiste } n \in \mathbb{N} \text{ tale che} & \mathbb{N}, v[n/x] \models P(x) \wedge \neg P(x) & \text{sse} \\
\text{Esiste } n \in \mathbb{N} \text{ tale che} & \mathbb{N}, v[n/x] \models P(x) \text{ e } \mathbb{N}, v[n/x] \models \neg P(x) & \text{sse} \\
\text{Esiste } n \in \mathbb{N} \text{ tale che} & P^A(v[n/x](x)) \text{ e } \mathbb{N}, v[n/x] \not\models P(x) & \text{sse} \\
\text{Esiste } n \in \mathbb{N} \text{ tale che} & P^A(n) \text{ e non } P(v[n/x](x)) & \text{sse} \\
\multicolumn{2}{l}{\text{Esiste } n \in \mathbb{N} \text{ tale che } n \text{ è pari e non } P(n)} & \text{sse} \\
\multicolumn{2}{l}{\text{Esiste } n \in \mathbb{N} \text{ tale che } n \text{ è pari e } n \text{ non è pari.}} &
\end{array}$$

La formula è quindi falsa, perché non esiste nessun numero naturale che è contemporaneamente pari e non pari.

A volte può essere utile dare direttamente la semantica dei connettivi $\rightarrow$, $\wedge$ e $\leftrightarrow$, invece che ridursi a $\wedge$, $\neg$ e $\exists$.

Lemma 4.23. *Sia φ una formula, A una struttura e v un'interpretazione in A. Allora si ha*

1. $A, v \models (\varphi \vee \psi)$ *se, e soltanto se,* $A, v \models \varphi$ *oppure* $A, v \models \psi$;
2. $A, v \models (\varphi \rightarrow \psi)$ *se, e soltanto se, ogni volta che* $A, v \models \varphi$ *si ha anche* $A, v \models \psi$;
3. $A, v \models (\varphi \leftrightarrow \psi)$ *se, e soltanto se,* $A, v \models \varphi \Leftrightarrow A, v \models \psi$;
4. $A, v \models (\forall x \varphi)$ *se, e soltanto se, per ogni* a *in* A, $A, v[a/x] \models \varphi$;

Dimostrazione. La dimostrazione richiede semplicemente di sviluppare le definizioni dei connettivi stabilite in Notazione 4.5 e poi applicare la Definizione 4.21. □

Esempio 4.24. Si consideri la formula

$$(P(x) \wedge Q(x)) \to (\forall x \exists y (P(x) \vee \neg Q(y)))\,.$$

Stabiliamo se la formula è vera o falsa nella struttura

$$A \coloneqq \mathbb{N}, \quad P^A(n) \Leftrightarrow n \text{ è pari}, \quad Q^A(n) \Leftrightarrow n \text{ è dispari}$$

sotto l'interpretazione

$$\nu(x) \coloneqq 2, \quad \nu(y) \coloneqq 5.$$

$$\begin{array}{ll}
\quad \mathbb{N}, \nu \models (P(x) \wedge Q(x)) \to (\forall x \exists y (P(x) \vee \neg Q(y))) & \text{sse} \\
\text{Se } \mathbb{N}, \nu \models (P(x) \wedge Q(x)) \text{ allora } \mathbb{N}, \nu \models (\forall x \exists y (P(x) \vee \neg Q(y))) & \text{sse} \\
\text{Se } \mathbb{N}, \nu \models P(x) \text{ e } \mathbb{N}, \nu \models Q(x) \quad \text{allora} & \\
\quad \text{per ogni } n \in \mathbb{N} \quad \mathbb{N}, \nu[n/x] \models \exists y (P(x) \vee \neg Q(y)) & \text{sse} \\
\text{Se } P^A(\nu(x)) \text{ e } Q^A(\nu(x)) \quad \text{allora} & \\
\quad \text{per ogni } n \in \mathbb{N} \text{ esiste } m \in \mathbb{N} \quad \mathbb{N}, \nu[n/x][m/y] \models P(x) \vee \neg Q(y) & \text{sse} \\
\text{Se 2 è pari e 2 è dispari allora} & \\
\quad \text{per ogni } n \in \mathbb{N} \text{ esiste } m \in \mathbb{N} & \\
\quad \text{o } \mathbb{N}, \nu[n/x][m/y] \models P(x) \text{ oppure } \mathbb{N}, \nu[n/x][m/y] \models \neg Q(y) & \text{sse} \\
\text{Se 2 è pari e 2 è dispari allora} & \\
\quad \text{per ogni } n \in \mathbb{N} \text{ esiste } m \in \mathbb{N} & \\
\quad \text{o } P^A(\nu[n/x][m/y](x)) \text{ oppure non } Q^A(\nu[n/x][m/y](y)) & \text{sse} \\
\text{Se 2 è pari e 2 è dispari allora} & \\
\quad \text{per ogni } n \in \mathbb{N} \text{ esiste } m \in \mathbb{N} \;\text{ o } P^A(n) \text{ oppure non } Q^A(m) & \text{sse} \\
\text{Se 2 è pari e 2 è dispari allora} & \\
\quad \text{per ogni } n \in \mathbb{N} \text{ esiste } m \in \mathbb{N} \text{ tali che o } n \text{ è pari oppure } m \text{ non è dispari} &
\end{array}$$

Poiché è vero che esiste un m in $\mathbb{N}$ che non è dispari, la tesi nell'implicazione è vera e dunque è vera tutta la formula.

Esempio 4.25. Si consideri la formula

$$(\forall x P(x) \vee \forall x Q(x)) \to (\forall x (\neg P(x) \to \forall y Q(y)))\,.$$

Stabiliamo se la formula è vera o falsa nella struttura

$$A \coloneqq \mathbb{N}, \quad P(n) \Leftrightarrow n \text{ è pari}, \quad Q(n) \Leftrightarrow n \text{ è dispari}$$

otto l'interpretazione

$$\nu(x) \coloneqq 0, \nu(y) \coloneqq 0$$

$$
\begin{array}{ll}
\mathbb{N}, v \models (\forall x P(x) \vee \forall x Q(x)) \rightarrow (\forall x(\neg P(x) \rightarrow \forall y Q(y))) & \text{sse} \\
\text{Se } \mathbb{N}, v \models (\forall x P(x) \vee \forall x Q(x)) \text{ allora } \mathbb{N}, v \models (\forall x(\neg P(x) \rightarrow \forall y Q(y))) & \text{sse} \\
\text{Se } \mathbb{N}, v \models \forall x P(x) \text{ oppure } \mathbb{N}, v \models \forall x Q(x) & \\
\text{allora per ogni } n \in \mathbb{N}\ \mathbb{N}, v[n/x] \models (\neg P(x) \rightarrow \forall y Q(y)) & \text{sse} \\
\text{Se per ogni } m \in \mathbb{N}\ \mathbb{N}, v[m/x] \models P(x) \text{ oppure per ogni } l \in \mathbb{N}\ \mathbb{N}, v[l/x] \models Q(x) & \\
\text{allora per ogni } n \in \mathbb{N} \text{ se } \mathbb{N}, v[n/x] \models \neg P(x) \text{ allora } \mathbb{N}, v \models \forall y Q(y)) & \text{sse} \\
\text{Se per ogni } m \in \mathbb{N}\ m \text{ è pari oppure per ogni } l \in \mathbb{N}\ l \text{ è dispari} & \\
\text{allora per ogni } n \in \mathbb{N} \text{ se } \mathbb{N}, v[n/x] \not\models P(x) & \\
\quad \text{allora per ogni } p \in \mathbb{N}\ \mathbb{N}, v[q/y] \models Q(y)) & \text{sse} \\
\text{Se ogni } m \in \mathbb{N} \text{ è pari, oppure ogni } l \in \mathbb{N} \text{ è dispari} & \\
\text{allora se ogni } n \in \mathbb{N} \text{ non è pari allora ogni } p \in \mathbb{N} \text{ è dispari.} &
\end{array}
$$

La formula è vera perché l'ipotesi dell'implicazione è sempre falsa (non è vero che ogni m è pari oppure ogni l è dispari).

Osservazione 4.26. Al contrario di quanto avviene nel Calcolo Proposizionale, le definizioni che abbiamo dato non consentono, in generale, di determinare in modo effettivo il valore di verità di una formula ben formata φ in una data interpretazione A, v . Infatti, se il dominio A è un insieme infinito e se la formula φ contiene dei quantificatori, per determinare il valore di verità $v^A(\varphi)$ sarebbe necessario calcolare il valore di verità delle infinite formule che si ottengono da φ sostituendo alle variabili quantificate gli infiniti elementi di A.

Notiamo infine che il valore di verità di una formula ben formata φ sotto una data interpretazione v dipende solo dalla restrizione di v all'insieme delle variabili libere di φ. Si ha infatti:

Proposizione 4.27. *Siano φ una formula ben formata e A una struttura. Sia $FV(\varphi) = \{y_1, y_2, \dots, y_n\}$ l'insieme delle variabili libere di φ . Allora, per ogni coppia di interpretazioni v_1 e v_2 in A, se $v_1(y_i) = v_2(y_i)$, per ogni $i = 1, \dots, n$, allora $A, v_1 \models \varphi$ sse $A, v_2 \models \varphi$.*

Dimostrazione. La dimostrazione, per induzione sulla struttura della formula φ, è immediata. □

In generale gli enunciati sono oggetti più semplici delle formule perché in ogni singola struttura essi possono assumere solo uno dei due valori di verità. Si noti però che non si può fare a meno di lavorare anche con formule aperte, perché ogni volta che dimostriamo o definiamo qualcosa per induzione sulla costruzione di una formula, per ridurre la complessità di enunciato del tipo $\exists x \varphi(x)$ dobbiamo considerare la formula aperta $\varphi(x)$. Per ovviare a questo problema alcuni autori introducono un linguaggio espanso $\mathcal{L}(A)$ che ha simboli di costante per ogni elemento della struttura A. Questo semplifica solo in apparenza le cose, perché rimane poi da chiarire come è possibile interpretare ogni nuovo simbolo di costante nel corrispettivo elemento di A.

Corollario 4.28. *Se* φ *è una formula chiusa, allora il suo valore di verità non dipende dalle interpretazioni. In altre parole se* φ *è una formula chiusa, allora per ogni struttura* A *e per ogni coppia di interpretazioni* ν, ν' *in* A*, si ha che* $\mathsf{A}, \nu \models \varphi$ *se, e soltanto se,* $\mathsf{A}, \nu' \models \varphi$*.*

Il precedente corollario semplifica notevolmente la gestione delle formule quando esse sono chiuse (=enunciati), poiché nel trattare questi oggetti non ci sarà bisogno fare attenzione alle valutazioni. Abbiamo scelto nel seguito di enunciare alcuni teoremi restringendoci alle sole formule chiuse proprio perché grazie a questa restrizione le dimostrazioni si semplificano notevolmente. Incoraggiamo il lettore interessato a provare a dimostrare anche le versioni per formule generali di questi teoremi.

4.2.1 *Validità, Soddisfacibilità e Modelli*

Definizione 4.29

Sian $\varphi \in \mathtt{Form}\forall$ e $\Gamma \subseteq \mathtt{Form}\forall$.

1. La formula φ è **logicamente valida** se essa è vera in ogni struttura. In altre parole se per ogni A e per ogni interpretazione ν in A si ha $\mathsf{A}, \nu \models \varphi$. In tal caso scriveremo $\models \varphi$.
2. La formula φ è **soddisfacibile** se esistono una struttura A ed un'interpretazione ν tale che $\mathsf{A}, \nu \models \varphi$.
3. L'insieme Γ è logicamente valido se tutte le formule in Γ sono logicamente valide. In tal caso scriveremo $\models \Gamma$.
4. L'insieme Γ è soddisfacibile se esiste una struttura A e una valutazione ν in A tale che $\mathsf{A}, \nu \models \gamma$ per tutte le formule $\gamma \in \Gamma$.
5. La formula φ è **conseguenza logica** di Γ, se per ogni struttura A ed ogni interpretazione ν per i quali si abbia $\mathsf{A}, \nu \models \gamma$ per ogni $\gamma \in \Gamma$, risulta anche $\mathsf{A}, \nu \models \varphi$. In tal caso scriveremo $\Gamma \models \varphi$,
6. Le formule φ e ψ sono **logicamente equivalenti** se si ha che $\{\varphi\} \models \psi$ e $\{\psi\} \models \varphi$, in tal caso scriveremo $\varphi \equiv \psi$. È facile vedere che $\varphi \equiv \psi$ se, e solo se, $\models \varphi \leftrightarrow \psi$.

Il concetto di formula logicamente valida e quello di tautologia sono collegati dal fatto che le strutture a livello proposizionali sono semplicemente le valutazioni. Ricordiamo che una tautologia è una qualsiasi formula proposizionale che abbia solo 1 nell'ultima colonna della sua tavola di verità, in altre parole una formula vera sotto ogni possibile valutazione. Similmente una formula logicamente valida è una formula del prim'ordine vera in ogni struttura.

Osservazione 4.30. Dalle definizioni precedenti seguono immediatamente i seguenti fatti. Se $\Gamma \cup \{\varphi\}$ è un insieme di enunciati allora:

1. φ è logicamente valida se, e solo se, $\neg\varphi$ non è soddisfacibile (cioè è **insoddisfacibile**).
2. φ è soddisfacibile se, e solo se, $\neg\varphi$ non è logicamente valida.
3. $\Gamma \models \varphi$ se, e solo se, $\Gamma \cup \neg\varphi$ è insoddisfacibile.

Quindi affermare che un enunciato φ non sia valido non implica che esso sia contraddittorio (cioè che $\neg\varphi$ sia valido), ma solo che $\neg\varphi$ è soddisfacibile.

Definizione 4.31

Se $\mathcal{K}$ una classe di strutture per un linguaggio $\mathcal{L}$ e φ una formula in $\mathcal{L}$, scriveremo $\mathcal{K} \models \varphi$ per indicare che per ogni $\mathsf{A} \in \mathcal{K}$ vale $\mathsf{A} \models \varphi$. Useremo inoltre la seguente notazione: $\mathsf{Th}(\mathcal{K}) := \{\varphi \mid \varphi \text{ enunciato di } \mathcal{L} \text{ e } \mathcal{K} \models \varphi\}$.

