Corso di Laurea in Informatica - A.A. 2016/17

Note sugli Insiemi, sul Calcolo Proposizionale, sulla Logica dei Predicati, e sulle Espressioni Regolari

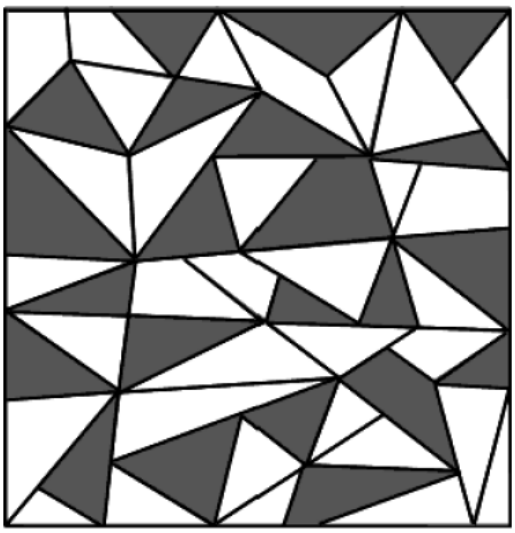
Materiale didattico per il corso

LMB: Linguaggio Matematico di Base, Modellazione e Ragionamento

Chiara Bodei, Roberto Bruni e Andrea Corradini

Dipartimento di Informatica, Università di Pisa

7 settembre 2016



Ringraziamenti.

Si ringraziano Francesca Levi, Paolo Mancarella e Simone Martini, autori di dispense didattiche dedicate alla logica per informatica dalle quali abbiamo tratto alcuni spunti, e Fabio Gadducci per averci aiutato nella revisione di queste note.

Indice

Capitolo 1

Introduzione

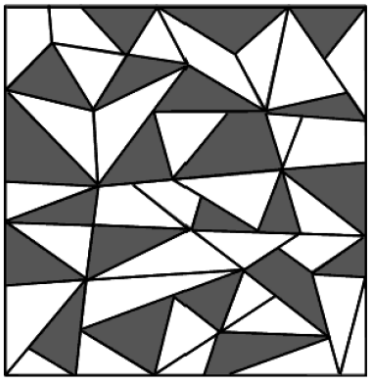
Queste note comprendono del materiale introduttivo su alcuni argomenti logico-matematici di fondamentale importanza per il Corso di Laurea in Informatica.

A fronte di una breve introduzione in stile rigoroso di concetti logico-matematici di base, l'obiettivo di queste note è di stimolare lo studente a utilizzare questi concetti in ragionamenti deduttivi, semplici ma non banali. In questo capitolo introduciamo alcuni argomenti logico-matematici di facile comprensione che hanno l'obiettivo di stimolare la curiosità del lettore e presentiamo il concetto di *dimostrazione per sostituzione* che è ampiamente usato nei capitoli che seguono. Gli argomenti dei capitoli successivi comprendono gli insiemi (Capitolo 2), il calcolo proposizionale (Capitolo 3), la logica predicativa (Capitolo 4), e le espressioni regolari (Capitolo 5). La presentazione di ogni argomento è accompagnata da numerosi esempi e da esercizi di difficoltà crescente riguardanti sia la comprensione delle nozioni introdotte, sia la capacità di applicare tecniche deduttive elementari per dimostrare la verità di enunciati o per confutarli.

Attraverso lo studio di queste note lo studente dovrebbe sviluppare una capacità di apprendimento non puramente nozionistico e una miglior comprensione del tipo di attitudine mentale richiesta dagli studi di Informatica.

1.1 Una metafora: la stella di Loyd

(a) Il Gioco del 15



(b) La stella di Loyd.

Figura 1.1: Due famosi giochi resi popolari da Samuel Loyd

Samuel Loyd (1841–1911) è stato forse il maggior creatore di giochi matematici di tutti i tempi, tra i quali il *Gioco del 15* (Figura 1.1(a)), in voga ancora oggi. Uno dei suoi giochi più famosi si intitola *la stella nascosta* ed è spesso usato come metafora della matematica (ma la morale sarebbe facilmente adattabile a molte altre attività umane). Il gioco consiste nell'individuare una stella a cinque punte nel disegno bicolore in Figura 1.1(b). (C'è davvero: non ci sono trucchi!).

- Molte persone individuano subito la stella: per loro è evidente, lampante, impossibile da ignorare. Quasi non concepiscono che altri possano non vederla.

- A molte altre persone occorrono invece molto tempo, impegno e perseveranza. Ma quando riescono a trovarla la soddisfazione sarà per loro maggiore e appagante.
- In ogni caso, una volta individuata la stella non sarà più possibile fingere di ignorarla e recuperare la cecità perduta per ripetere il gioco.

Speriamo che seguendo il Corso di Laurea in Informatica voi scopriate la via matematica di affrontare i problemi: poi non potrete più farne a meno.

1.2 Il linguaggio matematico

Se state leggendo queste note vi starete probabilmente chiedendo

Perché la matematica è così importante per un corso di studi in informatica?

La risposta non è immediata e merita alcune considerazioni. La prima considerazione è che:

L'informatica è una scienza che si occupa di sviluppare
teorie, modelli e tecnologie per gestire informazioni su sistemi automatizzati.

Da questo deriva che le teorie e i modelli utilizzati debbano basarsi su delle rappresentazioni dell'informazione che siano trattabili da sistemi automatizzati. Serve quindi un linguaggio che permetta di descrivere l'informazione, le sue proprietà e le sue trasformazioni. Questo linguaggio deve essere comprensibile sia agli umani che ai sistemi informatici, in modo che l'informazione possa essere rappresentata, memorizzata su opportuni supporti, trasmessa verso altri sistemi e dispositivi, elaborata e resa disponibile in formato comprensibile agli umani.

Mentre il linguaggio naturale è quello preferito dagli umani per comunicare tra loro, la necessità di essere trattabile da sistemi automatizzati introduce alcuni vincoli che ne limitano l'utilizzo rispetto alle esigenze appena descritte. Il linguaggio richiesto si distingue perché deve essere:

- universale (non dipende dalla nazionalità di chi lo usa)
- rigoroso (non origina equivoci)

Queste caratteristiche sono soddisfatte dal *linguaggio della matematica*, che come tale si presta bene a descrivere e comunicare fatti e concetti in modo non ambiguo.

ESEMPIO 1.1 (AMBIGUITÀ DEL LINGUAGGIO NATURALE)
Cosa rispondereste alla seguente domanda su un importo in Euro:

È di più mille e cinque o mille e cinquanta?

- *Aldo risponde "mille e cinque";*
- *Barbara risponde "mille e cinquanta";*
- *Ciro risponde "sono uguali".*

Chi ha ragione? Tutti e tre, perché hanno interpretato in modo diverso la domanda!

- *Aldo ha pensato: mille e cinque* $= 1500 > 1050 =$ *mille e cinquanta;*
- *Barbara ha pensato: mille e cinque* $= 1005 < 1050 =$ *mille e cinquanta;*
- *Ciro ha pensato: mille e cinque* $1000,5 = 1000,50 =$ *mille e cinquanta.*

Le diverse risposte sono quindi dovute all'ambiguità presente nella domanda. Se lo stesso quesito fosse stato espresso in notazione matematica tutti avrebbero risposto alla stessa maniera.

Il linguaggio naturale permette spesso di compensare la mancanza di precisione con un contesto di riferimento, mentre il linguaggio della matematica non lascia spazi a equivoci: la sua precisione è necessaria perché si occupa di situazioni astratte e quindi fuori da ogni contesto.

Il linguaggio della matematica ci aiuta anche a costruire modelli per rappresentare e ragionare su frammenti della realtà in modo sistematico: servendo da supporto indispensabile per comprendere certi fenomeni e situazioni; permettendoci di comprovare o confutare le nostre intuizioni su questi fenomeni; consentendoci di comunicare e illustrare le nostre scoperte ad altri.

Come succede con il linguaggio naturale, anche con il linguaggio matematico si possono esprimere concetti in modo più o meno elegante, comprensibile, ridondante, sintetico, ma se queste formulazioni sono equivalenti il sistema informatico le interpreta allo stesso modo.

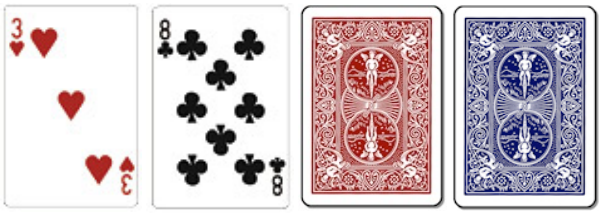
Con diversi esempi ed esercizi, queste note hanno anche l'obiettivo di sviluppare nel lettore la capacità di "formalizzare" enunciati espressi in linguaggio naturale, traducendoli in linguaggio matematico.

1.3 Il problema delle quattro carte

Nel campo del ragionamento deduttivo uno dei rompicapo logici più celebri è il cosiddetto *problema delle quattro carte*, ideato da Peter Cathart Wason (1924–2003), un celebre psicologo cognitivo impegnato nello studio della psicologia del ragionamento.

Il rompicapo è stato ideato da Wason nel 1966 per studiare come varia la capacità delle persone di risolvere lo stesso problema logico quando sia contestualizzato diversamente o, nello specifico, come l'esperienza quotidiana possa influenzare la risposta. Il problema di Wason è chiamato anche *Wason selection task*.

Esistono varie versioni del problema, che coinvolgono forme, lettere, colori e numeri. Di seguito ne riportiamo una delle versioni più note con la quale potrete confrontarvi.



[3 di cuori] [8 di fiori] [dorso rosso] [dorso blu]

Figura 1.2: Wason selection task.

ESERCIZIO 1.2 (WASON SELECTION TASK (CON CARTE DA GIOCO))
Su un tavolo ci sono quattro carte da gioco. Le facce visibili delle carte sul tavolo mostrano, nell'ordine 3 di cuori, 8 di fiori, dorso rosso e dorso blu (vedi Figura 1.2). Quali carte dovete girare per assicurarvi che la seguente proposizione sia vera?

Se la faccia anteriore di una carta reca un numero pari allora la faccia posteriore è rossa.

Se non risolvete correttamente il rompicapo non preoccupatevi troppo: nello studio di Wason meno del 10% dei soggetti che parteciparono all'esperimento riuscì a dare la risposta corretta.

Nel 1992 Griggs e Cox replicarono l'esperimento con alcuni studenti della Florida introducendo aspetti "sociali" per guidare il ragionamento. In questo caso la percentuale di risposte corrette fu di gran lunga superiore, nonostante la natura del problema fosse identica. Una delle spiegazioni possibili è che riconducendo l'asserzione a una regola sociale diffusa i soggetti dell'esperimento hanno già appreso come verificarla attraverso la pratica, anche senza avere familiarità con la logica.

ESERCIZIO 1.3 (WASON SELECTION TASK (CON BIRRA))
Un poliziotto entra in un locale della Florida dove un grande cartello ricorda ai clienti che

per bere birra devi avere più di 16 anni

Nel locale ci sono quattro clienti: un ragazzo che sta bevendo acqua, una ragazza che sta bevendo birra, un'anziana signora e un adolescente di 15 anni che tengono i loro bicchieri racchiusi tra le mani. Quali clienti deve controllare il poliziotto per verificare che la regola sia rispettata?

Alla fine di queste note avremo gli strumenti per formalizzare problemi di questo tipo nel linguaggio della matematica, e disporremo anche di alcuni metodi per risolverli. In particolare, vedremo nella Sezione 4.4.2 come presentare in modo formale l'Esercizio 1.3 e come impostarne il procedimento risolutivo.