Se Γ è un insieme di enunciati in un linguaggio $\mathcal{L}$ e A è una struttura per il linguaggio $\mathcal{L}$ scriveremo $\mathsf{A} \models \Gamma$ per indicare che $\mathsf{A} \models \varphi$ per ogni $\varphi \in \Gamma$. Useremo inoltre la seguente notazione: $\mathsf{Mod}(\Gamma) := \{\mathsf{A} \mid \mathsf{A} \text{ struttura per } \mathcal{L} \text{ e } \mathsf{A} \models \Gamma\}$.

Esercizio 4.32. Siano Σ e Δ insiemi arbitrari di enunciati in un linguaggio $\mathcal{L}$ e siano $\mathcal{H}$ e $\mathcal{K}$ classi arbitrarie di strutture per un linguaggio $\mathcal{L}$. Dimostrare i seguenti fatti:

- $\Sigma \subseteq \mathsf{Th}(\mathsf{K})$ se e soltanto se $\mathsf{K} \subseteq \mathsf{Mod}(\Sigma)$,
- Se $\Sigma \subseteq \Delta$ allora $\mathsf{Mod}(\Delta) \subseteq \mathsf{Mod}(\Sigma)$,
- Se $\Sigma \models \varphi$ allora $\mathsf{Mod}(\Sigma) \subseteq \mathsf{Mod}(\varphi)$,
- $\mathsf{Mod}(\Sigma \cup \Delta) = \mathsf{Mod}(\Sigma) \cap \mathsf{Mod}(\Delta)$,
- Se $\mathcal{K} \subseteq \mathcal{H}$ allora $\mathsf{Th}(\mathcal{H}) \subseteq \mathsf{Th}(\mathcal{K})$,
- $\mathsf{Th}(\mathcal{K} \cup \mathcal{H}) = \mathsf{Th}(\mathcal{K}) \cap \mathsf{Th}(\mathcal{H})$.

Lemma 4.33. *Sia φ una formula con $\mathsf{FV}(\varphi) = \{x_1, \ldots . x_n\}$, per ogni struttura A si ha*

$$\mathsf{A} \models \varphi \textit{ se, soltanto se, } \mathsf{A} \models \forall x_1 \ldots \forall x_n \varphi.$$

Lemma 4.34. *Per ogni formula φ si ha:*

$$\models \neg\neg\varphi \leftrightarrow \varphi, \tag{12}$$
$$\models \neg\forall x\varphi \leftrightarrow \exists x\neg\varphi, \qquad \models \neg\exists x\varphi \leftrightarrow \forall x\neg\varphi, \tag{13}$$
$$\models \forall x\forall y\varphi \leftrightarrow \forall y\forall x\varphi, \qquad \models \exists x\exists y\varphi \leftrightarrow \exists y\exists x\varphi, \tag{14}$$
$$\models \forall x(\varphi \wedge \psi) \leftrightarrow \forall x\varphi \wedge \forall x\psi, \qquad \models \exists x(\varphi \vee \psi) \leftrightarrow \exists x\varphi \vee \exists x\psi. \tag{15}$$

Se inoltre $x \notin \mathsf{FV}(\varphi)$ allora valgono anche le seguenti:

$$\models \forall y\varphi \leftrightarrow \forall x(\varphi[x/y]), \qquad \models \exists y\varphi \leftrightarrow \exists x(\varphi[x/y]), \tag{16}$$
$$\models \forall x(\varphi \vee \psi) \leftrightarrow \varphi \vee \forall x\psi, \qquad \models \exists x(\varphi \wedge \psi) \leftrightarrow \varphi \wedge \exists x\psi, \tag{17}$$
$$\models \forall x\varphi \leftrightarrow \varphi, \qquad \models \exists x\varphi \leftrightarrow \varphi. \tag{18}$$

Dimostrazione. Le dimostrazioni delle Equazioni da (13) a (18) sono tutte molto simili. Vediamo i dettagli della dimostrazione di Equazione (13) a titolo di esempio. Supponiamo che $\mathsf{FV}(\forall x\varphi) = \{z_1, \dots, z_n\}$. Allora occorre dimostrare che per ogni struttura A,

$$\mathsf{A} \models \forall z_1, \dots, \forall z_n (\neg\forall x\varphi \leftrightarrow \exists x \neg\varphi).$$

Equivalentemente, fissata un'arbitraria struttura A e un'arbitraria interpretazione ν in A, occorre mostrare che per ogni $a_1, \dots, a_n \in A$,

$$\mathsf{A}, \nu(a_1, \dots, a_n/x_1, \dots, x_n) \models (\neg\forall x\varphi \leftrightarrow \exists x\neg\varphi)$$

Utilizzando il Lemma 4.23, ciò diventa

$$\mathsf{A}, \nu(a_1, \dots, a_n/x_1, \dots, x_n) \models \neg\forall x\varphi \quad \Leftrightarrow \quad \mathsf{A}, \nu(a_1, \dots, a_n/x_1, \dots, x_n) \models \exists x\neg\varphi$$

che a sua volta, applicando la Definizione 4.21, equivale a

$$\begin{aligned} &\text{per ogni } a \in \mathsf{A}\ \mathsf{A}, \nu(a_1, \dots, a_n/x_1, \dots, x_n) \not\models \varphi(a/x) \\ &\Leftrightarrow \\ &\text{esiste } b \in \mathsf{A}\ \mathsf{A}, \nu(a_1, \dots, a_n/x_1, \dots, x_n) \models \neg\varphi(b/x) \end{aligned}$$

Quest'ultima equivalenza è ovviamente valida. □

Riguardo alla Equazione (17), si noti che l'ipotesi $x \notin \mathsf{FV}(\varphi)$ è cruciale. Infatti $\forall x(\mathsf{P}(x) \vee \mathsf{Q}(x))$ asserisce che preso un qualsiasi elemento di una data struttura, esso ha la proprietà P o ha la proprietà Q (ad esempio in $\mathbb{N}$ potrebbero essere interpretate come "pari" e "dispari"), mentre $\forall x\mathsf{P}(x) \vee \forall x\mathsf{Q}(x)$ asserisce che o tutti gli elementi di una struttura hanno la proprietà P o tutti hanno la proprietà Q (nell'interpretazione precedente: tutti in numeri naturali sono pari oppure sono tutti dispari). Ovviamente la prima non implica la seconda.

Riguardo alla Equazione (16), si noti che essa ha il seguente corollario immediato.

Corollario 4.35. *Ogni formula è logicamente equivalente a una le cui variabili libere sono tutte diverse da quelle vincolate.*

Lemma 4.36 (Teorema di sostituzione)**.** *Siano* t_1, t_2 *e* s *dei termini e* φ *una formula. Supponiamo che* t_1 *e* t_2 *siano sostituibili per* x *in* φ*, allora*

1. $\models (t_1 = t_2) \to (s(t_1/x) = s(t_2/x))$;
2. $\models (t_1 = t_2) \to (\varphi(t_1/x) \leftrightarrow \varphi(t_2/x))$.

Dimostrazione. Entrambi i punti asseriscono che una certa formula è valida in ogni struttura e sotto ogni interpretazione. Per dimostrarli prendiamo dunque una struttura arbitraria A e un'interpretazione arbitraria ν in A.

Punto 1. Cominciamo notando che per il Lemma 4.23, Punto 1, mostrare l'asserto è equivalente a far vedere che se $\mathsf{A}, \nu \models t_1 = t_2$ allora $\mathsf{A}, \nu \models s(t_1/x) = s(t_2/x)$. Il fatto che valga $\mathsf{A}, \nu \models t_1 = t_2$ è equivalente a dire che $\tilde{\nu}(t_1) = \tilde{\nu}(t_2)$. Procediamo per induzione sulla complessità di s.

Se s è una variabile allora possiamo avere due casi:

CASO 1) $s = x$ e in questo caso abbiamo $s(t_1/x) = t_1$ e $s(t_2/x) = t_2$. , dunque $A, v \models (s(t_1/x) = s(t_2/x))$ equivale a $A, v \models t_1 = t_2$ e ciò vale per ipotesi.

CASO 2) $s \neq x$ e abbiamo $s(t_1/x) = s = s(t_2/x)$ e l'asserto vale banalmente.

Se s è una costante abbiamo nuovamente $s(t_1/x) = s = s(t_2/x)$. Questo conclude il passo base.

Se ora $s = f(w_1, \dots, w_n)$ con $w_1, \dots, w_n \in \mathtt{Term}$, allora

$$s(t_1/x) = f(w_1(t_1/x), \dots, w_n(t_1/x)) \text{ e } s(t_2/x) = f(w_1(t_2/x), \dots, w_n(t_2/x)).$$

Ricordiamo che per la Definizione 4.20 si ha

$$\tilde{v}(s(t_1/x)) = f^A(\tilde{v}(w_1(t_1/x)), \dots, \tilde{v}(w_n(t_1/x))).$$

Ma per ipotesi induttiva per $1 \leqslant i \leqslant n$, $\tilde{v}(w_i(t_1/x)) = \tilde{v}(w_i(t_2/x))$, dunque abbiamo $\tilde{v}(s(t_1/x)) = \tilde{v}(s(t_2/x))$ e quindi $A, v \models s(t_1/x) = s(t_2/x)$.

La dimostrazione del Punto 2 è simile ed è lasciata per esercizio. □

Concludiamo questa sezione con un teorema di forma normale. Diremo che una formula φ è in **forma normale prenessa** se tutti i quantificatori in φ (se ce ne sono) appaiono all'inizio della formula, in altre parole se è della forma

$$Q_1 x_1 \dots Q_n x_n (\psi)$$

dove per $1 \leqslant i \leqslant n$, $Q_i \in \{\forall, \exists\}$ e ψ non ha quantificatori.

Teorema 4.37 (Forma normale prenessa)

Per ogni formula del prim'ordine φ esiste una formula χ in forma normale prenessa, tale che $\models \varphi \leftrightarrow \chi$.

Dimostrazione. Forniamo un algoritmo per spostare tutti i quantificatori dall'interno di una formula φ al suo inizio. Prima di tutto occorre riscrivere le abbreviazioni $\to$ e $\leftrightarrow$ come combinazioni di $\neg, \vee$ e $\wedge$. Mostriamo ora come far passare i quantificatori davanti a questi ultimi connettivi.

Se il quantificatore si trova dopo una negazione la formula φ avrà una delle seguenti forme:

$$\neg\exists x \psi_1 \qquad \text{oppure} \qquad \neg\forall x \psi_1.$$

In questo caso basta applicare la (13) del Lemma 4.34 per ottenere che tali formule sono equivalenti a

$$\forall x \neg \psi_1 \qquad \text{oppure} \qquad \exists x \neg \psi_1.$$

Se il quantificatore si trova dopo una congiunzione la formula φ sarà equivalente a una delle seguenti forme:

$$\psi_1 \wedge \exists x \psi_2 \qquad \text{oppure} \qquad \psi_1 \wedge \forall x \psi_2.$$

Nel primo caso possiamo scegliamo una variabile z *nuova*, nel senso che essa non appare nella formula. Applichiamo la (16) del Lemma 4.34 per riscrivere la formula nella forma equivalente $\psi_1 \wedge (\exists z(\psi_2[z/x]))$. A questo punto, poiché z è nuova siamo sicuri che l'ipotesi della (17) è soddisfatta e quindi possiamo riscrivere la formula nella sua forma equivalente $\exists z(\psi_1 \wedge (\psi_2[z/x]))$, dove il quantificatore è passato davanti al $\wedge$. Se invece la formula φ è della forma $\psi_1 \wedge \forall x \psi_2$, scegliamo ancora una volta una variabile z nuova, così da poter applicare le (18) e (16) e ottenere che φ è equivalente a $\forall z \psi_1 \wedge \forall z(\psi_2[z/x])$. A questo punto si può applicare la (15) per trasformare φ nella formula logicamente equivalente $\forall z(\psi_1 \wedge (\psi_2[z/x]))$.

Il terzo caso, in cui il quantificatore si trova dopo una disgiunzione è simmetrico al caso precedente.

□

4.3 La deduzione naturale per la logica del prim'ordine.

Come abbiamo fatto per la logica proposizionale nella Sezione 2.6 è il momento di introdurre un calcolo che riesca a catturare in maniera puramente sintattica il concetto di *conseguenza logica*. La deduzione naturale per la logica del prim'ordine è un'estensione di quella per la logica proposizionale. Passiamo dunque a un'analisi dei nuovi connettivi, cioè dei quantificatori.

4.3.0.1 *Quantificatore universale*

Quando facciamo matematica, per mostrare che vale una formula del tipo $\forall x \varphi(x)$ di solito operiamo come segue: prendiamo un x nel dominio arbitrario, mostriamo che x ha la proprietà φ e, dall'arbitrarietà di x, deduciamo che la proprietà φ vale per ogni elemento della struttura. Per codificare questo ragionamento nella sintassi è quindi necessario formalizzare cosa vuol dire che x è *arbitrario*. Intuitivamente x è arbitrario se non c'è nessuna ipotesi aggiuntiva su x. Se ad esempio stessimo considerando un x in $\mathbb{N}$, un'ipotesi del tipo $\exists y \in \mathbb{N}(x = 2y)$ ci farebbe perdere di generalità perché forzerebbe x ad essere un numero pari. Sintatticamente quindi potremmo dire che l'x di $\varphi(x)$ è *arbitrario* se tra le ipotesi che hanno portato a dimostrare $\varphi(x)$ non compaiono formule in cui x è una variabile libera. Arriviamo dunque alla seguente regola:

$$\begin{array}{c} \Gamma \\ \vdots \\ \mathrm{I}\forall \dfrac{\varphi}{\forall x \varphi} \end{array}$$

con la prescrizione che tale regola può essere utilizzata solo quando x non compare libera nelle ipotesi da cui φ dipende.

Eliminare un quantificatore universale è più semplice, infatti se abbiamo dimostrato che $\forall x\varphi(x)$ vale, allora sappiamo che $\varphi(t)$ vale per ogni termine t che sia sostituibile per x in f. Formalmente

$$\begin{array}{c} \Gamma \\ \vdots \\ \mathrm{E}\forall\ \dfrac{\forall x\varphi}{\varphi[t/x]} \end{array}$$

per ogni termine t sostituibile per x in φ.

4.3.0.2 *Quantificatore esistenziale*

Analizziamo ora il caso del quantificatore esistenziale. Quando vogliamo dimostrare che una formula del tipo $\exists x\varphi(x)$ vale, di solito quello che facciamo è costruire un termine t per cui possiamo provare che $\varphi(t)$ vale, per poi concluderne che $\exists x\varphi(x)$ vale. Formalmente abbiamo dunque:

$$\begin{array}{c} \Gamma \\ \vdots \\ \mathrm{I}\exists\ \dfrac{\varphi(t)}{\exists x\varphi[x/t]} \end{array}$$

dove t è un termine sostituibile per x in φ.

Eliminare un quantificatore esistenziale è un po' più difficile, perché sapere che vale $\exists x\varphi(x)$ non ci dà nessuna informazione su quale t potrebbe avere la proprietà φ. Ciò ricorda la situazione in cui si è dimostrato che vale $\varphi \vee \psi$, ma non si ha nessuna informazione sul quale delle due valga. Possiamo quindi procedere in maniera simile alla regole $\mathrm{E}\vee$: supponiamo di essere capaci di dimostrare, assumendo che valga $\varphi(x)$ una certa formula ψ e supponiamo che in tale dimostrazione non si è fatto uso di nessuna particolare proprietà di x, allora dal semplice fatto che esiste una x per cui $\varphi(x)$ vale, si può dimostrare ψ. In simboli:

$$\mathrm{E}\exists_1\ \dfrac{\exists x\varphi \qquad \begin{array}{c}[\varphi]^1 \\ \vdots \\ \psi\end{array}}{\psi}$$

Con la prescrizione che tale regola può essere applicata solo se la variabile x non compare libera in ψ né nelle ipotesi da cui ψ dipende oltre a φ stessa (in cui ovviamente può apparire libera).

Esempio 4.38. Vediamo come la regola $\mathrm{I}\forall$ possa essere dedotta dalle altre. Ricordiamo che $\forall x \varphi(x)$ è un'abbreviazione per $\neg\exists\neg\varphi(x)$. Dobbiamo dunque dimostrare che il passo

$$\mathrm{I}\forall\ \dfrac{\begin{matrix}\Gamma\\ \vdots\\ \varphi\end{matrix}}{\neg\exists\neg\varphi(x)}$$

è una derivazione (possibilmente composta da più passi) ogni qualvolta x non compaia libera nelle formule in Γ. Dunque sappiamo che in qualche maniera è possibile derivare φ da Γ e che x non appare libera nelle formule in Γ e vogliamo derivare $\neg\exists\neg\varphi(x)$; si consiglia di leggere la seguente derivazione partendo dal basso verso l'alto.

$$\mathrm{I}\neg_1\ \dfrac{\mathrm{E}\exists_1\ \dfrac{[\exists x\neg\varphi]^1 \qquad \dfrac{[\neg\varphi]^1 \qquad \begin{matrix}\Gamma\\ \vdots\\ \varphi\end{matrix}}{\bot}\ \mathrm{E}\neg}{\bot}}{\neg\exists\neg\varphi(x)}$$

Si noti che l'applicazione della regola $\mathrm{E}\exists$ è lecita proprio perché per ipotesi x non appare libera nelle ipotesi in Γ oltre a φ.

Esempio 4.39. Vediamo, come secondo esempio, come regola $\mathrm{E}\forall$ possa essere dedotta dalle altre. Occorre dimostrare che il passo

$$\mathrm{E}\forall\ \dfrac{\begin{matrix}\Gamma\\ \vdots\\ \neg\exists\neg\varphi\end{matrix}}{\varphi[t/x]}$$

è una derivazione (possibilmente composta da più passi) ogni qualvolta t è sostituibile per x in φ. Dunque sappiamo che in qualche maniera è possibile derivare $\neg\exists\neg\varphi$ da Γ e vogliamo derivare $\varphi[t/x]$.

$$\mathrm{RA}_1\ \dfrac{\mathrm{I}\neg\ \dfrac{\begin{matrix}\Gamma\\ \vdots\\ \neg\exists\neg\varphi(t)\end{matrix} \qquad \dfrac{[\neg\varphi(t)]^1}{\exists x\neg\varphi(x)}\ \mathrm{I}\exists}{\bot}}{\varphi(t)}$$

Esercizio 4.40. Produrre dimostrazioni dei seguenti fatti.

1. Se c è una costante che non compare in $\Gamma \cup \{\varphi\}$ e x è una variabile che non compare in Γ, da $\Gamma \vdash \varphi[c/x]$ segue $\Gamma \vdash \forall x\varphi(x)$

2. $\vdash \forall x(\varphi(x) \to \psi) \to (\exists x \varphi(x) \to \psi)$, dove $x \notin FV(\psi)$.
3. $\vdash \exists x \varphi(x) \to \exists y \varphi(y)$, se y non occorre in φ.
4. $\vdash \exists x(\varphi \to \psi(x)) \leftrightarrow (\varphi \to \exists x \psi(x))$, dove $x \notin FV(\varphi)$.

4.3.1 *Adeguatezza della deduzione naturale*

Vediamo che l'apparato deduttivo introdotto è compatibile con la semantica definita al primo ordine.

Teorema 4.41 (Adeguatezza del sistema assiomatico)

Per ogni insieme di formule $\Gamma \cup \{\varphi\}$, *se* $\Gamma \vdash \varphi$ *allora* $\Gamma \models \varphi$.

Dimostrazione. Per induzione sulla complessità della deduzione, verifichiamo soltanto che le regole di introduzione ed eliminazione di $\exists$ preservano la validità.

Verifichiamo che $\Gamma \models \exists x \varphi[x/t]$, sotto l'ipotesi induttiva: $\Gamma \models \varphi(t)$. Dobbiamo quindi verificare che ogni modello A di Γ è anche modello di $\exists x \varphi[x/t]$. Dunque, se A è un modello di Γ, allora per ipotesi di induzione, $A \models \varphi(t)$. Quindi, per ogni valutazione v, la struttura A rende vera la formula $\varphi^A(\tilde{v}(t))$. Di conseguenza, per ogni v esiste un $a \in A$ (basta porre $a = \tilde{v}(t)$) tale che $A, v[a/x] \models \varphi[x/t]$. Quindi $A, v \models \exists x \varphi(x)$ per ogni valutazione e $A \models \exists x \varphi(x)$.

Vediamo ora il caso dell'eliminazione di $\exists$.

$$\dfrac{\begin{matrix}\Gamma \\ \vdots \\ \exists x \psi\end{matrix} \qquad \begin{matrix}\Gamma, [\psi]^1 \\ \vdots \\ \varphi\end{matrix}}{\varphi}\, E\exists_1$$

Dunque abbiamo per ipotesi una derivazione di $\exists x \psi(x)$ da Γ di lunghezza inferiore, e quindi applicando l'ipotesi induttiva otteniamo $\Gamma \models \exists x \psi(x)$. Si noti che per ogni y sostituibile in ψ per x che non compare in Γ, abbiamo anche

$$\Gamma \models \exists y \psi(y). \tag{19}$$

Inoltre, sempre per ipotesi, abbiamo anche una dimostrazione di φ da Γ e $\psi(y)$, con y che non compare in Γ e φ. Utilizzando nuovamente l'ipotesi induttiva otteniamo che

$$\Gamma \cup \{\psi(y)\} \models \varphi. \tag{20}$$

Per dimostrare che $\Gamma \models \varphi$, prendiamo una struttura A e una valutazione v tali che $A, v \models \Gamma$. Allora dalla (19) otteniamo che $A, v \models \exists y \psi(y)$. In altri termini: esiste $a \in A$ tale che $A, v[a/y] \models \psi(y)$. Si noti che siccome y non appare libera in Γ, abbiamo anche

che $A, v[a/y] \models \Gamma$. Dunque la struttura A con la valutazione $v[a/y]$ soddisfa sia Γ che $\psi(y)$. Per la (20), deve valere $A, v[a/y] \models \varphi$, ma poiché y non appare libera in φ vale anche $A, v \models \varphi$. Quindi abbiamo stabilito che per ogni struttura A e ogni valutazione v se $A, v \models \Gamma$ allora $A, v \models \varphi$, in altre parole $\Gamma \models \varphi$. □

Poiché abbiamo deciso di includere sempre il simbolo di uguaglianza nei linguaggi del prim'ordine che considereremo, introduciamo anche delle regole di derivazione per l'uguaglianza, essi codificano il fatto che $=$ è una relazione di equivalenza *compatibile* con i termini e le formule.

$$\text{U1}\ \frac{}{x = x} \qquad \text{U2}\ \frac{x = y}{y = x} \qquad \text{U3}\ \frac{x = y \quad y = z}{x = z}$$

$$\text{U4}\ \frac{x_1 = y_1 \dots x_n = y_n}{t(x_1, \dots, x_n) = t(y_1, \dots, y_n)} \qquad \text{U5}\ \frac{x_1 = y_1 \dots x_n = y_n \quad \varphi(x_1, \dots, x_n)}{\varphi(y_1, \dots, y_n)}$$

Teorema 4.42 (Teorema di deduzione al prim'ordine)

Siano $\Gamma \subseteq \texttt{Form}\forall$ *e* $\varphi, \psi \in \texttt{Form}\forall$. *Si ha* $\Gamma \cup \{\varphi\} \vdash \psi$ *se e soltanto se* $\Gamma \vdash \varphi \to \psi$.

Dimostrazione. La dimostrazione segue banalmente dalle regole di introduzione ed eliminazione dell'implicazione. □

4.4 IL TEOREMA DI COMPLETEZZA

In questa sezione dimostriamo l'analogo del Teorema 2.57 per il calcolo dei predicati.

Definizione 4.43

Una **teoria** è un insieme di formule chiuse T, tale che ogni formula da esso deducibile vi appartiene. In simboli: se $T \vdash \varphi$, allora $\varphi \in T$.

Un insieme $\Delta \subseteq T$ tale che $T = \{\varphi \mid \Delta \vdash \varphi\}$ è detto **insieme di assiomi** per T. Diremo anche che T è assiomatizzata da Δ.

Il concetto di teoria coerente è definito come nel caso proposizionale: T è coerente se $T \nvdash \bot$.

Lemma 4.44. *Sia* T *una teoria del prim'ordine.*

1. *Le seguenti affermazioni sono equivalenti.*
   a) T *è incoerente,*

b) per ogni formula $\psi \in \texttt{Form}\forall$*, si ha* $T \vdash \psi$*,*

c) esiste $\psi \in \texttt{Form}\forall$ *tale che* $T \vdash \psi$ *e* $T \vdash \neg\psi$*.*

2. *Per ogni* $\varphi \in \texttt{Form}\forall$ *se* $T \nvdash \varphi$ *allora* $T \cup \{\neg\varphi\}$ *è coerente.*

3. *Se* T *è una teoria e* Δ *è un suo insieme di assiomi, allora* T *è coerente se, e solo se,* Δ *è coerente.*

Dimostrazione. 1. Si dimostra in maniera analoga al caso proposizionale. Osserviamo che l'ipotesi di φ formula chiusa ci assicura di poter utilizzare liberamente le regole di introduzione ed eliminazione dei quantificatori e il teorema di deduzione.

2. Dimostriamo la contronominale. Supponiamo che $T \cup \{\neg\varphi\}$ sia incoerente, allora esiste una derivazione con ipotesi in $T \cup \{\neg\varphi\}$ e conclusione $\perp$. Estendiamo tale derivazione con un ulteriore passaggio usando la regola di riduzione ad assurdo e otteniamo che $T \vdash \varphi$.

3. Poiché $\Delta \subseteq T$, se Δ è incoerente, allora ovviamente anche T lo è. Viceversa, supponiamo che $T \vdash \perp$, allora poiché le derivazioni sono oggetti finiti deve esistere un sottoinsieme finito $\Gamma \subseteq T$ tale che $\Gamma \vdash \perp$. Ma ogni formula in T è derivabile da Δ, quindi in particolare per ogni formula $\gamma \in \Gamma$, $\Delta \vdash \gamma$. Combinando le derivazioni di ogni γ (che sono in numero finito) con la derivazione che dà $\Gamma \vdash \perp$ si ottiene che $\Delta \vdash \perp$.

□

Definizione 4.45

Sia T una teoria nel linguaggio $\mathcal{L}$ e S una teoria in un linguaggio $\mathcal{L}'$. Diremo che

1. S è un'**estensione** di T se $T \subseteq S$ e $\mathcal{L} \subseteq \mathcal{L}'$.
2. S è un'**estensione conservativa** di T se:
   a) $T \subseteq S$ e
   b) per ogni formula φ nel linguaggio $\mathcal{L}$ si ha che $\varphi \in T$ se e soltanto se $\varphi \in S$.

Esempio 4.46. L'idea delle estensioni conservative nasce dalla diffusa pratica matematica di estendere il linguaggio tramite definizioni, per cui tutti gli esempi di questo tipo sono estensioni conservative. Ad esempio, si potrebbero introdurre i gruppi come strutture con un solo simbolo di funzione binaria $\cdot$. Gli assiomi sarebbero

$$\forall x \forall y \forall z\,(((x \cdot y) \cdot z) = (x \cdot (y \cdot z)))\,,$$
$$\exists x\big(\forall y((y \cdot x = y) \land (x \cdot y = y) \land \exists z((y \cdot z = x) \land (z \cdot y = x)))\big).$$

Poiché è possibile provare che un tale x è unico, possiamo estendere il linguaggio con una nuova costante 1 e aggiungere l'assioma

$$\forall x((x \cdot 1 = x) \wedge (1 \cdot x = x)).$$

Questa estensione è conservativa sulla prima.