1.4 Le dimostrazioni per sostituzione

Il modo con il quale effettueremo i calcoli e le dimostrazioni in queste note può essere illustrato con un esempio di algebra elementare certamente ben noto al lettore: l'identità del *prodotto notevole* $(a+b)(a-b) = (a^2-b^2)$. Questa uguaglianza esprime che, indipendentemente dai valori che scegliamo di sostituire al posto dei simboli a e b nelle due espressioni, il risultato del calcolo di $(a+b)(a-b)$ è lo stesso di quello del calcolo di a^2-b^2. Per esempio, se sostituiamo a con 3 e b con 1 abbiamo $(3+1)(3-1) = 4\cdot 2 = 8$ e $3^2-1^2 = 9-1 = 8$.

Come possiamo essere certi che l'uguaglianza valga per tutti i valori? Il tentativo di verificarla per ogni coppia di valori non è attuabile, perché il numero di coppie da considerare è infinito. In questi casi, l'algebra ci permette di condurre la dimostrazione a livello puramente simbolico, mediante una successione di uguaglianze, ciascuna di esse giustificata da qualche legge algebrica o da qualche identità già dimostrata. Nell'esempio specifico, possiamo immaginare che abbiate già incontrato la dimostrazione in un qualche testo di algebra o su una lavagna, scritta magari nel seguente modo:

$$(a+b)(a-b) = a^2 - \cancel{ab} + \cancel{ab} - b^2 = a^2 - b^2$$

Ma sareste in grado di giustificare i singoli passaggi? E di descrivere una tecnica automatica per condurre altre dimostrazioni analoghe a quella?

In queste note vedremo come affrontare problemi di questo tipo, in maniera sistematica, partendo da un insieme di leggi che definiscono le operazioni elementari, per esempio quelle che regolano le operazioni insiemistiche nel Capitolo 2 e i connettivi logici per la costruzione di formule proposizionali e predicative nei Capitoli 3 e 4.

In questa sezione, come primo esempio, ci concentriamo sull'uguaglianza di espressioni aritmetiche, con le quali presupponiamo che il lettore abbia familiarità. Rivisitando in modo rigoroso il metodo risolutivo già noto in campo aritmetico si presuppone che sarà più facile per il lettore applicarlo nei contesti oggetto dei capitoli successivi.

Per prima cosa presentiamo, in modo incrementale, le leggi degli operatori che compaiono nell'uguaglianza che intendiamo dimostrare: somma, differenza, prodotto e quadrato. Ciascuna legge esprime un'uguaglianza tra due espressioni con variabili. Per esempio, alcune leggi che si applicano alla somma e alla differenza sono le seguenti:

Leggi sulla somma e sulla differenza

$x + 0 = x$	$x - 0 = x$	(elemento neutro)
$-x + x = 0$	$x - x = 0$	(differenza)
$x + y = y + x$		(commutatività)
$x + (y + z) = (x + y) + z$	$x + (y - z) = (x + y) - z$	(associatività)

Ciascuna legge può essere applicata con una sostituzione opportuna delle variabili con espressioni a piacere garantendo che l'uguaglianza venga preservata. Consideriamo le leggi sulla somma. La legge dell'elemento neutro garantisce che sommando 0 a qualsiasi espressione non se ne modifica il valore. La legge di commutatività ci permette di invertire l'ordine degli addendi in un'espressione senza alterare il risultato. (Ovviamente la commutatività non vale nel caso della differenza). La legge di associatività garantisce che possiamo raggruppare gli addendi arbitrariamente senza alterare il risultato.

Nelle dimostrazioni procederemo applicando queste leggi a un'espressione di partenza per ricondurla a una certa espressione di arrivo, rispettando rigorosamente la forma delle espressioni. Per esempio, per derivare

l'uguaglianza $0+3=3$ non possiamo applicare direttamente la legge dell'elemento neutro ($x+0=x$), perché questa prevede che 0 sia il secondo addendo, non il primo. Dobbiamo invece applicare prima la legge di commutatività della somma ($0+3=3+0=3$).

Dato che ogni legge esprime un'uguaglianza, la possiamo applicare in entrambe le direzioni: sia per sostituire un'istanza del membro sinistro con la corrispondente istanza del membro destro, che viceversa (per sostituire un'istanza del membro destro con la corrispondente istanza del membro sinistro). Anche se l'orientamento è puramente indicativo, di solito le leggi vengono scritte in modo che la loro applicazione da sinistra verso destra porti ad una semplificazione dell'espressione.

Quando introduciamo le leggi relative a un nuovo operatore includiamo quelle che lo mettono in relazione con gli operatori introdotti in precedenza. Per esempio, nell'elenco delle leggi sul prodotto[1] riportate sotto includiamo le leggi di distributività su somma e differenza:

Leggi sul prodotto

$1x = x$	$0x = 0$	(elemento neutro e elemento assorbente)
	$xx = x^2$	(quadrato)
$xy = yx$		(commutatività)
$x(y + z) = xy + xz$	$x(y - z) = xy - xz$	(distributività a sinistra)
$(x + y)z = xz + yz$	$(x - y)z = xz - yz$	(distributività a destra)

Per comodità talvolta elencheremo direttamente alcune leggi ridondanti, per ridurre il numero di passaggi richiesti nelle dimostrazioni. È questo il caso delle leggi di distributività del prodotto sulla somma e sulla differenza, ripetute sopra nella versione distributiva a sinistra e distributiva a destra, anche se essendo il prodotto commutativo sarebbe stato sufficiente presentare una sola versione. In seguito, per semplicità ci riferiremo a tutte le varianti con il termine "distributività".

Adesso mostriamo come sfruttare (alcune del)le leggi elencate per dimostrare l'uguaglianza del prodotto notevole $(a+b)(a-b) = (a^2-b^2)$.

Per poter applicare la legge distributiva $(x+y)z = xz+yz$, dobbiamo sostituire, ovvero istanziare, x con l'espressione a, y con b e z con $(a-b)$, scritto $\{x \mapsto a, y \mapsto b, z \mapsto (a-b)\}$. Così possiamo derivare l'uguaglianza

$$(\underbrace{a}_{x} + \underbrace{b}_{y})\underbrace{(a-b)}_{z} = \underbrace{a}_{x}\underbrace{(a-b)}_{z} + \underbrace{b}_{y}\underbrace{(a-b)}_{z}$$

Inoltre ciascuna legge può essere applicata a una sotto-espressione che compare in un contesto più ampio. Questo principio, detto *principio di sostituzione* permette di sostituire parti di espressioni con altre espressioni a loro uguali, ovvero di ragionare su singole parti di espressioni. Per esempio, la legge distributiva $x(y-z) = xy-xz$ può essere istanziata mediante la sostituzione $\{x \mapsto a, y \mapsto a, z \mapsto b\}$ e applicata alla sotto-espressione $a(a-b)$ che compare all'interno del contesto $\underline{a(a-b)} + b(a-b)$ (qui l'occorrenza della sotto-espressione è evidenziata dalla sottolineatura). Grazie al principio di sostituzione e alla legge distributiva deriviamo l'uguaglianza:

$$\underbrace{a}_{x}(\underbrace{a}_{y} - \underbrace{b}_{z}) + b(a-b) = \underbrace{a}_{x}\underbrace{a}_{y} - \underbrace{a}_{x}\underbrace{b}_{z} + b(a-b)$$

In genere tali giustificazioni sono così ovvie da non essere menzionate esplicitamente; nel nostro caso, tuttavia, vogliamo usarle per annotare ogni passaggio. Di seguito useremo talvolta la sottolineatura per evidenziare la sotto-espressione alla quale si applica la legge e ometteremo spesso di specificare quale sostituzione si stia applicando.

Un modo per organizzare la dimostrazione è il seguente:

$$\begin{aligned} & (a+b)(a-b) \\ = & \quad \{ \text{ (distributività } (x+y)z = xz+yz) \text{ con sostituzione } \{x \mapsto a, y \mapsto b, z \mapsto (a-b)\} \ \} \\ & \underline{a(a-b)} + \underline{b(a-b)} \end{aligned}$$

[1] Di seguito useremo indifferentemente la giustapposizione (ab) e il simbolo $\times$ ($a \times b$) per indicare l'operatore di moltiplicazione.

$$
\begin{array}{ll}
= & \{ \text{ (distributività } x(y-z) = xy - xz\text{), due volte, la prima volta con sostituzione} \\
& \quad \{ x \mapsto a, y \mapsto a, z \mapsto b \} \text{ e la seconda con } \{ x \mapsto b, y \mapsto a, z \mapsto b \} \} \\
& (\underline{aa} - ab) + (ba - \underline{bb}) \\
= & \{ \text{ (quadrato } xx = x^2\text{), due volte, e (associatività) della somma } \} \\
& a^2 \underline{-ab + ba} - b^2 \\
= & \{ \text{ (commutatività) del prodotto, e (differenza } -x + x = 0\text{) } \} \\
& \underline{a^2 + 0} - b^2 \\
= & \{ \text{ (elemento neutro } x + 0 = x\text{) } \} \\
& a^2 - b^2
\end{array}
$$

La dimostrazione consiste dunque in una catena di uguaglianze, ciascuna corredata da una giustificazione, sotto la forma di un'identità algebrica; si noti come in tutte le uguaglianze eccetto la prima si sia implicitamente utilizzato il principio di sostituzione. Tutte le dimostrazioni di queste note si atterranno a questo formato. Invitiamo il lettore ad abituarsi a scrivere le soluzioni degli esercizi proposti nello stesso modo.

Per quanto riguarda le giustificazioni, si cercherà, soprattutto all'inizio, di essere quanto più possibile precisi. A tal fine, assumeremo che valgano le proprietà algebriche degli operatori aritmetici; l'uguaglianza (=) è riflessiva ($x = x$), simmetrica (se $x = y$ allora $y = x$) e transitiva (se $x = y$ e $y = z$, allora $x = z$). In virtù della transitività dell'uguaglianza =, un calcolo della forma:

$$
\begin{array}{ll}
& E_1 \\
= & \{ \text{ giustificazione}_1 \} \\
& E_2 \\
= & \{ \text{ giustificazione}_2 \} \\
& \cdots \\
= & \{ \text{ giustificazione}_{k-1} \} \\
& E_k
\end{array}
$$

costituisce una dimostrazione che $E_1 = E_k$. Si noti anche che dalle dimostrazioni di $E_1 = E$ ed $E_2 = E$ possiamo concludere che $E_1 = E_2$.

Oltre agli operatori algebrici definiti sopra, utilizzeremo anche altri operatori, che introdurremo di volta in volta. Siccome non vogliamo rifarci all'intuizione per la derivazione di identità che li coinvolgono, ciascuno di essi verrà introdotto insieme ad un gruppo di leggi che ne permette la manipolazione simbolica. Come primo esempio, consideriamo l'operatore binario di elevamento a potenza, governato dalle leggi seguenti:

Leggi sull'elevamento a potenza

$x^0 = 1$ se $x \neq 0$	$x^1 = x$	(esponente nullo e unitario)
$x^{(y+z)} = x^y x^z$	$(xy)^z = x^z y^z$	(regola della somma e del prodotto)
$(x^y)^z = x^{(yz)}$		(elevamento a potenza di una potenza)

Si noti che nel caso della legge per l'esponente nullo, l'uguaglianza è valida solo quando la base è diversa da 0: queste ipotesi a margine devono essere sempre garantite al momento di applicare l'uguaglianza, perché se fossero disattese potrebbero condurre a risultati errati. In generale, le dimostrazioni che faremo saranno valide solo sotto opportune ipotesi.

ESEMPIO 1.4 ($a\left(\frac{1}{a}\right) = 1$ SE $a \neq 0$)
Utilizzando le leggi viste in precedenza, e utilizzando la consueta notazione dell'inverso $\frac{1}{x}$ *per indicare* x^{-1}*, possiamo dimostrare che* $a\left(\frac{1}{a}\right) = 1$ *quando* $a \neq 0$*:*

$$
\begin{array}{ll}
& \underline{a}\ \left(\frac{1}{a}\right) \\
= & \{ \textit{ (esponente unitario } x^1 = x\textit{) } \} \\
& a^1\ \underline{\left(\frac{1}{a}\right)} \\
= & \{ \textit{ (definizione di inverso } \frac{1}{x} = x^{-1}\textit{) } \} \\
& a^1\ a^{-1} \\
= & \{ \textit{ (regola della somma } x^{(y+z)} = x^y x^z\textit{), applicata da destra verso sinistra } \}
\end{array}
$$

$$
\begin{array}{ll}
 & \underline{a^{1-1}} \\
= & \quad \{ \textit{ (differenza } x-x=0\textit{) } \} \\
 & \underline{a^0} \\
= & \quad \{ \textit{ (esponente nullo), sapendo per ipotesi che } a \neq 0 \ \} \\
 & 1
\end{array}
$$

In queste note, oltre a porre enfasi sull'uso del principio di sostituzione per dimostrare uguaglianze di espressioni, cercheremo di stimolare il ragionamento critico nella ricerca di controesempi. Nello specifico, una relazione di uguaglianza potrebbe valere solo per alcune sostituzioni delle sue variabili ma non per tutte, o non valere affatto. In questi casi, basta esibire una particolare sostituzione che rende diversi i risultati delle due espressioni coinvolte per confutare la presunta uguaglianza delle due espressioni.

ESEMPIO 1.5 (È VERO CHE L'OPERATORE DI ELEVAMENTO A POTENZA È COMMUTATIVO? ($x^y = y^x$?))
Per dimostrare la commutatività bisognerebbe fornire una prova della congettura $x^y = y^x$. Prima di cominciare a dimostrare una congettura, però, è bene soffermarsi a verificarne la validità su opportune sostituzioni, per accertarne la plausibilità. In questo caso, applicando la sostituzione $\{x \mapsto 2, y \mapsto 3\}$ all'espressione x^y otteniamo $2^3 = 8$ mentre applicando la stessa sostituzione all'espressione y^x otteniamo $3^2 = 9$. Quindi la sostituzione $\{x \mapsto 2, y \mapsto 3\}$ fornisce un controesempio alla congettura $x^y = y^x$. Anche se si possono trovare sostituzioni particolari che rendono uguali le espressioni x^y e y^x, ad esempio la sostituzione $\{x \mapsto 2, y \mapsto 2\}$, l'esistenza di un solo controesempio è sufficiente per dimostrare che la congettura è falsa.

1.5 Alcuni famosi problemi matematici

Gli strumenti che vi forniremo in queste note non vi permetteranno di risolvere ogni problema. A titolo di esempio, descriviamo di seguito tre famosi problemi matematici, di semplice formulazione ma di difficile soluzione, che speriamo possano stimolare la vostra curiosità. Questi problemi hanno tenuto impegnate le migliori menti matematiche per secoli e più recentemente sono stati affrontati con tecniche informatiche, diventando oggetto di studio di progetti di calcolo.[2] Siete invitati a soffermarvi su di essi per comprenderne fino in fondo gli enunciati: e se adesso ancora non ci riuscite, alla fine di queste note avrete gli strumenti per formalizzarli, anche se forse non per risolverli. Per facilitarne la comprensione, ricordiamo alcune semplici definizioni.

DEFINIZIONE 1.1 (DIVISORE, NUMERI PARI E DISPARI, NUMERI PRIMI)
*Dati due numeri naturali n e m, n **è un divisore di** m se esiste un naturale k tale che $m = k \times n$; in questo caso diciamo anche che m **è divisibile per** n.*
*Un naturale n è un numero **pari** se è divisibile per 2, altrimenti n è **dispari**.*
*Un naturale n è un numero **primo** se ha esattamente due divisori distinti.*[3]

1.5.1 L'Ultimo Teorema di Fermat (1637)

Pierre de Fermat (1601–1665) è stato un famoso matematico e magistrato francese. L'ultimo Teorema di Fermat è formulato dal seguente enunciato:

Dato un numero naturale $n > 2$ non esistono tre interi positivi a, b, c tali che $a^n + b^n = c^n$

Il teorema fu enunciato nel 1637 da Fermat senza una dimostrazione: quindi a dispetto del nome deve essere considerato una *congettura*, cioè un enunciato che l'autore ritiene vero anche senza una dimostrazione formale. Esso era espresso in una scritta ai margini di una copia dell'Arithmetica di Diofanto sulla quale Fermat era solito formulare molte delle sue famose teorie: *È impossibile separare un cubo in due cubi, o una potenza quarta in due potenze quarte, o in generale, tutte le potenze maggiori di due come somma della stessa potenza. Dispongo di una meravigliosa dimostrazione di questo teorema, che non può essere contenuta nel margine troppo stretto della pagina...* ma invece VOI AVRETE SEMPRE ABBASTANZA SPAZIO E FOGLI DURANTE L'ESAME.

[2] Le influenze di questi problemi non si sono fermate alle scienze matematiche e informatiche ma hanno contaminato altri ambiti culturali e artistici, facendo da sfondo o venendo menzionate in molti romanzi, film e serie televisive.

[3] Poiché ogni numero è divisibile per 1 e per se stesso, un numero primo non ha altri divisori. Si noti che 1 non è primo perché ha un solo divisore.

- Eulero fornì una dimostrazione per il caso $n = 3$.
- Fermat stesso fornì una dimostrazione per il caso $n = 4$.
- Legendre fornì una dimostrazione per il caso $n = 5$.
- Finalmente il teorema fu dimostrato nel 1994 da Andrew Wiles (dopo 7 anni di dedizione assoluta al problema e un falso allarme nel 1993), vincendo 50.000$ (la dimostrazione è lunga 200 pagine e sfrutta delle teorie non conosciute all'epoca di Fermat).

1.5.2 La Congettura di Eulero (1769)

Leonhard Euler (1707–1783), noto in Italia come Eulero, è stato un insigne matematico e fisico svizzero. La nota congettura recante il suo nome afferma che:

Dato $n > 2$ la somma di $n-1$ potenze n-esime di interi positivi non può eguagliare una potenza n-esima

In altri termini, la congettura afferma che quando $n > 2$ non esistono n interi positivi $a_1, ..., a_{n-1}, b$ tali che:

$$a_1^n + a_2^n + ... + a_{n-1}^n = b^n$$

- Per $n = 3$ è la congettura è un caso particolare dell'ultimo Teorema di Fermat: (non esistono a_1, a_2, b tali che $a_1^3 + a_2^3 = b^3$)
- Lander e Parkin (1966): confutarono la congettura per $n = 5$ col controesempio

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5.$$

- Elkies e Frye (1988): confutarono la congettura per $n = 4$, usando il calcolatore, col controesempio

$$95800^4 + 217519^4 + 414560^4 = 422481^4.$$

- Attualmente (2015) non sono noti controesempi per $n > 5$.

1.5.3 La Congettura di Goldbach (1742)

Christian Goldbach (1690–1764) è stato un matematico tedesco la cui fama è dovuta soprattutto ad una congettura sui numeri primi formulata nel 1742 e ancora aperta. Nonostante lo studio dei numeri primi possa apparire una materia molto astratta e speculativa, esso trova applicazioni in molti campi, ad esempio la crittografia moderna alla base delle transazioni finanziarie elettroniche.

La congettura di Goldbach è uno dei quesiti irrisolti più vecchi e affascinanti nella teoria dei numeri.

Ogni numero pari $n > 2$ può essere scritto come somma di due numeri primi (anche uguali)

- In una lettera indirizzata a Eulero, Goldbach congetturò che *ogni numero dispari $n > 5$ potesse essere scritto come somma di tre numeri primi* (oggi detta congettura "debole" di Goldbach).
- Eulero rispose con la versione più "forte" riportata sopra.
- In passato era stato offerto un premio di un milione di dollari... mai riscosso (valido solo entro aprile 2004, per pubblicizzare il libro *Lo zio Petros e la congettura di Goldbach*).
- Pogorzelski (1977): ha fornito una dimostrazione della congettura, che non è stata accettata dalla comunità matematica.
- Oliveira e Silva: hanno lanciato un progetto di calcolo distribuito *Goldbach conjecture verification* che ha verificato la congettura sino a $4 \cdot 10^{18}$ (aprile 2012).

1.6 Esercizi

Nella risoluzione degli esercizi proposti, giustificate sempre le risposte date, esprimendo il ragionamento che vi porta a concludere una certa deduzione, oppure fornendo opportuni controesempi.

1.6.1 Esercizi di comprensione

1.6.1.1 Quali sono le differenze principali tra il linguaggio della matematica e il linguaggio naturale?

1.6.1.2 Quali delle seguenti affermazioni ritenete di condividere:

(a) Il linguaggio della matematica serve a risolvere tutti i problemi reali.
(b) Il linguaggio della matematica permette di costruire modelli.
(c) Il linguaggio della matematica è volutamente ambiguo.
(d) Il linguaggio della matematica permette di veicolare idee.
(e) Il linguaggio della matematica permette di veicolare sentimenti.

1.6.1.3 L'ultimo teorema di Fermat è da ritenersi una congettura o un teorema?

1.6.1.4 Ci sono dei valori di n per i quali la congettura di Eulero possa ritenersi un teorema?

1.6.1.5 Per confutare la congettura di Goldbach quali valori dovreste fornire?

1.6.1.6 Il numero 1 è primo?

1.6.1.7 Il numero 29 è primo?

1.6.1.8 Il numero 39 è primo?

1.6.1.9 Il numero 101 è primo?

1.6.1.10 Il numero 1001 è primo?

1.6.1.11 Descrivete una procedura per verificare se un dato numero naturale n è primo oppure no.

1.6.2 Esercizi di approfondimento

1.6.2.1 Perché l'ipotesi $n > 2$ è necessaria nell'enunciato dell'ultimo teorema di Fermat?

1.6.2.2 Perché l'ipotesi $n > 2$ è necessaria nell'enunciato della congettura di Goldbach?

1.6.2.3 È vero che per ogni $n > 1$ il numero $2^n - 1$ è primo?

1.6.2.4 È vero che per ogni $n > 1$ il numero $n^2 + n + 41$ è primo?

1.6.2.5 È vero che l'area della circonferenza avente come raggio l'ipotenusa di un triangolo rettangolo è pari alla somma delle aree delle circonferenze aventi come raggi i cateti dello stesso triangolo?[4]

1.6.2.6 Provate a spiegare perché se la congettura forte di Goldbach fosse vera allora lo sarebbe necessariamente anche quella debole.

1.6.2.7 Se una gallina e mezza fanno un uovo e mezzo in un giorno e mezzo, quante uova fanno tre galline in tre giorni? Perché?

1.6.2.8 Quanto pesa un mattone che pesa un chilo più mezzo mattone? Perché?

1.6.2.9 È vero che il doppio del quadrato di 3 più 4 è uguale a 26? *"Certo!"*, risponde Lisa. *"No, è minore!"*, strilla Bart. *"Invece è maggiore...."*, pensa Maggie. Perché tutti e tre i fratelli potrebbero avere ragione?

[4] Si ringrazia Fabrizio Luccio per l'idea.

1.6.2.10 Mostrare come sia possibile che 3 per 10 più 2 possa dare come risultato sia 32 che 36.

1.6.2.11 Dimostrare o confutare la seguente congettura: ogni intero positivo dispari può essere espresso come il prodotto di due numeri dispari.

1.6.2.12 Dimostrare o confutare la seguente congettura: ogni intero positivo pari può essere espresso come il prodotto di due numeri pari.

1.6.2.13 Dimostrare o confutare la seguente congettura: non esiste alcun intero positivo che possa essere ottenuto come somma di tutti i suoi divisori positivi.

1.6.2.14 Dimostrare o confutare la seguente congettura: non esiste alcun intero positivo che possa essere ottenuto come somma dei suoi divisori positivi strettamente più piccoli di esso.

1.6.2.15 Confutare la relazione $a-(b-c)=(a-b)-c$.

1.6.2.16 Confutare la relazione $2a^2+2a=(a+1)^2$.

1.6.3 Esercizi che coinvolgono dimostrazioni per sostituzione

1.6.3.1 Si dimostrino le seguenti uguaglianze:

(a) $(a+b)^2=a^2+2ab+b^2$
(b) $(a-b)^2=(b-a)^2$
(c) $a^n=a^{n-1}a$
(d) $a^{n+m}a^{n-m}=a^{2n}$

1.6.3.2 Per ciascuna delle seguenti congetture, fornire una dimostrazione per sostituzione utilizzando le leggi algebriche viste in precedenza, oppure esibire un controesempio che confuti l'uguaglianza.