Esempio 4.47. La teoria degli anelli è un'estensione conservativa dei gruppi abeliani. Per dimostrare tale asserto si può usare il fatto (che non dimostriamo qui) che una teoria S nel linguaggio $\mathcal{L}'$ è un'estensione conservativa di una teoria T nel linguaggio $\mathcal{L}$ se ogni modello di T può essere esteso a un modello di S. Poiché ogni gruppo abeliano può essere dotato di una moltiplicazione di anello definendo $x \cdot y = 0$, si ottiene l'asserto. Si osservi che esistono gruppi abeliani che non sono estendibili ad anelli con unità. Se ad esempio un gruppo è tale che ogni suo elemento ha ordine infinito, ma gli ordini dei suoi elementi non hanno un maggiorante, allora questo non può essere esteso ad un anello con unità. Il motivo è che se ciò fosse possibile allora 1 avrebbe ordine finito, diciamo k, ma allora per ogni a nel gruppo si avrebbe $a + \overset{k \text{ volte}}{\dots} + a = a \cdot 1 + \overset{k \text{ volte}}{\dots} + a \cdot 1 = a \cdot (k) = a \cdot 0 = 0$ e quindi ogni elemento avrebbe ordine minore di k.

Definizione 4.48

Sia T una teoria in un linguaggio $\mathcal{L}$. Diremo che T è **Henkin** se per ogni formula chiusa nel linguaggio $\mathcal{L}$ del tipo $\exists x \varphi(x)$ esiste una costante $c \in \mathcal{L}$ tale che $(\exists x \varphi(x) \to \varphi[c/x]) \in T$. Tale costante c è detta **testimone** della formula $\exists x \varphi(x)$.

Osservazione 4.49. Così come nel caso proposizionale, se il linguaggio $\mathcal{L}$ è numerabile, l'insieme $\mathtt{Form}\forall$ è numerabile. In particolare, è possibile enumerare l'insieme delle formule chiuse nel linguaggio $\mathcal{L}$ e quello delle formule con al più una variabile libera. Nel resto di questa sezione, per semplificare la dimostrazione del teorema di completezza assumeremo che il linguaggio sia numerabile. La generalizzazione della dimostrazione a linguaggi di cardinalità superiore non presenta particolari difficoltà.

Definizione 4.50

Data una teoria T in un linguaggio $\mathcal{L}$, denoteremo con T^H la teoria nel linguaggio $\mathcal{L}^H$ così definiti:

- $\mathcal{L}^H := \mathcal{L} \cup \{c_\varphi \mid \exists x \varphi(x) \text{ formula chiusa nel linguaggio } \mathcal{L}\}$,
- Sia $\Delta := \{\exists x \varphi(x) \to \varphi[c_\varphi/x] \mid \exists x \varphi(x)$ *formula chiusa di* $\mathcal{L}\}$ Definiamo T^H come la teoria assiomatizzata da $T \cup \Delta$.

Lemma 4.51. *La teoria* T^H *è estensione conservativa di* T.

Dimostrazione. La teoria T^H è estensione di T per definizione. Dimostriamo che è conservativa.

Usando la notazione della Definizione 4.50, supponiamo inizialmente che un'enunciato arbitrario $\psi \in T^H$ sia dimostrabile da T e un solo assioma di Δ, che chiameremo δ_1. In simboli,

$$T \cup \{\delta_1\} \vdash \psi.$$

Quindi, tramite la regola di introduzione dell'implicazione, otteniamo

$$T \vdash \delta_1 \to \psi.$$

Poiché $\delta_1 \in \Delta$ essa avrà la forma $\exists x \varphi(x) \to \varphi[c_\varphi/x]$ per qualche formula chiusa $\exists x \varphi(x)$ di $\mathcal{L}$. Possiamo sostituire nella derivazione di $T \vdash \delta_1 \to \psi$ tutte le occorrenze della costante c_φ con una variabile y ancora mai utilizzata, ottenendo

$$T \vdash (\exists x \varphi(x) \to \varphi[y/x]) \to \psi.$$

Ora applichiamo un ulteriore passo di derivazione applicando la regola I$\forall$ e introduciamo il quantificatore $\forall y$, ciò è possibile perché y non compariva nella derivazione precedente, si veda Esercizio 4.40. Otteniamo così

$$T \vdash \forall y((\exists x \varphi(x) \to \varphi(y)) \to \psi).$$

Si noti che ψ rimane invariata dopo questa sostituzione perché ψ è nel linguaggio $\mathcal{L}$ e quindi sicuramente c_φ non occorre in ψ. Per la distributività dei quantificatori sull'implicazione (si vedano le Punti 1 e 4 del Esercizio 4.40), ricaviamo

$$T \vdash (\exists y(\exists x \varphi(x) \to \varphi(y))) \to \psi$$

e ancora

$$T \vdash (\exists x \varphi(x) \to \exists y \varphi[y/x])) \to \psi.$$

Poiché $\vdash \exists x \varphi(x) \to \exists y \varphi(y)$, si deduce $T \vdash \psi$.

Sia ora $T^H \vdash \psi$ e siano $\{\delta_1, \dots \delta_k\}$ gli assiomi di Δ che vengono usati nella dimostrazione di ψ. Si vede facilmente, con la stessa tecnica dimostrativa, che $T \cup \{\delta_1, \dots, \delta_n\} \vdash \psi$ implica $T \cup \{\delta_1, \dots, \delta_{n-1}\} \vdash \psi$. Quindi, procedendo per induzione su k, si ricava che $T^H \vdash \psi$ implica $T \vdash \psi$. $\square$

Osserviamo che la teoria T^H potrebbe non essere Henkin: aggiungendo le costanti e chiudendo per derivabilità rispetto ai nuovi assiomi, abbiamo generato nuove formule che potrebbero non avere testimoni in T^H. Per superare questo problema dobbiamo iterare infinite volte la costruzione.

Definizione 4.52

Data una teoria T in un linguaggio $\mathcal{L}$, denoteremo con $\overline{T}$ la teoria nel linguaggio $\overline{\mathcal{L}}$, entrambi definiti per ricorsione come segue:

$$T_0 \coloneqq T \qquad T_n \coloneqq (T_{n-1})^H \qquad \overline{T} \coloneqq \bigcup_{n \in \mathbb{N}} T_n.$$

$$\mathcal{L}_0 \coloneqq \mathcal{L} \qquad \mathcal{L}_n \coloneqq (\mathcal{L}_{n-1})^H \qquad \overline{\mathcal{L}} \coloneqq \bigcup_{n \in \mathbb{N}} \mathcal{L}_n.$$

Proposizione 4.53. *Se T è una teoria coerente allora $\overline{T}$ estende T, è Henkin ed è conservativa, quindi coerente.*

Dimostrazione. Data la seguente sequenza di teorie:

$$T_0 \coloneqq T \qquad T_n \coloneqq (T_{n-1})^H,$$

mostriamo per induzione su n che ogni T_n è estensione conservativa di T. Infatti, per il Lemma 4.51, per ogni $n \in \mathbb{N}$, T_n è una estensione conservativa di T_{n-1}. Supponiamo che T_{n-1} sia un'estensione conservativa di T e che ψ sia una formula nel linguaggio di T tale che $T_n \vdash \psi$. Per definizione della sequenza di teorie, deduciamo $T_{n-1} \vdash \psi$. Quindi, per ipotesi di induzione, $T \vdash \psi$ e T_n è conservativa rispetto a T. Da ciò deriva che $\overline{T}$ è un'estensione conservativa di T. Infatti, se ψ è una formula nel linguaggio di T tale che $\overline{T} \vdash \psi$ e siano $\psi_1, \dots \psi_m$ le formule di $\overline{T}$ usate nella dimostrazione. Poiché le teorie T_n formano una catena, denotiamo con s l'intero dato da $s = \max\{i \mid \psi_1, \dots \psi_m \in T_i\}$. Quindi, $T_s \vdash \psi$, ma allora $T \vdash \psi$.

Mostriamo ora che $\overline{T}$ è Henkin. Se $\exists x \varphi(x)$ è una formula nel linguaggio di $\overline{T}$, questa conterrà soltanto un numero finito di nuove costanti della forma c_ψ, quindi, poiché i linguaggi sono linearmente ordinati da $\subseteq$, esisterà un n tale che $\exists x \varphi(x)$ è una formula del linguaggio di T_n e $\exists x \varphi(x) \to \varphi[c_\varphi/x] \in T_{n+1}$. Quindi $\exists x \varphi(x) \to \varphi[c_\varphi/x] \in \overline{T}$.

Infine si noti che ogni estensione conservativa S di una teoria coerente T è a sua volta coerente. Se infatti S è contradditoria allora per ogni ψ nel linguaggio di T, $S \vdash \psi$ ma poiché S è conservativa abbiamo che anche $T \vdash \psi$ e quindi T è incoerente. $\square$

Il concetto di teoria massimalmente coerente è definito come nel caso proposizionale: T è massimalmente coerente se è coerente e se $\varphi \notin T$ allora $T \cup \{\varphi\} \vdash \bot$.

Lemma 4.54. *Ogni teoria coerente ammette una estensione massimalmente coerente. Se la teoria di partenza è di Henkin, la sua estensione massimale sarà ancora di Henkin.*

Dimostrazione. La dimostrazione è del tutto analoga a quella del Lemma 2.39. È possibile dimostrare che ogni catena nell'insieme

$$\{\mathcal{G} \mid T \subseteq \mathcal{G},\ \mathcal{G} \text{ estensione conservativa e coerente}\}$$

ammette un maggiorante, e quindi si può applicare il Lemma di Zorn per ottenere l'esistenza di un'estensione massimale S di T. La teoria S è ancora Henkin poiché S è nello stesso linguaggio di T: per ogni enunciato $\exists x \varphi(x)$ nel linguaggio di T, esiste c tale che $\exists x \varphi(x) \to \varphi[c/x] \in T \subseteq S$. $\square$

Lemma 4.55. *Se* T *è una teoria massimalmente coerente allora, per ogni* φ, ψ *formule nel linguaggio di* T*, valgono le seguenti:*

1. $T \vdash \varphi$ *o* $T \vdash \neg\varphi$*,*
2. $T \vdash \varphi \wedge \psi$ *se e soltanto se* $T \vdash \varphi$ *e* $T \vdash \psi$*.*

Dimostrazione. La dimostrazione è del tutto simile a quella del Lemma 2.41. □

Lemma 4.56. *Ogni insieme di enunciati coerente ammette un modello.*

Dimostrazione. Sia Γ un'insieme di enunciati coerente e sia T la teoria assiomatizzata da Γ, cioè $T := \{\psi \mid \Gamma \vdash \psi\}$. Sia $\overline{K}$ un'estensione di Henkin di T data dal Proposizione 4.53 e S l'estensione massimale di $\overline{K}$ data dalla Proposizione 4.53 e lemma 4.54. Sia $\mathcal{L}$ il linguaggio di S, definiamo una struttura B nel seguente modo:

1. il dominio B della struttura è dato dall'insieme dei termini chiusi del linguaggio $\mathcal{L}$;
2. per ogni predicato $P \in \mathcal{L}$, definiamo la relazione P^B data da $(t_1, \dots t_n) \in P^B$ se, soltanto se, $S \vdash P(t_1, \dots, t_n)$;
3. per ogni simbolo di funzione $f \in \mathcal{L}$, definiamo $f^B : B^n \to B$, $f^B(t_1, \dots t_n) = f(t_1, \dots, t_n)$, che è ancora un termine chiuso di $\mathcal{L}$;
4. ogni simbolo di costante viene mandato in se stesso, cioè $c^B = c$, per ogni costante c di $\mathcal{L}$.

La struttura così ottenuta non è ancora quella desiderata, in quanto non interpreta l'uguaglianza dei termini nella vera uguaglianza. Di conseguenza, consideriamo la relazione:

$$t \sim s \quad \text{se, soltanto se, } S \vdash t = s.$$

Il fatto che la relazione $\sim$ sia di equivalenza deriva direttamente dalle regole di deduzione naturale per $=$. La semplice verifica è lasciata al lettore. Consideriamo ora la struttura quoziente A ottenuta da B nel seguente modo:

1. il dominio A della struttura è dato $B/\sim$;
2. per ogni predicato $P \in \mathcal{L}$, $P^A = \{([t_1], \dots, [t_n]) \mid (t_1, \dots, t_n) \in P^B\}$;
3. per ogni simbolo di funzione $f \in \mathcal{L}$, definiamo $f^A : A^n \to A$, $f^A([t_1], \dots [t_n]) = [f^B(t_1, \dots, t_n)]$;
4. ogni simbolo di costante viene mandato nella sua classe di equivalenza, cioè $c^A = [c]$.

Usando la definizione di $\sim$, è immediato verificare che la struttura quoziente è ben definita, procedendo per induzione sulla costruzione dei termini chiusi.

Resta da verificare che A così definita è un modello per T, e cioè

$$A \models \varphi \text{ se, soltanto se, } S \vdash \varphi. \tag{21}$$

Verifichiamo la (21) per induzione sulla complessità della formula φ.

La base di induzione consiste nel caso in cui φ è un predicato applicato a dei termini. Si ha $A \models P(t_1, \ldots, t_m)$ se, e solo se, $(t_1^A, \ldots, t_n^A) \in P^A$, per la definizione di validità, ricordando che i termini $t_1, \ldots, t_n$ sono necessariamente chiusi perché φ è un enunciato. Inoltre è facile vedere, per induzione sulla complessità di t che $t^A = [t]$, dunque si ha $(t_1^A, \ldots, t_n^A) \in P^A$ se, e solo se, $([t_1], \ldots, [t_n]) \in P^A$. Quest'ultima condizione è equivalente a, $(t_1, \ldots, t_n) \in P^B$ per come abbiamo definito l'interpretazione di P nella struttura A. Infine $(t_1, \ldots, t_n) \in P^B$ vale se, e solo se, vale $S \vdash P(t_1, \ldots, t_n)$ per la definizione di B.

Vediamo quindi il passo induttivo, distinguendo tre casi.

Caso 1: φ coincide con $\neg\psi$. Si ha $A \models \neg\psi$ se, soltanto se, $A \not\models \psi$. Per ipotesi di induzione l'ultima asserzione è valida se, e solo se, $S \nvdash \psi$ e, poiché S è massimalmente coerente, per il Punto 1 del Lemma 4.55 questo vale se, e solo se, $S \vdash \varphi$.

Caso 2: φ coincide con $\varphi_1 \wedge \varphi_2$. Si ha allora $A \models \varphi_1 \wedge \varphi_2$ se e soltanto se $A \models \varphi_1$ e $A \models \varphi_2$. Per ipotesi induttiva l'ultima asserzione è valida se, e solo se, $S \vdash \varphi_1$ e $S \vdash \varphi_2$, poiché S è massimalmente coerente, per il Punto 2 del Lemma 4.55 questo vale se, e solo se, $S \vdash \varphi_1 \wedge \varphi_2$.

Caso 3: φ coincide con $\exists x\psi(x)$. Poiché φ è chiusa, x è l'unica variabile libera in ψ. Supponiamo che $A \models \exists x\psi(x)$ allora per definizione si ha che per ogni valutazione v esiste $a \in A$ tale che $A, v[a/x] \models \psi(x)$. Poiché $a \in A$, sarà $a = [t]$ per qualche termine chiuso t. Allora $A \models \psi[t/x]$, dove t è ovviamente sostituibile per x in φ perché è chiuso. Quindi per ipotesi induttiva $S \vdash \psi[t/x]$ e quindi applicando la regola $I\exists$, otteniamo $S \vdash \exists x\psi[x]$. Viceversa, supponiamo $S \vdash \exists x\psi[x]$. Siccome S è Henkin, $\exists x\psi(x) \to \psi(c_\psi) \in S$ e quindi applicando la regola $E \to$ otteniamo $S \vdash \psi(c_\psi)$. Per ipotesi induttiva allora $A \models \psi(c_\psi)$ e siccome c_ψ è un termine chiuso, questo implica che per ogni interpretazione v, esiste $a \in A$ tale che $A, v[a/x] \models \psi(x)$ da cui otteniamo $A \models \exists x\psi(x)$.

Concludendo, A è un modello per S. Poiché S estende T, il teorema è dimostrato. □

Teorema 4.57 (Completezza del calcolo dei predicati)

Sia $\Gamma \cup \{\varphi\}$ un insieme di enunciati. Si ha

$$\Gamma \vdash \varphi \quad \textit{se, e solo se,} \quad \Gamma \models \varphi.$$

Dimostrazione. Un implicazione è stata dimostrata nel Teorema 4.41, vediamo l'altra. Ragioniamo sulla contronominale e quindi supponiamo che $\Gamma \nvdash \varphi$. Per il Lemma 4.44, $\Gamma \cup \{\neg\varphi\}$ è coerente, quindi il Lemma 4.56 garantisce l'esistenza di un modello A per $\Gamma \cup \{\neg\varphi\}$. Pertanto, A è un modello di Γ tale che $A \not\models \varphi$, da ciò possiamo concludere che $\Gamma \not\models \varphi$. □

Per stabilire i risultati della prossima sezione sarà utile "contare" gli elementi del modello A costruito durante la dimostrazione del Lemma 4.56. Per farlo in maniera generale, abbandoniamo l'ipotesi semplificativa che la cardinalità del linguaggio sia numerabile.

Teorema 4.58 (Esistenza dei modelli)

Se Γ è un insieme coerente di enunciati in un linguaggio tale che $|\mathtt{VarX}| = \aleph_0$ e che $\mathcal{L} = (f_1 \dots, f_u, P_1, \dots, P_v, \{c_i\}_{i \in K})$ con $u, v \in \mathbb{N}$ e $|K| = \mu$. Allora, ponendo $\kappa := \max\{\aleph_0, \mu\}$, Γ ammette un modello di cardinalità al più κ.

Dimostrazione. L'esitenza del modello è garantita dal Lemma 4.56. Per stabilire la cardinalità di tale modello A occorre stabilire la cardinalità dei termini chiusi nel linguaggio $\overline{\mathcal{L}}$, visto che l'essere passati da $\overline{T}$ a S non ha modificato il linguaggio. Vediamo inizialmente quanti termini è possibile costruire nel linguaggio $\mathcal{L}$.

Si noti che l'assioma della scelta implica che, se α e β sono due cardinali, allora $\alpha + \beta = \alpha \cdot \beta = \max\{\alpha, \beta\}$.

Definiamo:

$$\begin{aligned} \mathtt{Term}_0 &:= \{c \mid c \text{ simbolo di constante in } \mathcal{L}\} \cup \mathtt{VarX}, \\ \mathtt{Term}_{n+1} &:= \mathtt{Term}_n \cup \{f(t_1, \dots, t_m) \mid f \text{ simbolo di funzione in } \mathcal{L} \text{ e } t_1, \dots, t_m \in \mathtt{Term}_n\} \end{aligned}$$

Allora si vede facilmente che $\mathtt{Term} = \bigcup_{n \in \mathbb{N}} \mathtt{Term}_n$. Mostriamo per induzione che $|\mathtt{Term}_n| \leqslant \kappa$ per ogni $n \in \mathbb{N}$. Infatti $|\mathtt{Term}_0| = |K| + \aleph_0 = \mu + \aleph_0 = \kappa$. Supponiamo ora che $|\mathtt{Term}_n| \leqslant \kappa$ e mostriamo che $|\mathtt{Term}_{n+1}| \leqslant \kappa$. Si ha che

$$|\mathtt{Term}_{n+1}| = \sum_{f_1}^{f_u} |\{f_i(t_1, \dots, t_m) \mid t_1, \dots, t_m \in \mathtt{Term}_n\}| = \sum_{a_1}^{a_u} |\mathtt{Term}_n|^{a_i}$$

dove a_i corrisponde all'arietà di f_i per $i \leqslant u$. Sia $a := \max\{a_1, \dots, a_u\}$ Dunque $|\mathtt{Term}_{n+1}| \leqslant u \cdot \kappa^a = \kappa$. Quindi $|\mathtt{Term}| \leqslant \aleph_0 \cdot \kappa = \kappa$.

Definiamo ora

$$\begin{aligned} \mathtt{Form}\forall_0 &:= \{P(t_1, \dots, t_m) \mid P \text{ simbolo di predicato in } \mathcal{L} \text{ e } t_1, \dots t_m \in \mathtt{Term}\}, \\ \mathtt{Form}\forall_{n+1} &:= \mathtt{Form}\forall_n \cup \{\varphi_1 \wedge \varphi_2, \neg\varphi_1, \forall x \varphi_1 \mid \varphi_1, \varphi_2 \in \mathtt{Form}\forall_n\}. \end{aligned}$$

Allora si vede facilmente che $\mathtt{Form}\forall = \bigcup_{n \in \mathbb{N}} \mathtt{Form}\forall_n$e, come nel caso precedente, si ha $|\mathtt{Form}\forall| \leqslant \kappa$.

Possiamo vedere che l'insieme delle formule del tipo $\exists x \varphi(x)$ ha cardinalità κ. Infatti, per quanto visto prima sicuramente la sua cardinalità è minore o uguale a κ e inoltre il sottoinsieme di formule $\{\exists x(x = c) \mid c \text{ simbolo di costante in } \mathcal{L}\}$ ha almeno cardinalità κ.

Ora analizziamo come cresce la cardinalità del linguaggio prendendo le estensioni Henkin definite nella Definizione 4.50. Per quanto visto sopra la cardinalità delle costanti in $\mathcal{L}^H$ è κ e quindi $\mathcal{L}^H$ ha κ termini e κ enunciati, quindi $\overline{\mathcal{L}}$ ha $\aleph_0 \cdot \kappa = \kappa$ termini e enunciati. Possiamo quindi concludere che i termini chiusi di $\overline{L}$ sono κ e dunque gli elementi di A, che corrispondono alle classi di equivalenza dei termini di $\overline{L}$, sono al più κ. $\square$

Concludiamo questa sezione osservando che il teorema di Completezza del calcolo dei predicati implica immediatamente la *compattezza* della logica del prim'ordine. Tuttavia, nella sezione Sezione 4.5 daremo una dimostrazione diretta di questo teorema sfruttando la costruzione degli ultraprodotti.

Corollario 4.59 (Compattezza della logica del prim'ordine)**.** *Sia* $\Gamma \cup \{\varphi\}$ *un insieme di formule. Si ha che* $\Gamma \models \varphi$ *se e soltanto se esiste un sottoinsieme finito* $\Delta \subseteq \Gamma$ *tale che* $\Delta \models \varphi$*.*

Dimostrazione. L'implicazione da sinistra verso destra è banale, perché, com'è semplice verificare applicando la definizione di conseguenza logica, aggiungendo formule a un insieme le sue conseguenze logiche non diminuiscono. Per il viceversa, supponiamo $\Gamma \models \varphi$. Per il teorema di Completezza del calcolo dei predicati allora vale $\Gamma \vdash \varphi$, ma le derivazioni sono oggetti finiti, quindi la derviazione di φ usa un numero finito di ipotesi in Γ, chiamando tale insieme di formule Δ si ha che $\Delta \vdash \varphi$. Usando un'altra volta il teorema di Completezza del calcolo dei predicati si ottiene che $\Delta \models \varphi$, come desiderato. $\square$

4.5 ULTRAPRODOTTI E COMPATTEZZA DELLA LOGICA DEL PRIM'ORDINE.

Definizione 4.60

Date due $\mathcal{L}$-strutture A e B, diremo che una funzione $h\colon A \to B$ è un **omomorfismo** se:

1. per ogni simbolo di costante c in $\mathcal{L}$, si ha $h(c^A) = c^B$,
2. per ogni simbolo di funzione f in $\mathcal{L}$ di arietà n si ha $h(f^A(a_1,\dots,a_n)) = f^B(h(a_1),\dots,h(a_n))$,
3. per ogni simbolo di predicato P in $\mathcal{L}$ di arietà m, si ha che se $(a_1,\dots,a_m) \in P^A$ allora $(h(a_1),\dots,h(a_m)) \in P^B$.

Definizione 4.61

Date due strutture nello stesso linguaggio A e B diremo che sono **elementarmente equivalenti**, in simboli $A \equiv B$, se per ogni enunciato φ si ha

$$A \models \varphi \text{ se, soltanto se, } B \models \varphi.$$

Definizione 4.62

Date due strutture nello stesso linguaggio A e B diremo che A è una **sottostruttura elementare** di B (o equivalentemente che B è un'**estensione elementare** di A), in simboli $A \preceq B$, se $A \subseteq B$ e per ogni formula $\varphi(x_1, \ldots, x_n)$ e per ogni tupla $a_1, \ldots, a_n \in A$ si ha

$$A \models \varphi(a_1, \ldots, a_n) \text{ se, soltanto se, } B \models \varphi(a_1, \ldots, a_n).$$

Se esiste un isomorfismo f tra C ed A e $A \preceq B$ allora diremo che C è elementarmente immergibile in B. Detta ι la mappa che immerge A in B, chiameremo la mappa $\iota \circ f$ **immersione elementare**.

È immediato, ma importante, osservare che $A \preceq B$ implica $A \equiv B$, ma non viceversa.

In questa sezione introdurremo una costruzione che permette di creare estensioni elementari di più strutture alla volta.

Per costruire un ultraprodotto partiamo da una famiglia di $\mathcal{L}$-strutture $\{A_i \mid i \in I\}$ indicizzate da qualche insieme I. Il primo passo è costruire il prodotto diretto di tali strutture, si noti che tale costruzione ha senso qualsiasi sia il linguaggio $\mathcal{L}$.

Definizione 4.63

Data una famiglia di $\mathcal{L}$-strutture $\{A_i \mid i \in I\}$, definiamo il **prodotto diretto** delle A_i, in simboli $A = \prod_{i \in I} A_i$ come la struttura il cui supporto è dato dal prodotto cartesiano $\bigtimes_{i \in I} A_i$ e

a) per ogni simbolo di costante c in $\mathcal{L}$, $c^A := (c^{A_i} \mid i \in I)$;

b) per ogni simbolo di funzione f in $\mathcal{L}$, il valore di f^A su una n-upla arbitraria $(\bar{a}_1, \ldots, \bar{a}_n)$ con $\bar{a}_j = (a_{ij} \mid i \in I)$ è dato da $f^A(\bar{a}_1, \ldots, \bar{a}_n) := (f^{A_i}(a_{i1}, \ldots, a_{in}) \mid i \in I)$;

c) per ogni simbolo di predicato P in $\mathcal{L}$, $P^A(\bar{a}_1, \ldots, \bar{a}_n)$ vale se, e soltanto se, $P^{A_i}(a_{i1}, \ldots, a_{in})$ vale per ogni $i \in I$.

Si noti che per ogni $i \in I$ c'è una **proiezione canonica** (=funzione suriettiva canonica) π_i definita su $A = \prod_{i \in I} A_i$ come $\pi_i(\bar{a}) := a_i$.

Se $\mathcal{F}$ è una famiglia di sottoinsiemi di I ha senso definire la relazione su $A = \prod_{i \in I} A_i$

$$\bar{a} \sim_{\mathcal{F}} \bar{b} \text{ se, soltanto se, } \{i \in I \mid \pi_i(\bar{a}) = \pi_i(\bar{b})\} \in \mathcal{F} \tag{22}$$

Affinché la relazione $\sim_{\mathcal{F}}$ si comporti bene rispetto alla struttura di A è ovvio che sarà necessario imporre delle restrizioni su $\mathcal{F}$.

Notazione 4.64. Se I è un qualsiasi insieme chiameremo **filtro** (o rispettivamente **ultrafiltro**) su I un filtro (o rispettivamente ultrafiltro) sull'algebra di Boole $\langle \wp(I), \cap, \cup, {}^c, \emptyset, I\rangle$, nel senso della Definizione 3.78.