(a) $(1+\frac{1}{a})(1-\frac{1}{a})=(a^2-1)(\frac{1}{a})^2$?
(b) $(a-1)(a^2+a+1)=a^3-1$?
(c) $a^{2n}+2a^n+1=(a^n+1)^2$?
(d) Associatività dell'elevamento a potenza: $a^{(b^c)}=(a^b)^c$?
(e) Distributività rispetto alla somma delle basi: $(a+b)^c=a^c+b^c$?
(f) Distributività rispetto al prodotto degli esponenti: $a^{bc}=a^ba^c$?

Capitolo 2

Gli insiemi

In questo capitolo esaminiamo una delle nozioni fondamentali della matematica: la nozione di *insieme*. Supponendo che il lettore abbia già incontrato questi concetti nel corso degli studi precedenti, all'interno di questo capitolo esamineremo brevemente le principali operazioni di confronto e di composizione tra insiemi e le principali leggi che le regolano. Infine vedremo come dimostrare l'uguaglianza di insiemi usando tre tecniche diverse: le dimostrazioni discorsive (*ad hoc*), basate direttamente sulla definizione di uguaglianza tra insiemi; le dimostrazioni basate sui diagrammi di Eulero-Venn, intuitive e che non richiedono particolare creatività, ma di applicabilità limitata; e le dimostrazioni per sostituzione, che sfruttano le leggi sugli insiemi e le tecniche di manipolazione algebrica introdotte nella Sezione 1.4. Nel presentare le tecniche di dimostrazione daremo enfasi anche alla costruzione di controesempi per confutare enunciati erronei.

2.1 Rappresentare gli insiemi

DEFINIZIONE 2.1 (INSIEME)
*Un **insieme** è una collezione di oggetti, detti **elementi**, in cui l'ordine degli elementi e le eventuali ripetizioni non contano.*

Riteniamo utile evidenziare la differenza tra insiemi e *sequenze*: mentre nei primi l'ordine non è importante, nelle seconde l'ordinamento degli elementi è indispensabile perché questi vengono identificati in base alla posizione che occupano nella sequenza. Inoltre, mentre gli insiemi non contengono ripetizioni, lo stesso elemento può comparire più volte in posizioni diverse di una stessa sequenza.

ESEMPIO 2.1 (INSIEMI E SEQUENZE)
Per apprezzare la differenza, immaginate di considerare i caratteri tipografici come elementi di riferimento. Chiaramente questa dispensa costituisce una particolare sequenza di tali caratteri. Se invece prendiamo l'insieme dei caratteri che compaiono nella dispensa, otteniamo una collezione estremamente ridotta (presentabile in un paio di righe).

A volte converrà ipotizzare che tutti gli elementi che consideriamo appartengono a un *insieme universo* $\mathcal{U}$: quando necessario renderemo questa assunzione esplicita.

Usiamo lettere maiuscole come $A, B, C, \ldots$ per denotare gli insiemi, e lettere minuscole come $a, b, c, \ldots$ per denotarne gli elementi. L'usuale simbolo di *appartenenza* $\in$ permette di indicare, scrivendo $a \in A$, che l'elemento a appartiene all'insieme A; barrando il simbolo di appartenenza, cioè scrivendo $a \notin A$, indichiamo invece che a non appartiene ad A.

Ci sono vari modi per *definire* o *rappresentare* un insieme, cioè per indicare quali sono i suoi elementi. Per esempio, si può definire un insieme **per enumerazione** (oppure **in modo estensionale**) elencandone tutti gli elementi (racchiusi tra parentesi graffe e separati da virgole). Vediamo alcuni esempi:

ESEMPIO 2.2 (INSIEMI DEFINITI PER ENUMERAZIONE)
- *I giorni della settimana:* $\{$ *lunedì*, *domenica*, *giovedì*, *sabato*, *martedì*, *mercoledì*, *venerdì* $\}$.
- *Le ore in un giorno:* $\{0, 1, 2, 13, 14, 15, 16, 17, 18, 19, 20, 11, 12, 3, 4, 22, 6, 7, 8, 9, 10, 21, 5, 23\}$.

- *Le vocali:* $\{\mathsf{a},\mathsf{u},\mathsf{i},\mathsf{e},\mathsf{o}\}$.

Per ribadire che l'ordine degli elementi non ha alcuna importanza, abbiamo volutamente scritto gli insiemi sopra in modo da non rispettare l'ordine col quale siamo soliti elencare gli oggetti corrispondenti. Una versione del tutto equivalente, ma di più facile consultazione è riportata sotto:

- *I giorni della settimana:* $\{\mathsf{lunedì},\mathsf{martedì},\mathsf{mercoledì},\mathsf{giovedì},\mathsf{venerdì},\mathsf{sabato},\mathsf{domenica}\}$.
- *Le ore in un giorno:* $\{0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23\}$.
- *Le vocali:* $\{\mathsf{a},\mathsf{e},\mathsf{i},\mathsf{o},\mathsf{u}\}$.

E se gli insiemi sono molto grandi, o infiniti? Si usano i puntini sospensivi (...) per sottintendere la regola di enumerazione:

- *I minuti in un'ora:* $\{1,2,...,60\}$
- *I numeri da 1 a mille:* $\{1,2,...,1000\}$
- *I numeri pari positivi:* $\{2,4,6,...\}$
- *I caratteri alfanumerici:* $\{a,b,...,z,A,B,...,Z,0,1,...,9\}$

TERMINOLOGIA 2.3 (ALCUNI INSIEMI NOTEVOLI) *Introduciamo alcuni simboli standard per denotare degli insiemi che incontreremo spesso:*

- $\mathcal{U}$ *(l'insieme* ***universo*** *di riferimento).*
- $\varnothing = \{\}$ *(****l'insieme vuoto****).*
- $\mathbb{N} = \{0,1,2,...\}$ *(l'insieme dei numeri* ***naturali****).*
- $\mathbb{N}^+ = \{1,2,...\}$ *(l'insieme dei numeri* ***naturali positivi****).*
- $\mathbb{Z} = \{...,-2,-1,0,1,2,...\}$ *(l'insieme dei numeri* ***interi****).*

Invece di elencarne gli elementi, un insieme può essere rappresentato o definito **per proprietà** (oppure **in modo intensionale**), descrivendo una proprietà soddisfatta da tutti e soli i suoi elementi. Senza poter anticipare quanto vedremo nel capitolo sulla logica dei predicati (Capitolo 4), di seguito indichiamo con P una generica proprietà e con la notazione $P(a)$ il fatto che l'elemento $a \in \mathcal{U}$ gode della proprietà P (diciamo anche che a *soddisfa* P). Assumiamo inoltre che preso un elemento a e una proprietà P, o a soddisfa P, oppure no.[1]

Per esempio, per un insieme di persone, si potrebbe voler considerare la proprietà di *"essere nati nel 1993"* oppure la proprietà di *"avere il nome che inizia con la lettera 'A'"*; per un insieme di numeri, la proprietà di *"essere divisibile per* 2*"* (essere pari), oppure di *"essere maggiore di* 0*"* (essere positivi).

TERMINOLOGIA 2.4 (DEFINIZIONE DI INSIEMI PER PROPRIETÀ) *Useremo la seguente notazione per indicare l'insieme costituito da tutti gli elementi di un dato insieme X che godono di una certa proprietà P:*

$$A = \{a \mid a \in X \text{ e } P(a)\}$$

O più semplicemente:

$$A = \{a \in X \mid P(a)\}$$

O ancora più semplicemente, quando X è ovvio dal contesto (per esempio se X è l'universo $\mathcal{U}$*):*

$$A = \{a \mid P(a)\}$$

[1] Questo serve a escludere, per esempio, quei casi in cui si possa voler dire che la proprietà è soddisfatta al 70% oppure in cui la proprietà possa essere talvolta soddisfatta da un elemento e altre volte no. Questi casi non sono affrontati in queste note.

Per il momento descriveremo le proprietà usando il linguaggio naturale, ma più avanti nel corso (nel Capitolo 4) vedremo come essere più rigorosi e formali, sfruttando le formule della logica dei predicati.

ESEMPIO 2.5 (INSIEMI DEFINITI PER PROPRIETÀ)
Vediamo alcuni esempi:

- $\mathbb{N}^p = \{ n \in \mathbb{N}^+ \mid n \text{ è pari} \}$ *(l'insieme dei numeri* ***pari positivi****)*
- $\mathbb{N}^d = \{ n \in \mathbb{N}^+ \mid n \text{ è dispari} \}$ *(l'insieme dei numeri* ***dispari positivi****)*
- $\mathbb{P} = \{ p \in \mathbb{N}^+ \mid p \text{ è primo} \}$
- $A^* = \{ a_1 a_2 \dots a_n \mid n \in \mathbb{N} \text{ e } a_1, a_2, \dots, a_n \in A \}$ *(l'insieme di tutte le* ***sequenze finite****, di qualsiasi lunghezza (anche nulla), composte da elementi dell'insieme A)*
- $Exp_2 = \{ n \mid \text{esiste } k \in \mathbb{N} \text{ tale che } n = 2^k \}$ *(l'insieme delle potenze di 2)*
- $AR = \{ x \mid x \text{ è un'auto rossa} \}$ *(l'insieme di tutte le auto rosse).*

La *cardinalità* di un insieme offre una misura della sua "grandezza". Se A è un insieme contenente esattamente n elementi distinti tra loro (con $n \in \mathbb{N}$), diciamo che A è un insieme **finito** e che A ha **cardinalità** n. La cardinalità di un insieme A viene indicata con $|A|$. Per esempio, la cardinalità $|V|$ dell'insieme delle vocali $V = \{ \mathsf{a}, \mathsf{e}, \mathsf{i}, \mathsf{o}, \mathsf{u} \}$ è 5. Si noti invece che $|\varnothing| = 0$, dato che l'insieme vuoto non contiene nessun elemento.

Il concetto di cardinalità si può estendere a insiemi con un numero infinito di elementi, ma questo esula dagli argomenti di queste note.

2.1.1 I paradossi

La definizione di insieme che abbiamo dato è piuttosto intuitiva, ma poco precisa (per esempio siamo stati vaghi sul concetto di elemento... e lo resteremo). In particolare, un insieme potrebbe a sua volta essere visto come elemento (un anno è un insieme di mesi, ogni mese un insieme di giorni, ogni giorno un insieme di ore,...).

Tuttavia questa definizione conduce facilmente a *paradossi* (inconsistenze logiche) come evidenziato da Bertrand Russell nel 1902.

ESEMPIO 2.6 (IL PARADOSSO DI RUSSEL)
Sia $\mathbb{S}$ l'insieme di tutti gli insiemi X che non appartengono a sé stessi:

$$\mathbb{S} = \{ X \mid X \notin X \}$$

Ma essendo $\mathbb{S}$ un insieme, cosa possiamo dire di esso?

- *se $\mathbb{S} \notin \mathbb{S}$ allora l'insieme $\mathbb{S}$ gode della proprietà che caratterizza tutti gli elementi di $\mathbb{S}$, e quindi $\mathbb{S} \in \mathbb{S}$, in contrasto con l'ipotesi!*
- *se $\mathbb{S} \in \mathbb{S}$ allora per definizione si ha $\mathbb{S} \notin \mathbb{S}$ (perché tutti e soli gli elementi che soddisfano quella proprietà appartengono a $\mathbb{S}$), di nuovo in contrasto con l'ipotesi!*

Il problema all'origine del paradosso è quello di formalizzare il fatto che A è un insieme se e solo se possiamo stabilire con esattezza (senza contraddizioni) se $a \in A$ oppure no, per ogni elemento a dell'universo $\mathcal{U}$ fissato. Una trattazione approfondita che eviti tali paradossi esula dagli obiettivi di queste note: accenniamo solo che esistono teorie assiomatiche degli insiemi che scongiurano la presenza di paradossi. Per semplicità in seguito faremo sempre riferimento alla definizione *intuitiva* di insieme.