Lemma 4.65. *Se $\mathcal{F}$ è un filtro su I allora $\sim_{\mathcal{F}}$ è una relazione di equivalenza su $\prod_{i\in I} A_i$.*

Dimostrazione. Esercizio. □

Lemma 4.66. *Se $\mathcal{F}$ è un filtro su I allora $\sim_{\mathcal{F}}$ è una $\mathcal{L}$-congruenza su $\prod_{i\in I} A_i$. In altre parole,*

a) per ogni simbolo di funzione f di arietà n in $\mathcal{L}$ si ha che se $\bar{a}_1 \sim_{\mathcal{F}} \bar{b}_1, \dots, \bar{a}_n \sim_{\mathcal{F}} \bar{b}_n$ allora $f(\bar{a}_1, \dots, \bar{a}_n) \sim_{\mathcal{F}} f(\bar{b}_1, \dots, \bar{b}_n)$;

b) per ogni simbolo di predicato di arietà m P in $\mathcal{L}$ si ha che se $\bar{a}_1 \sim_{\mathcal{F}} \bar{b}_1, \dots, \bar{a}_m \sim_{\mathcal{F}} \bar{b}_m$ e $\{i \mid P^{A_i}(\pi_i(\bar{a}_1), \dots, \pi_i(\bar{a}_m))\} \in \mathcal{F}$ allora $\{j \mid P^{A_j}(\pi(\bar{b}_1), \dots, \pi_i(\bar{b}_m))\} \in \mathcal{F}$.

Dimostrazione. Esercizio. □

I due precedenti lemmi danno senso alla seguente definizione.

Definizione 4.67

Data una famiglia di $\mathcal{L}$-strutture $\{A_i \mid i \in I\}$ e un ultrafiltro $\mathcal{F}$ su I, definiamo l'**ultraprodotto** delle A_i, in simboli $A \coloneqq \prod_{i\in I} A_i/\mathcal{F}$ come la struttura il cui supporto è dato dal quoziente del prodotto cartesiano $\bigtimes_{i\in I} A_i/\sim_{\mathcal{F}}$ e

1. per ogni simbolo di costante c in $\mathcal{L}$, definiamo $c^A = [(c^{A_i} \mid i \in I)]_{\sim_{\mathcal{F}}}$ (la classe di equivalenza modulo la relazione $\sim_{\mathcal{F}}$);
2. per ogni simbolo di funzione f di arietà n in $\mathcal{L}$, il valore di f^A su un'arbitraria n-upla $[\bar{a}_1]_{\sim_{\mathcal{F}}}, \dots, [\bar{a}_n]_{\sim_{\mathcal{F}}}$ è definito da $[f^A([\bar{a}_1]_{\sim_{\mathcal{F}}}, \dots, [\bar{a}_n]_{\sim_{\mathcal{F}}})]_{\sim_{\mathcal{F}}} \coloneqq [(f^{A_i}(\pi_i(\bar{a}_1), \dots, \pi_i(\bar{a}_n))]_{\sim_{\mathcal{F}}}$;
3. per ogni simbolo di predicato P di arietà m in $\mathcal{L}$, $P^A([\bar{a}_1]_{\sim_{\mathcal{F}}}, \dots, [\bar{a}_m]_{\sim_{\mathcal{F}}})$ vale se, e soltanto se, $\{i \in I \mid P^{A_i}(\pi_i(\bar{a}_1), \dots, \pi_i(\bar{a}_m))\} \in \mathcal{F}$.

Se tutte le strutture A_i sono tutte isomorfe, l'ultraprodotto appena definito è detto **ultrapotenza**.

È chiaro dalla costruzione appena definita che l'ultraprodotto $\prod_{i\in I} A_i/\mathcal{F}$ è una struttura appropriata per lo stesso linguaggio delle A_i. Quindi ha senso chiedersi come sia collegata la verità delle formule del prim'ordine nell'ultraprodotto e nelle strutture di partenza. Il teorema di Łoš qui sotto, dà una risposta completa a questa domanda.

Per capire come sono collegate le interpretazioni nelle A_i con le interpretazioni in $\prod_{i\in I} A_i/\mathcal{F}$, per un arbitrario $\mathcal{F}$, si noti che se $\{\nu_i \mid i \in I\}$ è una famiglia di interpretazioni, dove per ogni $i \in I$, $\nu_i \colon \mathsf{Var} \to A_i$, allora si può costruire un'interpretazione $\prod \nu_i$ in $\prod_{i\in I} A_i/\mathcal{F}$ ponendo, per ogni $x \in \mathsf{Var}$, $\nu(x) \coloneqq [(\nu_i(x) \mid i \in I)]_{\sim_{\mathcal{F}}}$.

Teorema 4.68 (Łoš)

Sia $(\mathsf{A}_i \mid i \in I)$ *una famiglia di strutture nello stesso linguaggio del prim'ordine* $\mathcal{L}$ *e sia* $\mathcal{F}$ *un ultrafiltro su* I. *Sia* $\mathsf{A} := \prod_{i \in I} \mathsf{A}_i/\mathcal{F}$ *l'ultraprodotto della* A_i. *Per ogni* $\mathcal{L}$*-formula e per ogni famiglia di interpretazioni* $\{v_i \mid i \in I\}$, *con* $v_i \colon \mathsf{Var} \to \mathsf{A}_i$ *per* $i \in I$, *si ha*

$$\mathsf{A}, \prod v_i \models \varphi \text{ se, soltanto se, } \{i \in I \mid \mathsf{A}_i, v_i \models \varphi\} \in \mathcal{F}.$$

Dimostrazione. La dimostrazione è per induzione sulla complessità di φ. Se φ è atomica della forma $t_1 = t_2$, supponiamo che $\tilde{v}(t_1) = [\bar{a}_1]_{\sim_\mathcal{F}}$ e $\tilde{v}(t_2) = [\bar{a}_2]_{\sim_\mathcal{F}}$, allora abbiamo:

$$\begin{aligned}
\mathsf{A}, v \models \varphi &\Leftrightarrow [\bar{a}_1]_{\sim_\mathcal{F}} = [\bar{a}_2]_{\sim_\mathcal{F}} \Leftrightarrow \bar{a}_1 \sim_\mathcal{F} \bar{a}_2 \\
&\Leftrightarrow \{i \in I \mid \pi_i(\bar{a}_1) = \pi_i(\bar{a}_2)\} \in \mathcal{F} && \text{per la Equazione (22)} \\
&\Leftrightarrow \{i \in I \mid \mathsf{A}_i \models \tilde{v}_i(t_1) = \tilde{v}_i(t_2)\} \in \mathcal{F} && \text{per Definizione 4.21, Punto 1.}
\end{aligned}$$

Se φ è atomica della forma $\mathsf{P}(t_1, \ldots, t_n)$, supponiamo che $\tilde{v}(t_j) = [\bar{a}_j]_{\sim_\mathcal{F}}$ per ogni $1 \leqslant j \leqslant n$, allora abbiamo:

$$\begin{aligned}
\mathsf{A}, v \models \varphi &\Leftrightarrow \mathsf{P}^\mathsf{A}(\tilde{v}(t_1), \ldots, \tilde{v}(t_n)) \text{ vale in } \mathsf{A} \\
&\Leftrightarrow \{i \in I \mid \mathsf{P}^\mathsf{A}(\pi_i(\bar{a}_1), \ldots, \pi_i(\bar{a}_n)\} \in \mathcal{F} && \text{per Definizione 4.67, Punto 3,} \\
&\Leftrightarrow \{i \in I \mid \mathsf{A}_i, v \models \mathsf{P}(t_1, \ldots, t_n)\} \in \mathcal{F} && \text{per Definizione 4.21, Punto 1.}
\end{aligned}$$

Supponiamo ora che l'asserto valga per tutte le formule di complessità inferiore a n e supponiamo che φ abbia complessità uguale ad n, allora abbiamo i seguenti casi:

- $\varphi = \varphi_1 \wedge \varphi_2$. Allora φ_1 e φ_2 hanno complessità inferiore a n e dunque per loro vale l'ipotesi induttiva. Si ha allora

$$\begin{aligned}
\mathsf{A}, v \models \varphi_1 \wedge \varphi_2 &\Leftrightarrow \mathsf{A}, v \models \varphi_1 \text{ e } \mathsf{A}, v \models \varphi_2 \\
&\Leftrightarrow \{i \in I \mid \mathsf{A}_i, v_i \models \varphi_1\} \in \mathcal{F} \text{ e } \{i \in I \mid \mathsf{A}_i, v_i \models \varphi_2\} \in \mathcal{F} \\
&\qquad \text{per ipotesi induttiva} \\
&\Leftrightarrow \{i \in I \mid \mathsf{A}_i, v_i \models \varphi_1\} \cap \{i \in I \mid \mathsf{A}_i, v_i \models \varphi_2\} \in \mathcal{F} \\
&\qquad \text{perché } \mathcal{F} \text{ è un filtro,} \\
&\Leftrightarrow \{i \in I \mid \mathsf{A}_i, v_i \models \varphi_1 \text{ e } \mathsf{A}_i, v_i \models \varphi_2\} \in \mathcal{F} \\
&\qquad \text{per le proprietà insiemistiche} \\
&\Leftrightarrow \{i \in I \mid \mathsf{A}_i, v_i \models \varphi_1 \wedge \varphi_2\} \in \mathcal{F} \\
&\qquad \text{per Definizione 4.21, Punto 3.}
\end{aligned}$$

- $\varphi = \neg\varphi_1$. Allora φ_1 ha complessità inferiore a n e dunque per essa vale l'ipotesi induttiva. Si ha allora

$$\begin{aligned} A, \nu \models \neg\varphi_1 &\Leftrightarrow A, \nu \not\models \varphi_1 \\ &\Leftrightarrow \{i \in I \mid A_i, \nu_i \models \varphi_1\} \notin \mathcal{F} && \text{per ipotesi induttiva} \\ &\Leftrightarrow \{i \in I \mid A_i, \nu_i \not\models \varphi_1\} \in \mathcal{F} && \text{per Lemma 3.79, Punto 3} \\ &\Leftrightarrow \{i \in I \mid A_i, \nu_i \models \neg\varphi_1\} \in \mathcal{F} && \text{per Definizione 4.21, Punto 2.} \end{aligned}$$

- $\varphi = \exists x \varphi_1(x)$. Definiamo

$$D \coloneqq \{i \in I \mid A_i, \nu_i \models \exists x \varphi_1(x)\}$$

Osserviamo che, poiché φ_1 ha complessità inferiore a n, per essa vale l'ipotesi induttiva. Si ha allora

$$\begin{aligned} A, \nu \models \exists x \varphi_1(x) \Leftrightarrow\ & \text{esiste } \bar{a} \in \bigtimes_{i \in I} A_i \text{ tale che } A, \nu \left[{}^{[\bar{a}]_{\sim_{\mathcal{F}}}}\!/_{x}\right] \models \varphi_1(x) \\ \Leftrightarrow\ & \text{esiste } \bar{a} \in \bigtimes_{i \in I} A_i, \text{ tale che} \\ & \{i \in I \mid A_i, \nu_i \left[{}^{\pi_i(\bar{a})}\!/_{x}\right] \models \varphi_1(x)\} \in \mathcal{F} \end{aligned}$$

per ipotesi induttiva. Per concludere la dimostrazione basta far vedere che

$$\left\{i \in I \mid A_i, \nu_i \left[{}^{\pi_i(\bar{a})}\!/_{x}\right] \models \varphi_1(x)\right\} = \{i \in I \mid A_i, \nu_i \models \exists x \varphi_1(x)\} = D.$$

L'inclusione da sinistra verso destra è banale. Viceversa, se $i \in D$ si ha $A_i, \nu_i \models \exists x \varphi_1(x)$, dunque per ogni $i \in D$ esiste $b_i \in A_i$ tale che $A_i, \nu_i[b_i/x] \models \varphi_1(x)$. Grazie all'assioma di scelta è possibile formare una sequenza $\bar{c} = (c_i \mid i \in I)$, tale che per ogni $i \in D$ si ha $A_i, \nu_i[c_i/x] \models \varphi_1(x)$. Si ha dunque che $D \subseteq \{i \in I \mid A_i, \nu_i[\pi(\bar{c})/x] \models \varphi_1(x)\}$. Questo conclude la dimostrazione.

□

Sia $(A_i \mid i \in I)$ una famiglia di copie isomorfe di A e $\mathcal{F}$ un ultrafiltro su I. Sia a^* la sequenza nel prodotto delle A_i tale che $\pi_i(a^*) = a$ per ogni $i \in I$. Definiamo una mappa $d \colon A \to \prod_{i \in I} A_i/\mathcal{F}$ ponendo $d(a) = [a^*]_\sim$; tale mappa è detta **immersione canonica**.

Corollario 4.69. *L'immersione canonica è un'immersione elementare di A in $A^I/\mathcal{F}$.*

Corollario 4.70. *Se $(A_i \mid i \in I)$ è una famiglia di copie isomorfe di A e $\mathcal{F}$ un ultrafiltro su I allora $A \equiv \prod_{i \in I} A_i/\mathcal{F}$.*

Concludiamo questo excursus con un'applicazione della costruzione appena vista per dare una dimostrazione del Teorema di Compattezza indipendente dal Teorema di Completezza.

Teorema 4.71 (Compattezza della logica del prim'ordine)

Un insieme Γ di formule del prim'ordine ha un modello se, e soltanto se, ogni suo sottoinsieme finito ha un modello.

Dimostrazione. Se Γ ha un modello, questo è banalmente un modello per ogni suo sottoinsieme finito. Vediamo quindi l'altra implicazione.

Supponiamo che ogni sottoinsieme finito $\Delta \subseteq \Gamma$ abbiamo un modello, e sia

$$I \coloneqq \{\Delta \subseteq \Gamma \mid \Delta \text{ è finito}\}.$$

Per ogni sottoinsieme $\Delta \in I$, sia M_Δ un modello fissato, che esiste per ipotesi. In simboli, $M_\Delta \models \Delta$. Per ogni $\Delta \in I$, consideriamo la sua *estensione* Δ^* definita dagli elementi di I che contengono Δ. Questo sarà un insieme di elementi di I e quindi un elemento dell'algebra di Boole $\wp(I)$. In simboli,

$$\Delta^* \coloneqq \{\Theta \in I \mid \Delta \subseteq \Theta\} \in \wp(I).$$

Nell'algebra di Boole $\wp(I)$ possiamo definire il sottoinsieme

$$\mathrm{Ext} \coloneqq \{\Delta^* \mid \Delta \in I\} \subseteq \wp(I).$$

Vediamo che Ext ha la FIP. Infatti, per ogni coppia $\Delta_1^*, \Delta_2^* \in \mathrm{Ext}$ si ha che il sottoinsieme finito di Γ dato dall'unione $\Delta_1 \cup \Delta_2$ è una estensione di entrambi Δ_1 e Δ_2, quindi $\Delta_1 \cup \Delta_2 \in \Delta_1^* \cap \Delta_2^*$, dunque l'intersezione non è vuota.