2.2 Confrontare gli insiemi

Poiché un insieme è univocamente determinato dagli elementi che gli appartengono, si può usare questo criterio per confrontare due insiemi.

DEFINIZIONE 2.2 (INCLUSIONE, UGUAGLIANZA E DISUGUAGLIANZA TRA INSIEMI)
Dati due insiemi A e B, si dice che A è un ***sottoinsieme*** *di B, indicato con $A \subseteq B$, se e solo se ogni elemento di A è anche elemento di B. In questo caso diciamo anche che A è* ***contenuto*** *in B.*

Diciamo inoltre che A e B sono ***uguali****, scritto $A = B$, se e solo se hanno esattamente gli stessi elementi. Ovviamente, $A = B$ se e solo se valgono sia $A \subseteq B$ che $B \subseteq A$. Viceversa, diciamo che A e B sono* ***diversi****, scritto $A \neq B$, se e solo se esiste almeno un elemento che è contenuto in uno dei due insiemi, ma non nell'altro.*

Diciamo anche che A è un ***sottoinsieme stretto*** *di B (oppure è* ***contenuto strettamente*** *in B), indicato con $A \subset B$, se e solo se $A \subseteq B$ e $A \neq B$.*

Infine diciamo che A e B sono ***disgiunti*** *se e solo se non hanno alcun elemento in comune.*

Dalle definizioni appena introdotte deriva che possiamo sfruttare la relazione di appartenenza ($\in$) nel modo seguente per confrontare due insiemi:

- per dimostrare che $A \subseteq B$ basta mostrare che ogni elemento a che appartiene ad A appartiene anche a B (si dimostra che se $a \in A$ allora $a \in B$)
- per dimostrare che $A = B$ si può mostrare che ogni elemento di A appartiene a B e viceversa, ogni elemento di B appartiene ad A (si dimostrano separatamente le due inclusioni $A \subseteq B$ e $B \subseteq A$)
- per dimostrare che $A \subset B$ si può mostrare che ogni elemento di A appartiene a B, ma che esiste un elemento di B che non appartiene ad A (si dimostra che $A \subseteq B$ e si fornisce almeno un elemento $b \in B$ tale che $b \notin A$)
- per dimostrare che A e B sono disgiunti si deve mostrare che ogni elemento di A non appartiene a B, e che ogni elemento di B non appartiene ad A

Nell'Esempio 4.13 vedremo come sia possibile descrivere in modo formale le tecniche di dimostrazione appena elencate, vedendo in particolare il caso dell'inclusione stretta.

Vediamo alcuni esempi di confronti tra insiemi, per ognuno dei quali forniamo una possibile giustificazione.

ESEMPIO 2.7 (UGUAGLIANZE E INCLUSIONI TRA INSIEMI)

1. $\mathbb{N}^+ \subseteq \mathbb{N}$:
   infatti se $n \in \mathbb{N}^+$ allora n è un naturale positivo, ma allora è un naturale, e quindi $n \in \mathbb{N}$.

2. $\{ n \in \mathbb{N}^+ \mid n \geq n^2 \} = \{ 1 \}$:
   infatti il numero 1 (unico elemento del secondo insieme) soddisfa la proprietà che definisce il primo insieme (perché $1 \geq 1^2$) e quindi $\{ 1 \} \subseteq \{ n \in \mathbb{N}^+ \mid n \geq n^2 \}$; d'altra parte nessun altro elemento di $\mathbb{N}^+$ soddisfa la proprietà, visto che $2 < 2^2$, e che se $0 < n < n^2$ allora segue che $n+1 < n^2+1 < n^2+2n+1 = (n+1)^2$; questo mostra l'altra inclusione.

3. $\{ n+m \mid n \in \mathbb{N}^d, m \in \mathbb{N}^d \} = \mathbb{N}^p$:
   infatti la somma di due numeri dispari è un numero pari (quindi $\{ n+m \mid n \in \mathbb{N}^d, m \in \mathbb{N}^d \} \subseteq \mathbb{N}^p$), e per ogni numero pari $n > 0$ vale $n = (n-1)+1$, dove $n-1$ ed 1 sono chiaramente numeri naturali dispari (quindi $\{ n+m \mid n \in \mathbb{N}^d, m \in \mathbb{N}^d \} \supseteq \mathbb{N}^p$).

   Si noti che l'uguaglianza sarebbe falsa se $\mathbb{N}^p$ contenesse lo zero.

4. *Dato un qualsiasi insieme A, vale $\varnothing \subseteq A$.*
   Infatti dovremmo mostrare che per ogni elemento a tale che $a \in \varnothing$, vale $a \in A$. Ma poiché non ci sono elementi in $\varnothing$, non bisogna dimostrare nulla e l'inclusione vale in modo banale.

   Questa argomentazione potrebbe sembrare poco convincente a una prima lettura. Facciamo vedere, in modo equivalente, che non è vero che $\varnothing \not\subseteq A$. Infatti, per mostrare che $\varnothing \not\subseteq A$ dovremmo trovare un elemento di $\varnothing$ che non è in A. Ma dato che non ci sono elementi in $\varnothing$, questo è necessariamente falso, e quindi $\varnothing \subseteq A$.

5. *Dati tre insiemi A, B e C, se $A \subset B$ e $B \subseteq C$, allora $A \subset C$.*
   Dobbiamo mostrare, assumendo che $A \subset B$ e $B \subseteq C$, che (1) per ogni $a \in A$ vale $a \in C$, e che (2) esiste $c \in C$ tale che $c \notin A$. Infatti, per (1), se $a \in A$ allora (visto che vale $A \subset B$) $a \in B$, e quindi (visto che vale $B \subseteq C$) $a \in C$. D'altra parte, per (2), visto che vale $A \subset B$, sappiamo che esiste un elemento $b \in B$ tale che $b \notin A$; ma poiché vale $B \subseteq C$ sappiamo che $b \in C$ e quindi scegliamo $c = b$.

2.3 Comporre insiemi

A partire da alcuni insiemi possiamo definirne altri selezionando elementi comuni oppure che compaiono in un insieme ma non nell'altro, oppure in uno qualsiasi degli insiemi.

DEFINIZIONE 2.3 (OPERAZIONI SU INSIEMI)

- *L'**intersezione** di due insiemi A e B, denotata $A \cap B$, è l'insieme che contiene (tutti e soli) gli elementi che appartengono sia ad A che a B. In formule, $A \cap B = \{ x \mid x \in A \text{ e } x \in B \}$.*
- *L'**unione** di due insiemi A e B, denotata $A \cup B$, è l'insieme che contiene (tutti e soli) gli elementi che sono elementi di A oppure di B (o anche di entrambi). In formule, $A \cup B = \{ x \mid x \in A \text{ oppure } x \in B \}$.*
- *Il **complemento** di un insieme A (rispetto all'insieme universo $\mathcal{U}$), scritto $\overline{A}$, è l'insieme che contiene (tutti e soli) gli elementi dell'universo che non appartengono ad A. In formule, $\overline{A} = \{ x \mid x \in \mathcal{U} \text{ e } x \notin A \}$ oppure, lasciando l'universo implicito, $\overline{A} = \{ x \mid x \notin A \}$.*
- *La **differenza** di un insieme A con un insieme B, scritta $A \setminus B$, è l'insieme che contiene (tutti e soli) gli elementi di A che non stanno in B. In formule, $A \setminus B = \{ x \mid x \in A \text{ e } x \notin B \}$.*

  *Nel caso particolare in cui $B \subseteq A$, si dice anche che $A \setminus B$ è il **complemento** di B rispetto a A.*

2.3.1 I diagrammi di Eulero-Venn

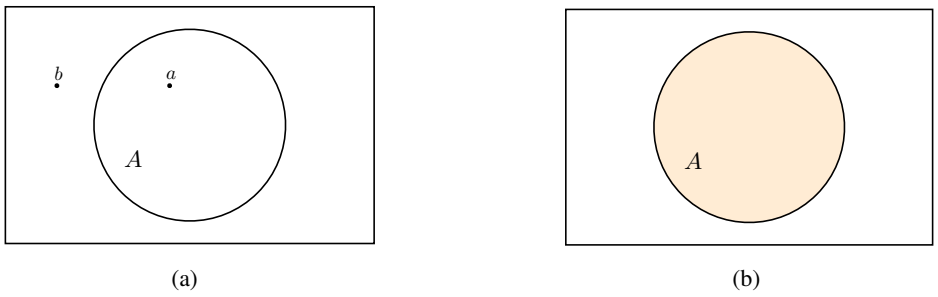
I diagrammi di Eulero-Venn sono un utile strumento per facilitare il ragionamento sulle relazioni tra insiemi e sulle operazioni tra insiemi con una notazione grafica e intuitiva. In generale, l'uso dei diagrammi non può in alcun modo sostituire le dimostrazioni di certe proprietà. Piuttosto, se ne consiglia l'uso per verificare rapidamente se una certa relazione tra insiemi sia da ritenersi valida oppure no prima di procedere con la dimostrazione. L'uso dei diagrammi di Eulero-Venn è altresì utile per identificare opportuni controesempi quando le dimostrazioni non siano possibili.

La notazione grafica di Eulero-Venn si basa sui seguenti principi:

- L'insieme universo $\mathcal{U}$ viene rappresentato da un rettangolo.
- Gli elementi vengono rappresentati come punti all'interno del rettangolo.
- Dentro il rettangolo usiamo circonferenze, ovali e altre forme per rappresentare gli insiemi.
- Se A è incluso in B allora la forma che rappresenta A è posta all'interno della forma che rappresenta B.
- Se A e B sono insiemi disgiunti allora le loro forme non si intersecano.
- Le aree di alcune forme possono essere riempite con colori o tratteggi diversi per essere messe in evidenza.

Per esempio, in Figura 2.1(a) vengono mostrati un insieme A e due elementi a e b con $a \in A$ e $b \notin A$ e in Figura 2.1(b) viene messo in evidenza l'insieme A usando un riempimento colorato.

Le operazioni su insiemi viste in precedenza possono essere esemplificate efficacemente usando i diagrammi di Eulero-Venn. In questo caso nelle figure bisogna disporre le forme in modo da rappresentare tutte le possibili combinazioni di appartenenza e non appartenenza di elementi, e il riempimento colorato viene usato per indicare l'area che rappresenta l'insieme risultante dall'operazione. Per esempio, con due insiemi A e B, bisogna rappresentare quattro aree nel diagramma, corrispondenti ai casi: 1) $a \in A$ e $a \in B$; 2) $a \in A$ e $a \notin B$; 3) $a \notin A$ e $a \in B$; 4) $a \notin A$ e $a \notin B$ (si veda la Figura 2.2 dove il cerchio di sinistra rappresenta l'insieme A e quello



(a) (b)

Figura 2.1: Un insieme A.

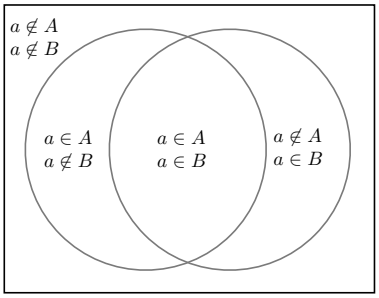


Figura 2.2: Caratterizzazione delle aree di un diagramma di Eulero-Venn con due insiemi.

di destra l'insieme B). In generale, se sono coinvolti n insiemi servono 2^n aree. Questo rende molto complicato e poco efficace usare i diagrammi di Eulero-Venn che coinvolgano quattro ($2^4 = 16$ aree) o più insiemi.

Le operazioni di intersezione, unione, complemento e differenza tra insiemi sono rappresentate rispettivamente nelle Figure 2.3(a), 2.3(b), 2.3(c), e 2.3(d).[2]

I diagrammi evidenziano alcuni fatti importanti, facilmente derivabili anche dalle definizioni, e che sono utili per ragionare sulle relazioni tra insiemi. Presi due insiemi A e B qualsiasi si ha che:

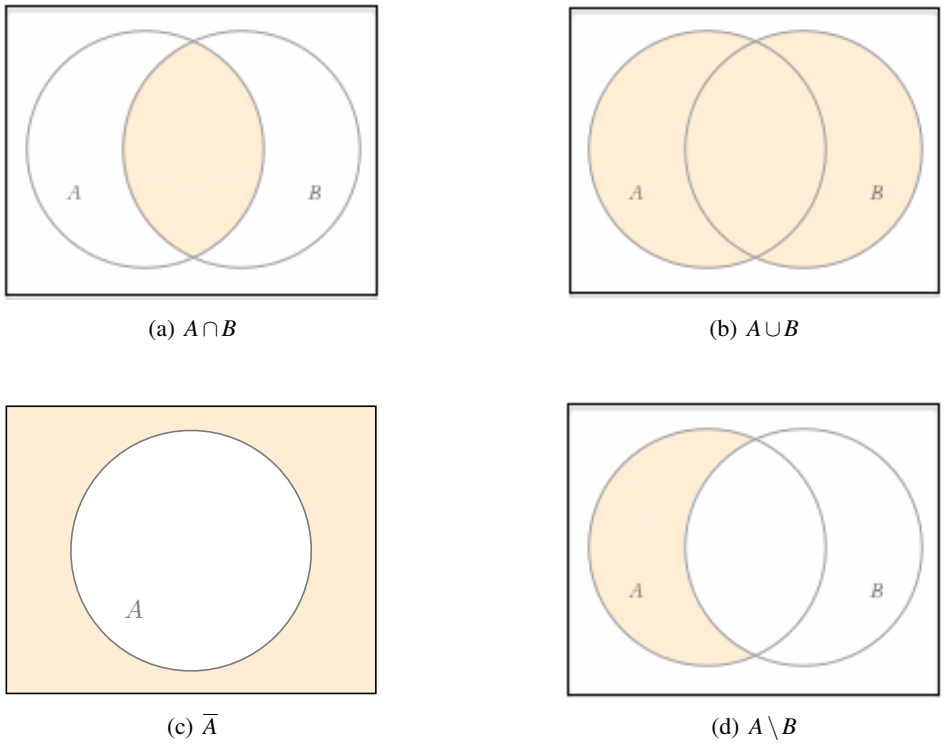
1. $(A \cap B) \subseteq A$, cioè ogni elemento di $A \cap B$ appartiene anche ad A, e analogamente $(A \cap B) \subseteq B$ (Fig. 2.3(a)).
2. $A \subseteq (A \cup B)$, cioè ogni elemento di A appartiene anche ad $A \cup B$; e analogamente $B \subseteq (A \cup B)$ (Fig. 2.3(b)).
3. $A \cap \overline{A} = \varnothing$, cioè un insieme e il suo complemento sono disgiunti; inoltre $A \cup \overline{A} = \mathcal{U}$ (Fig. 2.3(c)).
4. $(A \setminus B) \subseteq A$, cioè ogni elemento di $A \setminus B$ appartiene necessariamente ad A (Fig. 2.3(d)).

A titolo di curiosità riportiamo in Figura 2.4(a) il diagramma di Eulero-Venn che illustra l'intersezione di quattro insiemi e in Figura 2.4(b) quello per rappresentare l'intersezione di cinque insiemi.

ESEMPIO 2.8 (COMPOSIZIONE DI INSIEMI)

1. $\{1,2,3\} \cap \{1,3,5\} = \{1,3\}$: *infatti è immediato verificare che l'insieme* $\{1,3\}$ *contiene tutti e soli gli elementi che compaiono sia nell'insieme* $\{1,2,3\}$ *che nell'insieme* $\{1,3,5\}$.
2. $\{1,2,3\} \cup \{1,3,5\} = \{1,2,3,5\}$: *infatti l'insieme* $\{1,2,3,5\}$ *contiene tutti e soli gli elementi che compaiono nell'insieme* $\{1,2,3\}$ *oppure nell'insieme* $\{1,3,5\}$.
3. $\{1,2,3\} \setminus \{1,3,5\} = \{2\}$: *infatti l'insieme* $\{2\}$ *contiene tutti e soli gli elementi che compaiono nell'insieme* $\{1,2,3\}$ *ma non nell'insieme* $\{1,3,5\}$.
4. $\{1,3,5\} \setminus \{1,2,3\} = \{5\}$: *infatti l'insieme* $\{5\}$ *contiene tutti e soli gli elementi che compaiono nell'insieme* $\{1,3,5\}$ *ma non nell'insieme* $\{1,2,3\}$.

[2] I diagrammi sono stati prodotti utilizzando lo strumento `http://www.wolframalpha.com`.



(a) $A \cap B$ (b) $A \cup B$

(c) $\overline{A}$ (d) $A \setminus B$

Figura 2.3: Le operazioni su insiemi illustrate coi diagrammi di Eulero-Venn.

5. *Gli esempi 3 e 4 mostrano che in generale* $A \setminus B \neq B \setminus A$.

6. $\mathbb{N}^p \cup \mathbb{N}^d = \mathbb{N}^+$*: infatti possiamo verificare le due inclusioni separatamente notando che: 1) preso un numero* $n \in \mathbb{N}^p \cup \mathbb{N}^d$*, si ha che o* $n \in \mathbb{N}^p$ *e allora* $n \in \mathbb{N}^+$ *perché* $\mathbb{N}^p \subseteq \mathbb{N}^+$*, oppure* $n \in \mathbb{N}^d$ *e allora* $n \in \mathbb{N}^+$ *perché* $\mathbb{N}^d \subseteq \mathbb{N}^+$*; 2) preso un numero positivo* $n \in \mathbb{N}^+$*, si ha che* n *o è pari e quindi* $n \in \mathbb{N}^p \subseteq \mathbb{N}^p \cup \mathbb{N}^d$*, oppure* n *è dispari e quindi* $n \in \mathbb{N}^d \subseteq \mathbb{N}^p \cup \mathbb{N}^d$.

7. $\mathbb{N}^p \cap \mathbb{N}^d = \varnothing$*: infatti nessun numero positivo è contemporaneamente pari e dispari (l'inclusione* $\varnothing \subseteq \mathbb{N}^p \cap \mathbb{N}^d$ *è ovvia, si veda l'Esempio 2.7(4)).*

8. $\mathbb{N} \cup \mathbb{Z} = \mathbb{Z}$*: infatti possiamo verificare le due inclusioni separatamente notando che: 1) preso un numero* $n \in \mathbb{N} \cup \mathbb{Z}$*, si ha che o* $n \in \mathbb{N}$ *e allora* $n \in \mathbb{Z}$ *perché* $\mathbb{N} \subseteq \mathbb{Z}$*, oppure* $n \in \mathbb{Z}$*; 2) banalmente* $\mathbb{Z} \subseteq \mathbb{N} \cup \mathbb{Z}$ *per quanto osservato sopra a proposito delle relazioni tra insiemi costruiti per unione.*

   Lo stesso ragionamento può essere generalizzato per dimostrare che presi due qualsiasi insiemi $A \subseteq B$ *si ha che* $(A \cup B) = B$.

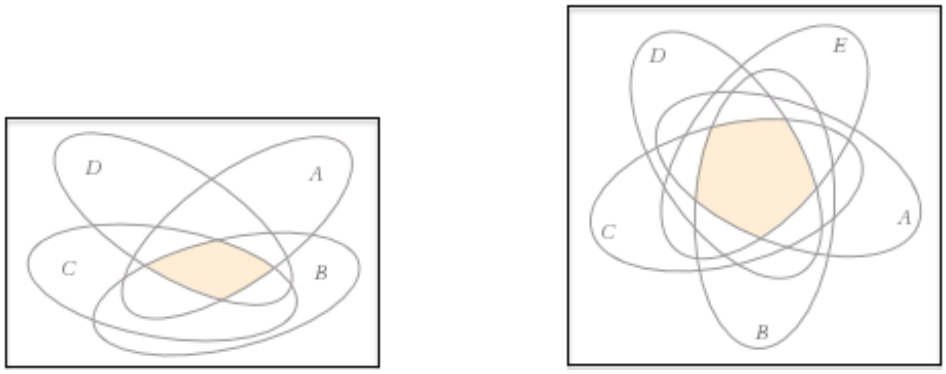
9. $\mathbb{N} \cap \mathbb{Z} = \mathbb{N}$*: infatti possiamo verificare le due inclusioni separatamente notando che: 1) banalmente* $\mathbb{N} \cap \mathbb{Z} \subseteq \mathbb{N}$ *per quanto osservato sopra a proposito delle relazioni tra insiemi costruiti per intersezione; 2) preso un numero* $n \in \mathbb{N}$*, si ha che* $n \in \mathbb{Z}$ *perché* $\mathbb{N} \subseteq \mathbb{Z}$*, e quindi* $n \in \mathbb{N} \cap \mathbb{Z}$.

   Lo stesso ragionamento può essere generalizzato per dimostrare che presi due qualsiasi insiemi $A \subseteq B$ *si ha che* $(A \cap B) = A$.

10. $\mathbb{N} \setminus \mathbb{N}^+ = \{0\}$*: infatti* 0 *è l'unico numero naturale non positivo.*

11. $\overline{\mathbb{N}^+} = \{0\}$*, assumendo come universo di riferimento l'insieme* $\mathbb{N}$*: l'uguaglianza equivale a* $\mathbb{N} \setminus \mathbb{N}^+ = \{0\}$.

NOTA 2.9 *In generale, se A e B sono insiemi finiti si ha* $|A \cup B| \leq |A| + |B|$*. Sapreste spiegare perché?*



(a) $((A \cap B) \cap C) \cap D$ (b) $(((A \cap B) \cap C) \cap D) \cap E$

Figura 2.4: Diagrammi di Eulero-Venn con quattro e cinque insiemi.

2.4 Dimostrazione di uguaglianze di insiemi

Componendo insiemi tramite le operazioni viste è possibile ottenere lo stesso risultato in modi diversi. Per esempio, è immediato convincersi che per qualunque coppia di insiemi A e B, vale $A \cup B = B \cup A$. Altre uguaglianze sono meno immediate, per esempio il fatto che $\overline{(A \cup \overline{B})} = B \cap \overline{A}$ è vera per ogni A e B.

L'obiettivo di questa sezione è quello di discutere alcune tecniche per dimostrare uguaglianze del tipo $E_1 = E_2$, dove E_1 ed E_2 sono espressioni costruite a partire da insiemi generici (indicati con A, B, C, ...) applicando le operazioni su insiemi introdotte nella Definizione 2.3. Affinché l'uguaglianza in questione valga, bisogna che essa sia vera per ogni possibile sostituzione degli insiemi generici in essa contenuti con degli insiemi concreti. Per esempio, l'uguaglianza $A \cup B = A \cap B$ non è vera. Infatti anche se essa vale per opportune scelte di A e B (per esempio se $A = B = \mathbb{N}$), essa non vale per altre scelte (per esempio se $A = \mathbb{N}$ e $B = \varnothing$, abbiamo $A \cup B = \mathbb{N} \cup \varnothing = \mathbb{N}$, mentre $A \cap B = \mathbb{N} \cap \varnothing = \varnothing$, e ovviamente $\mathbb{N} \neq \varnothing$).

2.4.1 Le leggi sugli insiemi

Presentiamo di seguito alcune uguaglianze notevoli tra insiemi, che chiameremo anche *leggi*, rimandando alle prossime sezioni alcune considerazioni su come possano essere dimostrate.