Di conseguenza, per Corollario 3.83, esiste un ultrafiltro U di $\wp(I)$ che contiene Ext. Consideriamo allora l'ultraprodotto $M = \prod_{\Delta \in I} M_\Delta / U$. Vediamo che M è un modello per Γ, cioè $M \models \varphi$ per ogni $\varphi \in \Gamma$.

Per ogni $\varphi \in \Gamma$, sia $\{\varphi\}^*$ la sua estensione. Per definizione di estensione, $\{\varphi\}^* = \{\Delta \in I \mid \varphi \in \Delta\} \in \mathrm{Ext} \subseteq U$. Inoltre, per ogni sottoinsieme $\Delta \in I$, se $\varphi \in \Delta$ allora $M_\Delta \models \varphi$. Ne ricaviamo che $\{\varphi\}^* \subseteq \{\Delta \in I \mid M_\Delta \models \varphi\}$. Poiché U è un filtro $\{\Delta \in I \mid M_\Delta \models \varphi\} \in U$. Segue dal Teorema 4.68 che $M \models \varphi$ e il teorema è dimostrato. □

Esercizio 4.72. Mostrare che gli enunciati del Corollario 4.59 e del Teorema 4.71 sono equivalenti.

4.6 APPLICAZIONI DEI TEOREMI DI COMPLETEZZA E COMPATTEZZA.

Teorema 4.73 (Löwenheim-Skolem all'ingiù)

Sia Γ un insieme di enunciati in un linguaggio $\mathcal{L}$ tale che $|\mathcal{L}| = \kappa$. Se Γ ha un mo-

dello di cardinalità infinita $\lambda > \kappa$, allora Γ ha modelli di ogni cardinalità κ' tale che $\max\{\kappa, \aleph_0\} \leqslant \kappa' \leqslant \lambda$.

Dimostrazione. Sia κ' tale che $\max\{\kappa, \aleph_0\} \leqslant \kappa' \leqslant \lambda$. Aggiungiamo al linguaggio di Γ un insieme di nuove costanti $\{c_i \mid i \in I\}$ di cardinalità κ' e consideriamo $\Gamma' \coloneqq \{c_i \neq c_j \mid i \neq j\}$. Per ipotesi Γ ha un modello A di cardinalità λ, estendiamo A per interpretare tutte le nuove costanti c_i. Siccome $\lambda \geqslant \kappa'$, tutte le costanti possono essere interpretate in elementi diversi e dunque A è un modello anche di Γ'. Ciò implica che Γ' è coerente. Notiamo che il linguaggio di Γ' ha cardinalità κ'. Quindi per il Teorema 4.58 Γ' ha un modello di cardinalità al più κ'. Inoltre, siccome in questo modello sono veri tutti gli assiomi aggiuntivi di Γ' della forma $c_i \neq c_j$ il modello deve avere cardinalità maggiore o uguale a κ'. Ne segue che il modello ha cardinalità esattamente uguale a κ'. □

Esempio 4.74. Sia Γ l'insieme degli enunciati validi in $\mathbb{R}$ nel linguaggio del prim'ordine $(+, \cdot, -, 0, 1)$. Allora, per il teorema di Löwenheim-Skolem all'ingiù Γ ha un modello di cardinalità $\aleph_0$.

Esempio 4.75 (Paradosso di Skolem)**.** Sia Γ l'insieme degli assiomi della teoria degli insiemi (ad esempio quelli di ZF). Se Γ ha un modello, allora per il teorema di Löwenheim-Skolem all'ingiù, ha un modello di cardinalità $\aleph_0$. La situazione è paradossale perché in teoria degli insiemi è possibile dimostrare l'esistenza di insiemi più che numerabili, ma per quanto appena dimostrato essi dovrebbero essere all'interno di un modello enumerabile. Tuttavia, questa non è una contraddizione, il punto chiave è che l'*enumerabilità* vista dall'interno del modello non è la stessa di quella vista dall'esterno. In altre parole, per dimostrare che un insieme è enumerabile, bisogna trovare una biezione con i numeri naturali. Nella situazione in cui ci troviamo, il modello è così debole da non accorgersi di alcune biezioni.

Teorema 4.76 (Löwenheim-Skolem all'insù)

Sia Γ un insieme di enunciati in un linguaggio $\mathcal{L}$ tale che $|\mathcal{L}| = \kappa$. Se Γ ha un modello infinito, allora Γ ha un modello di cardinalità κ' per ogni $\kappa' \geqslant$ $\max(\aleph_0, \kappa)$.

Dimostrazione. Aggiungiamo al linguaggio di Γ un insieme di nuove costanti $\{c_i \mid i \in I\}$ di cardinalità κ' e consideriamo $\Gamma' \coloneqq \{c_i \neq c_j \mid i \neq j\}$. Dimostriamo che Γ' è finitamente soddisfacibile. Sia $\Delta \subseteq \Gamma'$ un insieme finito. L'insieme Δ conterrà allora un numero finito di assiomi riguardanti le nuove costanti, quindi $\Delta = \Gamma_0 \cup \{c_i \neq c_j \mid i, j \leqslant p \text{ e } i \neq j\}$ dove Γ_0 è un sottoinsieme finito di Γ e $p \in \mathbb{N}$. Per ogni siffatto Δ possiamo espandere il modello di Γ dato dalle ipotesi per interpretare i nuovi simboli di constante c_i con $i \leqslant p$ in elementi distinti del modello (perché le costanti sono in numero finito), dunque Γ' è finitamente soddisfacibile. Per la Compattezza della logica del prim'ordine, Γ' ammette un modello B. Poiché B deve interpretare κ' variabili in elementi distinti, esso avrà cardinalità almeno κ'. Possiamo ora applicare il Löwenheim-Skolem all'ingiù per ottenere un modello di Γ' che ha cardinalità esattamente κ'. Ovviamente, tale modello sarà anche un modello di Γ e ciò conclude la dimostrazione. $\square$

Vediamo ora alcune conseguenze dei teoremi appena dimostrati.

Lemma 4.77. *Se un insieme di enunciati Γ ha modelli finiti di cardinalità arbitraria, allora Γ ha un modello infinito*

Dimostrazione. Sia ε_n la seguente formula del prim'ordine:

$$\varepsilon_n := \exists x_1 \exists x_2 \dots \exists x_n \left(\bigwedge_{i \neq j, i,j \leqslant n} (x_i \neq x_j) \right). \tag{23}$$

È facile vedere che ε_n vale esattamente nei modelli che hanno almeno n elementi. Consideriamo l'insieme di enunciati $\Gamma' := \Gamma \cup \{\varepsilon_n \mid n \in \mathbb{N}\}$. Per l'ipotesi, ogni sottoinsieme finito di Γ' è soddisfacibile, dunque per la Compattezza della logica del prim'ordine Γ' ha un modello. Questo modello deve necessariamente essere infinito perché soddisfa ε_n per ogni $n \in \mathbb{N}$. $\square$

Definizione 4.78

Una classe di strutture $\mathcal{K}$ è detta **assiomatizzabile** o **elementare** se esiste un insieme di formule Σ tale che $\mathcal{K} = \mathrm{Mod}(\Sigma)$. Se Σ è finito diremo che $\mathcal{K}$ è **finitamente assiomatizzabile**.

Corollario 4.79. *Sia $\mathcal{K}$ una classe di strutture con modelli finiti di cardinalità arbitraria. Allora la classe $\mathcal{K}_{fin}$ delle strutture finite in $\mathcal{K}$ non è elementare.*

Dimostrazione. Se esistesse Σ insieme di enunciati tali che $A \in \mathrm{Mod}\,\Sigma$ se e soltanto se $A \in \mathcal{K}_{\mathrm{fin}}$, allora $\mathrm{Mod}\,\Sigma$ avrebbe modelli finiti di cardinalità arbitraria, dunque per il Lemma 4.77 avrebbe anche modelli infiniti. $\square$

Il contenuto del Corollario 4.79 è spesso enunciato dicendo che la finitezza non è una nozione esprimibile al prim'ordine.

Lemma 4.80. *Se $\mathcal{K} = \mathrm{Mod}(\Sigma)$ e $\mathcal{K}$ è finitamente assiomatizzabile, allora esiste un sottoinsieme finito $\Delta \subseteq \Sigma$ tale che $\mathcal{K} = \mathrm{Mod}(\Delta)$.*

Dimostrazione. Sia $\mathcal{K} = \mathrm{Mod}(\Psi)$ con Ψ finito. Sia ψ la congiunzione di tutte le formule in Ψ (ψ è una formula ben formata perché Ψ è finito). Poiché i modelli di Σ sono gli stessi di Ψ abbiamo che $\Sigma \models \psi$ e dunque, per il teorema di Compattezza della logica del prim'ordine devono esistere $\varphi_1, \dots, \varphi_m$ tali che $\{\varphi_1, \dots, \varphi_m\} \models \psi$. Ora abbiamo:

$$\begin{aligned} &\{\varphi_1, \dots, \varphi_m\} \subseteq \Sigma && \text{e quindi } \mathcal{K} = \mathrm{Mod}(\Sigma) \subseteq \mathrm{Mod}(\{\varphi_1, \dots, \varphi_m\}), \\ &\{\varphi_1, \dots, \varphi_m\} \models \psi && \text{e quindi } \mathrm{Mod}(\{\varphi_1, \dots, \varphi_m\}) \subseteq \mathrm{Mod}(\psi) = \mathcal{K}. \end{aligned}$$

Dunque possiamo concludere che $\mathrm{Mod}(\{\varphi_1, \ldots, \varphi_m\}) = \mathcal{K}$. □

Lemma 4.81. *Una classe di strutture $\mathcal{K}$ è finitamente assiomatizzabile se e soltanto se sia $\mathcal{K}$ che il suo complemento $\mathcal{K}^c$ sono assiomatizzabili.*

Dimostrazione. Per l'implicazione da sinistra verso destra basta osservare che se $\mathcal{K} = \mathrm{Mod}(\varphi_1, \ldots, \varphi_m)$, allora $\mathcal{K} = \mathrm{Mod}(\varphi_1 \wedge \cdots \wedge \varphi_m)$ e quindi $\mathcal{K}^c = \mathrm{Mod}(\neg(\varphi_1 \wedge \cdots \wedge \varphi_m))$.

Viceversa sia $\mathcal{K} = \mathrm{Mod}(\Sigma)$ e $\mathcal{K}^c = \mathrm{Mod}(\Delta)$. Allora $\emptyset = \mathcal{K} \cap \mathcal{K}^c = \mathrm{Mod}(\Sigma \cup \Delta)$. Per la Compattezza della logica del prim'ordine devono esistere $\sigma_1, \ldots, \sigma_n \in \Sigma$ e $\delta_1, \ldots, \delta_m \in \Delta$ tali che $\mathrm{Mod}(\sigma_1, \ldots, \sigma_n, \delta_1, \ldots, \delta_m) = \emptyset$. Quindi da un lato $\mathcal{K} = \mathrm{Mod}(\Sigma) \subseteq \mathrm{Mod}(\sigma_1, \ldots, \sigma_n)$, dall'altro se $A \in \mathrm{Mod}(\sigma_1, \ldots, \sigma_n)$ allora

$$
\begin{aligned}
&A \notin \mathrm{Mod}(\delta_1, \ldots, \delta_m) && \text{perché } \mathrm{Mod}(\sigma_1, \ldots, \sigma_n) \cap \mathrm{Mod}(\delta_1, \ldots, \delta_m) = \emptyset \\
&A \notin \mathcal{K}^c && \text{perché } \mathcal{K}^c = \mathrm{Mod}(\Delta) \subseteq \mathrm{Mod}(\delta 1, \ldots, \delta_m),
\end{aligned}
$$

dunque $A \in \mathcal{K}$. Possiamo allora concludere che $\mathcal{K} = \mathrm{Mod}(\sigma_1, \ldots, \sigma_n)$. □

Esempio 4.82. Segue dal lemma precedente che *la classe delle strutture infinite in un linguaggio $\mathcal{L}$ è assiomatizzabile ma non finitamente assiomatizzabile*. Infatti la classe delle strutture infinite in un linguaggio $\mathcal{L}$ è assiomatizzata dall'insieme delle formule $\{\varepsilon_n \mid n \in \mathbb{N}\}$ del Lemma 4.77, ma sempre in base al Lemma 4.77 le strutture finite nel linguaggio $\mathcal{L}$ non sono assiomatizzabili e quindi, per il Lemma 4.81 la classe delle strutture infinite nel linguaggio $\mathcal{L}$ non può essere finitamente assiomatizzabile.

Esempio 4.83. La classe dei campi di caratteristica p per p numero naturale positivo è assiomatizzata dagli assiomi dei campi e la formula $1 \overset{p \text{ volte}}{+ \cdots +} 1 = 0$. La classe dei campi di caratteristica 0 è assiomatizzabile ma non finitamente assiomatizzabile. Infatti gli assiomi dei campi insieme alle infinite formule $\{1 \overset{p \text{ volte}}{+ \cdots +} 1 \neq 0 \mid p \in \mathbb{N} \setminus \{0\}\}$ assiomatizzano i campi di caratteristica 0, ma se questa fosse finitamente assiomatizzabile, per il Lemma 4.80 dovrebbe esistere un sottoinsieme finito $F \subseteq \mathbb{N}$ tale che gli assiomi dei campi insieme alle formule $\{1 \overset{p \text{ volte}}{+ \cdots +} 1 \neq 0 \mid p \in F \setminus \{0\}\}$ assiomatizzano i campi di caratteristica finita, ma siccome F è finito ha un massimo, dicamo k. Sia q un numero primo maggiore di k, allora il campo degli interi modulo q soddisfa tutti gli assiomi $\{1 \overset{p \text{ volte}}{+ \cdots +} 1 \neq 0 \mid p \in F \setminus \{0\}\}$ ma non ha caratteristica 0.