PROPOSIZIONE 1 (LEGGI SU UNIONE, INTERSEZIONE, COMPLEMENTO E DIFFERENZA)
Per ogni insieme A, B e C nell'universo $\mathcal{U}$ valgono le seguenti uguaglianze:

Leggi su intersezione e unione

$A \cap A = A$	$A \cup A = A$	*(idempotenza)*
$A \cap B = B \cap A$	$A \cup B = B \cup A$	*(commutatività)*
$A \cap (B \cap C) = (A \cap B) \cap C$	$A \cup (B \cup C) = (A \cup B) \cup C$	*(associatività)*
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	*(distributività a sinistra)*
$(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$	$(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$	*(distributività a destra)*

Leggi su complemento e differenza

$\overline{(\overline{A})} = A$		*(doppio complemento)*
$\overline{(A \cap B)} = \overline{A} \cup \overline{B}$	$\overline{(A \cup B)} = \overline{A} \cap \overline{B}$	*(De Morgan)*
$A \setminus B = A \cap \overline{B}$		*(differenza)*

Si osservi la struttura delle leggi sopra elencate, che esprimono proprietà fondamentali degli operatori su insiemi. Per ogni operatore vengono presentate prima le leggi che descrivono l'effetto di una o più applicazioni

dello stesso operatore (*idempotenza*, *associatività*, *commutatività*, *doppio complemento*). Poi vengono elencate leggi che descrivono l'interazione di un operatore con quelli introdotti precedentemente (*distributività*, *De Morgan*). Infine la *legge della differenza* mostra che la differenza è un *operatore derivato*, perché si può esprimere in termini di intersezione e complemento, permettendoci di eliminarla da una qualunque espressione.[3]

Alcune delle leggi presentate sono del tutto ovvie (come *idempotenza* e *commutatività*). Altre, come *distributività* e *De Morgan* sono meno evidenti. Comunque per giustificare in modo *formale* queste leggi bisogna fornirne una **prova** o **dimostrazione** che mostri che l'uguaglianza vale sempre, qualunque siano gli insiemi considerati. Vedremo alcuni esempi di dimostrazioni (sia di tipo discorsivo che grafiche) nelle prossime due sezioni. Successivamente sfrutteremo le leggi appena introdotte per dimostrare uguaglianze più complesse, utilizzando la tecnica di dimostrazione per sostituzione presentata nella Sezione 1.4.

ESEMPIO 2.10 (CONTROESEMPI ALL'UGUAGLIANZA DI INSIEMI)
Naturalmente non tutte le uguaglianze che possiamo scrivere sono vere. Per esempio, non è vera, in generale, la seguente uguaglianza:

$$(A \cap B) \cup (C \cap D) = (A \cup B) \cap (C \cup D)$$

Per confutarla è sufficiente fornire un controesempio, il più semplice che riusciamo a individuare. Nello specifico, è immediato verificare che l'uguaglianza non vale quando si prenda $A = C = \{1\}$ *e* $B = D = \varnothing$.

2.4.2 Leggi su insiemi notevoli

Vi sono alcune leggi che descrivono il comportamento degli operatori con due insiemi notevoli, l'universo $\mathcal{U}$ e l'insieme vuoto $\varnothing$.

PROPOSIZIONE 2 (LEGGI SU INSIEMI NOTEVOLI)
Per ogni insieme A *nell'universo* $\mathcal{U}$ *valgono le seguenti uguaglianze:*

Leggi su $\varnothing$ ***e*** $\mathcal{U}$		
$A \cap \mathcal{U} = A$	$A \cup \varnothing = A$	*(elemento neutro)*
$A \cap \varnothing = \varnothing$	$A \cup \mathcal{U} = \mathcal{U}$	*(elemento assorbente)*
$\overline{\varnothing} = \mathcal{U}$	$\overline{\mathcal{U}} = \varnothing$	*(complemento)*
$A \cap \overline{A} = \varnothing$	$A \cup \overline{A} = \mathcal{U}$	*(complementarità)*

2.4.3 Le dimostrazioni discorsive

Le dimostrazioni che probabilmente conoscete meglio alternano la notazione matematica (non ambigua, universale) con frasi in linguaggio naturale (ambiguo, deve essere tradotto a seconda della nazionalità del lettore). Sono quelle più comuni nei libri e cercano di rendere leggibili e meno tediose le prove puramente formali, guidando il lettore ma saltando alcuni passaggi logici del tutto ovvi. Le dimostrazioni discorsive, se corrette, possono sempre essere completate con i passaggi saltati e tradotte nel linguaggio della matematica per ottenere delle prove formali (non ambigue, universalmente leggibili e verificabili) del tutto equivalenti.

Uno degli obiettivi di queste note è proprio quello di conciliare le due visioni, discorsiva e formale, per poter costruire argomentazioni solide, per presentarle ad altri e per verificare quelle di altri.

Vediamo, come esempio, la dimostrazione in stile discorsivo della seconda legge di De Morgan.

ESEMPIO 2.11 (DIMOSTRAZIONE DELLA SECONDA LEGGE DI DE MORGAN: $\overline{(A \cup B)} = \overline{A} \cap \overline{B}$)
Per dimostrare l'uguaglianza, come ricordato nella Sezione 2.2, possiamo far vedere (qualsiasi insiemi A, B *si considerino) che ogni elemento di* $\overline{(A \cup B)}$ *è anche elemento di* $\overline{A} \cap \overline{B}$ *e viceversa.*

Possiamo procedere dimostrando le due inclusioni separatamente:

1. $\overline{(A \cup B)} \subseteq \overline{A} \cap \overline{B}$

[3] Analogamente si potrebbe fare per l'unione, che è esprimibile con intersezione e complemento, oppure per l'intersezione, esprimibile con unione e complemento, ma eviteremo di farlo come di consuetudine per maneggiare espressioni più semplici.

2. $\overline{(A \cup B)} \supseteq \overline{A} \cap \overline{B}$

- *Per prima cosa facciamo vedere che* $\overline{(A \cup B)} \subseteq \overline{A} \cap \overline{B}$.
  Preso un qualsiasi $x \in \overline{(A \cup B)}$, *dobbiamo mostrare che* $x \in \overline{A} \cap \overline{B}$.
  Per definizione di complemento, se $x \in \overline{(A \cup B)}$ *vuol dire che* $x \notin A \cup B$. *Quindi* $x \notin A$ *e* $x \notin B$.
  Dato che $x \notin A$, *per definizione di complemento si ha* $x \in \overline{A}$.
  Analogamente, dato che $x \notin B$, *per definizione di complemento si ha* $x \in \overline{B}$.
  Ma allora $x \in \overline{A} \cap \overline{B}$ *e abbiamo finito.*
- *Resta da far vedere che* $\overline{A} \cap \overline{B} \subseteq \overline{(A \cup B)}$.
  Prendiamo un qualsiasi elemento $y \in \overline{A} \cap \overline{B}$. *Dobbiamo far vedere che* $y \in \overline{(A \cup B)}$.
  Dato che $y \in \overline{A} \cap \overline{B}$, *per definizione di intersezione si ha che* $y \in \overline{A}$ *e* $y \in \overline{B}$.
  Dunque, per definizione di complemento, si ha $y \notin A$ *e* $y \notin B$.
  Ma se y *non appartiene a* A *e non appartiene a* B *allora non appartiene alla loro unione, quindi* $y \notin A \cup B$.
  Per definizione di complemento, questo vuol dire che $y \in \overline{(A \cup B)}$ *e abbiamo finito.*

Si noti che le due dimostrazioni sono composte dagli stessi passaggi ma in ordine inverso: in questi casi non occorre dimostrare separatamente le due inclusioni, ma basta una sequenza di equivalenze logiche (dette "se-e-solo-se")

2.4.4 Le dimostrazioni grafiche

In molti casi i diagrammi di Eulero-Venn permettono di presentare prove *visive*, facili da seguire e convincenti anche per chi non abbia basi matematiche.

ESEMPIO 2.12 (PROPRIETÀ DELL'INCLUSIONE CON DIAGRAMMI DI EULERO-VENN)
La Figura 2.5 mostra in modo intuitivo e diretto il fatto che se $A \subseteq B$, *allora*

1. *se* $a \in A$ *allora* $a \in B$;
2. *se* $c \notin B$ *allora* $c \notin A$.

Naturalmente entrambi questi fatti derivano direttamente dalla definizione di inclusione tra insieme.

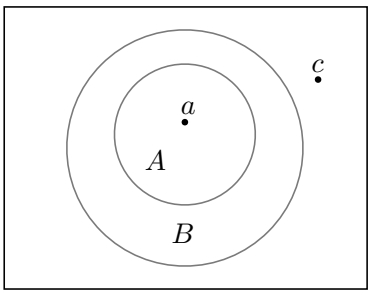
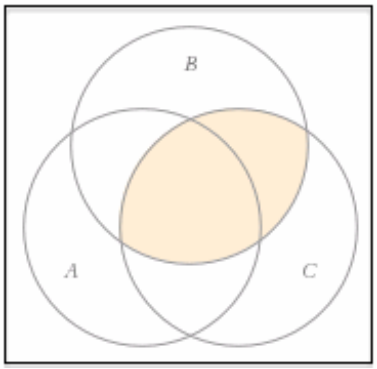
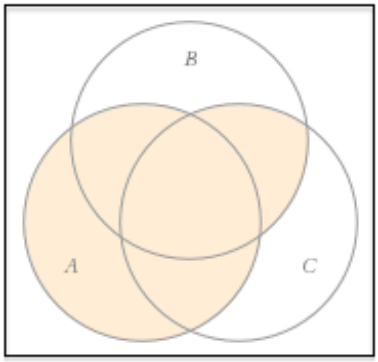


Figura 2.5: Proprietà dell'inclusione con diagrammi di Eulero-Venn

Come sempre, ricordate che le dimostrazioni grafiche sono più intuitive che convincenti: dovrebbero essere sempre accompagnate da una dimostrazione più precisa. Comunque si applicano bene a uguaglianze dirette che coinvolgano fino a tre insiemi.

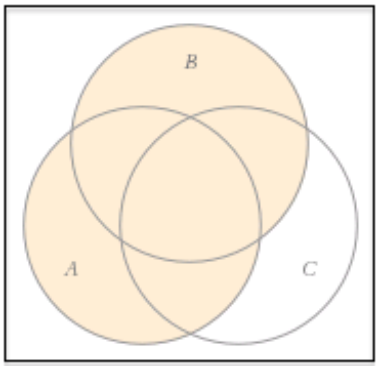


(a) $B \cap C$

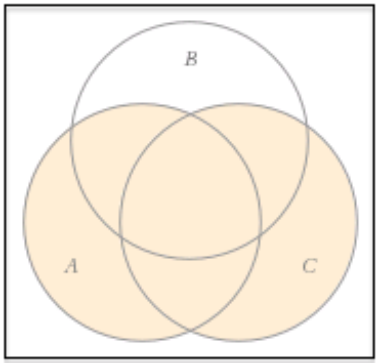


(b) $A \cup (B \cap C)$

Figura 2.6: Costruzione per passi del diagramma di Eulero-Venn per l'insieme $A \cup (B \cap C)$.



(a) $A \cup B$



(b) $A \cup C$

Figura 2.7: Costruzione per passi del diagramma di Eulero-Venn per l'insieme $(A \cup B) \cap (A \cup C)$.

ESEMPIO 2.13 (DIMOSTRAZIONE DI $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ CON DIAGRAMMI DI EULERO-VENN)
La dimostrazione procede confrontando due diagrammi di Eulero-Venn: nel primo si evidenzia l'area corrispondente al termine che compare a sinistra dell'uguaglianza da dimostrare; nel secondo si evidenzia l'area corrispondente al termine destro; e infine si osserva che le due aree evidenziate coincidono.

Per costruire il diagramma di Eulero-Venn per $A \cup (B \cap C)$, procediamo per passi: partendo dal diagramma che rappresenta i tre insiemi A, B e C, evidenziamo dapprima l'area corrispondente all'intersezione tra B e C (Figura 2.6(a)) e successivamente l'area ottenuta dall'unione dell'insieme A con l'area precedentemente individuata (Figura 2.6(b)). Si noti che l'area comprende tutto l'insieme A più la parte in comune tra B e C.