Infine la classe dei campi di caratteristica maggiore di zero non è assiomatizzabile, perché se lo fosse per il Lemma 4.81 la classe dei campi di caratteristica 0 dovrebbe essere finitamente assiomatizzabile.

Esercizio 4.84. Dimostrare che i campi algebricamente chiusi sono assiomatizzabili ma non finitamente assiomatizzabili.

Esercizio 4.85. Dimostrare che i gruppi privi di torsioni sono assiomatizzabili ma non finitamente assiomatizzabili.

4.7 complementi: il metodo dei tableaux per la logica del prim'ordine.

A differenza della logica proposizionale, verificare che una formula del primo ordine ben formata sia logicamente valida è un compito abbastanza complicato, infatti essa è logicamente valida se è valida in tutti i possibili domini di interpretazione e per tutte le possibili interpretazioni delle variabile. Una tale classe è infinita, è perciò impossibile controllare caso per caso che la proprietà valga (cosa che invece facciamo in logica proposizionale quando calcoliamo riga per riga la tavola di verità).

In questa breve sezione presenteremo un metodo più efficace per la verifica di tautologie del primo ordine. L'algoritmo, che chiameremo `Tab`∀ costruisce, a partire da una formula, un albero di possibili valutazioni per quella formula. Partendo dalla negazione della formula data, se un ramo dell'albero dovesse arrivare a conclusione positivamente, otterremmo un'interpretazione che falsifica la formula data; questa non sarebbe dunque logicamente valida. Se viceversa l'algoritmo dovesse chiudere tutti i rami negativamente (cioè con qualche contraddizione all'interno di ogni ramo) allora vorrebbe dire che è impossibile falsificare la formula data o, equivalentemente, che essa è logicamente valida.

L'algoritmo `Tab`∀ è un'estensione di quello dato all'inizio della Sezione 2.7, quindi le regole per gestire i connettivi proposizionali sono le stesse trovate in precedenza.

Descriviamo quindi solo come trattare i quantificatori.

I passi per i quantificatori da effettuare nell'algoritmo `Tab`∀ si dividono in due tipi: del I tipo e del II tipo.

4.7.1 *Regole del I tipo.*

Se $\varphi = \exists x \varphi_1$ allora l'albero si prolunga come segue:

$$\begin{array}{c} V(\exists x \varphi_1) \\ | \\ V(\varphi_1[c/x]) \end{array}$$

qui il simbolo di costante c è nuovo, nel senso che esso deve essere scelto tra i simboli di costante che non appaiono nell'albero (non è necessario che c appartenga al linguaggio). Intuitivamente, se vogliamo verificare $\varphi = \exists x \varphi_1$ bisogna verificare che $\varphi_1[c/x]$ valga per qualche costante c.

Se $\varphi = \forall x \varphi_1$ allora l'albero si prolunga come segue:

$$\begin{array}{c} F(\forall x \varphi_1) \\ | \\ F(\varphi_1[c/x]) \end{array}$$

anche qui il simbolo di costante c è nuovo, nel senso che esso deve essere scelto tra i simboli di costante che non appaiono nell'albero (non è necessario che c appartenga al linguaggio). Intuitivamente, se vogliamo falsificare $\varphi = \forall x \varphi_1$ bisogna falsificare $\varphi_1[c/x]$ per qualche costante c.

Come al solito, nelle regole del I tipo, il nodo a cui è stata applicata la regola viene segnato poiché esso non verrà più considerato. Al contrario i nodi a cui si applicano regole del II tipo non verranno segnati perché essi vanno riconsiderati ogni volta che un nuovo simbolo di costante appare nell'albero.

4.7.2 *Regole del II tipo.*

Se $\varphi = \exists x \varphi_1$ allora l'albero si prolunga come segue:

$$\begin{array}{c} F(\exists x \varphi_1) \\ | \\ F(\varphi_1[c_1/x]) \\ | \\ \vdots \\ | \\ F(\varphi_1[c_n/x]) \end{array}$$

qui $c_1, \dots, c_n$ sono tutte i simboli di costante già apparsi nel ramo che stiamo prolungando. Se non dovessero essere apparsi simboli di constatante precedentemente, se ne introduce uno nuovo. Intuitivamente, se vogliamo falsificare $\varphi = \exists x \varphi_1$ dobbiamo falsificare ogni $\varphi_1[c_i/x]$ per ogni possibile costante c_i presa in considerazione.

Se $\varphi = \forall x \varphi_1$ allora l'albero si prolunga come segue:

$$\begin{array}{c} V(\forall x \varphi_1) \\ | \\ V(\varphi_1[c_1/x]) \\ | \\ \vdots \\ | \\ V(\varphi_1[c_n/x]) \end{array}$$

qui $c_1, \dots, c_n$ sono tutte i simboli di costante già apparsi nel ramo che stiamo prolungando. Se non dovessero essere apparsi simboli di constatante precedentemente, se ne introduce uno nuovo. Intuitivamente, se vogliamo verificare $\varphi = \forall x \varphi_1$ dobbiamo verificare $\varphi_1[c/x]$ per ogni costante c_i già presa in considerazione.

Le regole del secondo tipo non vengono applicate una sola volta, ma si *riattivano* ogni volta che appare un nuovo simbolo di costante nel ramo a cui esse appartengono. Questo fa sì che, al contrario di quello che succede nell'algoritmo in logica proposizionale, questo algoritmo possa andare avanti all'infinito (si veda l'Esempio 4.87).

Esempio 4.86. Dimostriamo che $\neg\forall x\varphi(x) \leftrightarrow \exists x\neg\varphi(x)$ è logicamente valida.

$$\mathsf{F}((\neg\forall x\varphi(x) \to \exists x\neg\varphi(x)) \wedge (\exists x\neg\varphi(x) \to \neg\forall x\varphi(x)))^*$$

$$\begin{array}{cc}
\mathsf{F}(\neg\forall x\varphi(x) \to \exists x\neg\varphi(x))^* & \mathsf{F}(\exists x\neg\varphi(x) \to \neg\forall x\varphi(x))^* \\
| & | \\
\mathsf{V}(\neg\forall x\varphi(x))^* & \mathsf{V}(\exists x\neg\varphi(x))^* \\
| & | \\
\mathsf{F}(\exists x\neg\varphi(x)) & \mathsf{F}(\neg\forall x\varphi(x))^* \\
| & | \\
\mathsf{F}(\forall x\varphi(x))^* & \mathsf{V}(\forall x\varphi(x)) \\
| & | \\
\mathsf{F}(\varphi(c_1)) & \mathsf{V}(\neg\varphi(c_2))^* \\
| & | \\
\mathsf{F}(\neg\varphi(c_1))^* & \mathsf{F}(\varphi(c_2)) \\
| & | \\
\mathsf{V}(\varphi(c_1)) & == \\
| & \\
== &
\end{array}$$

Poiché tutti i rami portano a una contraddizione la formula è logicamente valida

Esempio 4.87. Consideriamo ora la formula $\exists x \forall y \varphi(x, y)$.

$$
\begin{array}{c}
F(\exists x \forall y \varphi(x,y)) \\
| \\
F(\forall y \varphi(c_1, y))^* \\
| \\
F(\varphi(c_1, c_2)) \\
| \\
F(\forall y \varphi(c_2, y))^* \\
| \\
F(\varphi(c_2, c_3)) \\
| \\
F(\forall y \varphi(c_3, y))^* \\
| \\
F(\varphi(c_3, c_4)) \\
| \\
\vdots
\end{array}
$$

Come si vede, l'algoritmo entra in un ciclo dal quale non uscirà mai, generando sempre nuove costanti.

Esempio 4.88. Si consideri la formula

$$(\exists x \varphi(x) \vee \exists x \psi(x)) \to (\forall x \exists y (\neg \varphi(x) \vee \neg \psi(y))) \ .$$

$$
\begin{array}{c}
F((\exists x\varphi(x) \vee \exists x\psi(x)) \to (\forall x\exists y(\neg\varphi(x) \vee \neg\psi(y))))^{*} \\
| \\
V(\exists x\,(\varphi(x) \vee \psi(x)))^{*} \\
| \\
F((\forall x\exists y(\neg\varphi(x) \vee \neg\psi(y))))^{*} \\
| \\
V(\varphi(c) \vee \psi(c))^{*} \\
| \\
F(\exists y(\neg\varphi(d) \vee \neg\psi(y))) \\
\begin{array}{cc}
V(\varphi(c)) & V(\psi(c)) \\
| & | \\
F(\neg\varphi(d) \vee \neg\psi(c)))^{*} & F(\neg\varphi(d) \vee \neg\psi(c)))^{*} \\
| & | \\
F(\neg\varphi(d))^{*} & F(\neg\varphi(d))^{*} \\
| & | \\
F(\neg\psi(c))^{*} & F(\neg\psi(c))^{*} \\
| & | \\
V(\varphi(d)) & V(\varphi(d)) \\
| & | \\
V(\psi(c)) & V(\psi(c)) \\
| & | \\
F(\neg\varphi(d) \vee \neg\psi(d)))^{*} & F(\neg\varphi(d) \vee \neg\psi(d)))^{*} \\
| & | \\
F(\neg\varphi(d))^{*} & F(\neg\varphi(d))^{*} \\
| & | \\
F(\neg\psi(d))^{*} & F(\neg\psi(d))^{*} \\
| & | \\
V(\varphi(d)) & V(\varphi(d)) \\
| & | \\
V(\psi(d)) & V(\psi(d))
\end{array}
\end{array}
$$

Non è logicamente valida perché non si chiudono tutti i rami.

Esempio 4.89. Si consideri la formula

$$(\forall x\varphi(x) \vee \forall x\psi(x)) \to (\forall x(\neg\varphi(x) \to \forall y\psi(y)))\ .$$

$$\begin{array}{c}
F((\forall x\varphi(x) \vee \forall x\psi(x)) \to (\forall x(\neg\varphi(x) \to \forall y\psi(y))))^* \\
| \\
V(\forall x\varphi(x) \vee \forall x\psi(x))^* \\
| \\
F(\forall x(\neg\varphi(x) \to \forall y\psi(y)))^* \\
| \\
F(\neg\varphi(c_1) \to \forall y\psi(y))^* \\
| \\
V(\neg\varphi(c_1))^* \\
| \\
F(\forall y\psi(y))^* \\
| \\
F(\varphi(c_1)) \\
| \\
F(\psi(c_2)) \\
\swarrow \qquad \searrow \\
\begin{array}{cc}
V(\forall x\varphi(x)) & V(\forall x\psi(x)) \\
| & | \\
V(\varphi(c_1)) & V(\psi(c_1)) \\
| & | \\
V(\varphi(c_2)) & V(\psi(c_2)) \\
| & | \\
=== & ===
\end{array}
\end{array}$$

È logicamente valida perché si chiudono tutti i rami.

Esempio 4.90. Si consideri la formula

$$(\forall x\varphi(x) \wedge \forall x\psi(x)) \to (\exists x(\neg\varphi(x) \vee \neg\psi(x)) \to (\varphi(x) \wedge \neg\varphi(x))) \ .$$

$$
\begin{array}{c}
F((\forall x\varphi(x) \wedge \forall x\psi(x)) \to (\exists x(\neg\varphi(x) \vee \neg\psi(x)) \to (\varphi(x) \wedge \neg\varphi(x))))^{*} \\
| \\
V(\forall x\varphi(x) \wedge \forall x\psi(x))^{*} \\
| \\
F(\exists x(\neg\varphi(x) \vee \neg\psi(x)) \to (\varphi(x) \wedge \neg\varphi(x)))^{*} \\
| \\
V(\exists x(\neg\varphi(x) \vee \neg\psi(x)))^{*} \\
| \\
F(\varphi(x) \wedge \neg\varphi(x)) \\
| \\
V(\forall x\varphi(x)) \\
| \\
V(\forall x\psi(x)) \\
| \\
V(\neg\varphi(c_1) \vee \neg\psi(c_1))^{*} \\
\begin{array}{cc}
\swarrow & \searrow \\
V(\neg\varphi(c_1))^{*} & V(\neg\psi(c_1))^{*} \\
| & | \\
F(\varphi(c_1)) & F(\psi(c_1)) \\
| & | \\
V(\varphi(c_1)) & V(\varphi(c_1)) \\
| & | \\
=== & ===
\end{array}
\end{array}
$$

È logicamente valida perché si chiudono tutti i rami.

INDICE ANALITICO

LISTA DEI TEOREMI

RIFERIMENTI IN ITALIANO

[1] Francesco Berto. *Logica da zero a Gödel*. Laterza, 2008.

[2] Lorenzo Tortora de Falco and Vito Michele Abrusci. *Logica: Dimostrazioni e modelli al primo ordine*. Springer, 2014.

[3] Edward J. Lemmon. *Elementi di logica. Con gli esercizi risolti*. Laterza, 2008.

[4] Elliott Mendelson. *Introduzione alla logica matematica*. Bollati Boringhieri, 1977.

[5] Daniele Mundici. *Logica: metodo breve*, volume 50. Springer Science & Business Media, 2011.

[6] Piergiorgio Odifreddi. *Il diavolo in cattedra. La logica da Aristotele a Gödel*. Einaudi, 2015.

[7] Dario Palladino. *Corso di logica. Introduzione al calcolo dei predicati*. Carocci, 2010.

RIFERIMENTI DI BASE IN INGLESE

[8] Steven Givant and Paul Halmos. *Introduction to Boolean algebras*. Springer Science & Business Media, 2008.

[9] Paul Halmos and Steven Givant. *Logic as algebra*. Cambridge University Press, 1998.

[10] Paul R Halmos. *Algebraic logic*. Courier Dover Publications, 2016.

[11] James Donald Monk. *Mathematical logic*, volume 37. Springer Science & Business Media, 2012.

[12] Dirk Van Dalen. *Logic and structure*. Springer, 2004.