Procediamo analogamente per costruire il diagramma di Eulero-Venn corrispondente a $(A \cup B) \cap (A \cup C)$: partendo dal diagramma che rappresenta i tre insiemi A, B e C, evidenziamo dapprima l'area corrispondente all'unione tra A e B (Figura 2.7(a)), poi quella corrispondente all'unione tra A e C (Figura 2.7(b)) e infine coloriamo l'area ottenuta dall'intersezione tra le aree precedentemente individuate, scoprendo che essa coincide con l'area evidenziata in Figura 2.6(b).

I diagrammi di Eulero-Venn possono anche essere utili per trovare controesempi.

ESEMPIO 2.14 (USO DI DIAGRAMMI PER INDIVIDUARE CONTROESEMPI)
La dimostrazione per identificare un controesempio all'ugualianza di insiemi procede confrontando due diagrammi di Eulero-Venn: nel primo si evidenzia l'area corrispondente al termine sinistro; nel secondo si evidenzia l'area corrispondente al termine destro; e infine, dopo aver osservato che le due aree evidenziate non coincidono si esibisce un controesempio che popola una delle aree ma non l'altra.

Dimostriamo con i diagrammi di Eulero-Venn che in generale

$$A \cup (B \cap C) \neq (A \cup B) \cap C$$

Il diagramma di Eulero-Venn per $A \cup (B \cap C)$ è quello visto in Figura 2.6(b) e riportato in Figura 2.8(a). Quello per $(A \cup B) \cap C$ si ottiene facilmente a partire dal diagramma in Figura 2.7(a), evidenziando l'area in

(a) $A \cup (B \cap C)$ (b) $(A \cup B) \cap C$

Figura 2.8: Diagrammi di Eulero-Venn per gli insiemi $A \cup (B \cap C)$ e $(A \cup B) \cap C$.

comune tra $A \cup B$ e C (Figura 2.8(b)). È immediato notare che le aree evidenziate nei due diagrammi non coincidono e che quella nel secondo diagramma (Figura 2.8(b)) è contenuta strettamente in quella del primo diagramma (Figura 2.8(a)). Possiamo quindi dedurre che

$$A \cup (B \cap C) \supseteq (A \cup B) \cap C$$

ma non il viceversa. A questo punto, per costruire un controesempio all'uguaglianza delle due espressioni, basta popolare con un elemento una delle aree che sono colorate nel primo diagramma ma non nel secondo. Per esempio, possiamo prendere $A = \{1\}$ e $B = C = \varnothing$, da cui si ha $A \cup (B \cap C) = \{1\}$ e $(A \cup B) \cap C = \varnothing$.

2.4.5 Le dimostrazioni (formali) per sostituzione

La tecnica di dimostrazione per sostituzione, introdotta nella Sezione 1.4 per dimostrare uguaglianze algebriche, può essere usata in modo del tutto analogo per dimostrare uguaglianze di insiemi, sfruttando come giustificazioni le leggi della Sezione 2.4.1, o anche le nuove uguaglianze già dimostrate. Vediamo alcuni esempi di dimostrazioni di questo tipo.

ESEMPIO 2.15 (DIMOSTRAZIONE DI $A \cup (A \cap B) = A \cap (A \cup B)$)
Dimostriamo per sostituzione che per ogni A, B:

$$A \cup (A \cap B) = A \cap (A \cup B)$$

Partiamo dal membro sinistro dell'uguaglianza, e mostriamo che si può trasformare nel membro destro con una sequenza di uguaglianze in cui ad ogni passo una sottoespressione viene sostituita con una equivalente. Come giustificazione di ogni passaggio indichiamo la legge applicata.

$$\begin{aligned} & A \cup (A \cap B) \\ = & \quad \{ \textit{(distributività)} \} \\ & \underline{(A \cup A)} \cap (A \cup B) \\ = & \quad \{ \textit{(idempotenza), applicata alla sotto-formula sottolineata} \} \\ & A \cap (A \cup B) \end{aligned}$$

ESEMPIO 2.16 (DIMOSTRAZIONE DI $\overline{(A \cup \overline{B})} = B \cap \overline{A}$)

$$\begin{aligned} & \underline{\overline{(A \cup \overline{B})}} \\ = & \quad \{ \textit{(De Morgan)} \} \\ & \overline{A} \cap \underline{\overline{(\overline{B})}} \\ = & \quad \{ \textit{(doppio complemento)} \} \\ & \overline{A} \cap B \\ = & \quad \{ \textit{(commutatività)} \} \\ & B \cap \overline{A} \end{aligned}$$

ESEMPIO 2.17 (DIMOSTRAZIONE DI $A \cap (B \setminus C) = (A \cap B) \setminus C$)

$$
\begin{aligned}
& A \cap \underline{(B \setminus C)} \\
= \quad & \{ \textit{(legge della differenza)} \} \\
& A \cap (B \cap \overline{C}) \\
= \quad & \{ \textit{(associatività)} \} \\
& (A \cap B) \cap \overline{C} \\
= \quad & \{ \textit{(legge della differenza), al contrario} \} \\
& (A \cap B) \setminus C
\end{aligned}
$$

2.5 Esercizi

2.5.1 Esercizi di comprensione

2.5.1.1 È vero che la lunghezza di questa frase è uguale alla cardinalità dell'insieme dei caratteri che la compongono? Perché?

2.5.1.2 È vero che mentre gli interi 83.348 e 3.844 sono diversi gli insiemi delle loro cifre coincidono?

2.5.1.3 È vero che esiste un insieme di cardinalità 0? È unico?

2.5.1.4 Fornire un esempio di insiemi disgiunti ma non vuoti.

2.5.1.5 Fornire un esempio di due insiemi disgiunti A e B tali che $A \subseteq B$.

2.5.1.6 È vero che gli insiemi $A = \{5,3,1\}$ e $B = \{3,1,5\}$ sono uguali? Perché?

2.5.1.7 È vero che gli insiemi $A = \{\}$ e $B = \{\varnothing\}$ sono uguali? Perché?

2.5.1.8 Elencare gli elementi che appartengono all'insieme $\{x \in \mathbb{N} \mid x^2 = 2\}$

2.5.1.9 Elencare gli elementi che appartengono all'insieme $\{x \mid x \text{ è una nota musicale}\}$

2.5.1.10 Elencare gli elementi che appartengono all'insieme $\{x \mid x \text{ è una lettera della parola "matematica"}\}$

2.5.1.11 Elencare gli elementi che appartengono all'insieme $\{x \in \mathbb{N} \mid x \text{ è un numero dispari minore di } 19\}$

2.5.1.12 Elencare gli elementi che appartengono all'insieme

$$\{x \in \mathbb{N} \mid x < 100 \text{ e } x \text{ è il quadrato di un qualche numero intero}\}.$$

2.5.1.13 È vero che $a \in \{a\}$? Perché?

2.5.1.14 È vero che $\{a\} \subseteq \{a\}$? Perché?

2.5.1.15 È vero che $\varnothing \subseteq \{\}$? Perché?

2.5.1.16 È vero che $\varnothing \subset \{\}$? Perché?

2.5.1.17 È vero che $\varnothing \subseteq \{a\}$? Perché?

2.5.1.18 È vero che $\varnothing \in \{a\}$? Perché?

2.5.1.19 Dati $A = \{a,b,c,d\}$, $B = \{a,b,d\}$ e $C = \{a,b\}$ dire se le seguenti relazioni sono vere o false:

(a) $A \subseteq B$

(b) $A \nsubseteq B$

(c) $B \subseteq A$

(d) $B \nsubseteq C$

(e) $C \nsubseteq A$

(f) $C \subseteq B$

(g) $B \subseteq C$

(h) $C \nsubseteq B$

2.5.1.20 Dati $A = \{a,b,c\}$ e $B = \{a,d\}$ calcolare i seguenti insiemi e le loro cardinalità:

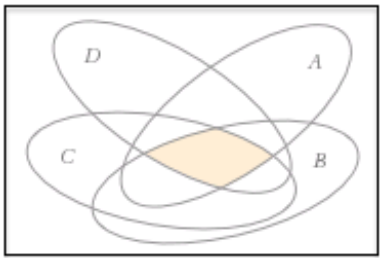
(a) $A \cap B$

(b) $A \cup B$

(c) $A \setminus B$

(d) $B \setminus A$

2.5.1.21 Con riferimento alla figura a destra, individuare le aree che rappresentano i seguenti insiemi:



(a) $\{a \in A \mid a \in B \text{ e } a \in C \text{ e } a \notin D\}$

(b) $\{a \in A \mid a \notin B \text{ e } a \in C\}$

(c) $\{a \in A \mid a \in B\}$

(d) $\{a \in A \mid a \in B \text{ o } a \notin C\}$

2.5.1.22 Dare due insiemi A e B diversi ma non disgiunti.

2.5.1.23 Dare due insiemi A e B diversi e tali che $A \cup B = A$.

2.5.1.24 Dare due insiemi A e B diversi e tali che $A \cap B = B$.

2.5.1.25 Dare tre insiemi A,B,C tali che $A \cap B = B \cap C$ e $A \neq C$.

2.5.2 Esercizi di approfondimento

Confrontare gli insiemi

2.5.2.1 Descrivere esplicitamente come si può dimostrare rispettivamente che:

(a) $A \not\subseteq B$;

(b) $A \neq B$;

(c) $A \not\subset B$.

2.5.2.2 Dimostrare che le seguenti relazioni tra insiemi valgono, oppure fornire opportuni controesempi quando non siano soddisfatte.

(a) $\{n \in \mathbb{N} \mid n > n^2\} = \varnothing$

(b) $\{n+m \mid n \in \mathbb{N}^p, m \in \mathbb{N}^d\} = \{n \in \mathbb{N}^d \mid n > 1\}$

(c) $\mathbb{N}^+ \subset \mathbb{N}$

(d) $\mathbb{Z} \neq \mathbb{N}$

(e) $\mathbb{N}^+ \neq \varnothing$

(f) $\mathbb{P} \cap \mathbb{N}^d = \varnothing$

(g) $\mathbb{N}^p \neq \mathbb{N}^d$

(h) $\mathbb{N} \neq \{n \mid n \in \mathbb{N}^p \text{ oppure } n \in \mathbb{N}^d\}$

(i) $\mathbb{N}^+ \neq \{n \mid n \in \mathbb{N}^p \text{ oppure } n \in \mathbb{N}^d\}$

(j) $A \subseteq A$, per qualunque insieme A

(k) $A \subset A$, per qualunque insieme A

(l) $A = A$, per qualunque insieme A

(m) se $A \subseteq B$ e $B \subseteq C$ allora $A \subseteq C$, per insiemi arbitrari A, B e C

(n) se $A \subseteq B$ e $B \subset C$ allora $A \subset C$, per insiemi arbitrari A, B e C

2.5.2.3 Dimostrare che $\mathbb{Z} \setminus \mathbb{N} = \{-n \mid n \in \mathbb{N}^+\}$.

2.5.2.4 Dimostrare che $\mathbb{N} \setminus \mathbb{Z} = \varnothing$.

2.5.2.5 Dimostrare che $\mathbb{N}^p \setminus \mathbb{N}^d = \mathbb{N}^p$

Comporre gli insiemi

2.5.2.6 Assumendo come universo di riferimento l'insieme $\mathbb{N}$, dimostrare che:

(a) $\overline{\mathbb{N}^p} = \{0\} \cup \mathbb{N}^d$

(b) $\overline{\mathbb{N}^d} = \{0\} \cup \mathbb{N}^p$.

2.5.2.7 Sappiamo che $A \subseteq B$.

(a) Cosa possiamo dire su $A \cap B$?

(b) Cosa possiamo dire su $A \cup B$?

(c) È vero che $A \setminus B = A$?

(d) È vero che $B \setminus A = B$?

(e) È vero che $A \setminus B = \varnothing$?

2.5.2.8 Ricordando che $\mathbb{P}$ è l'insieme dei numeri primi, dare un insieme A tale che $A \cup \mathbb{N}^+ = \mathbb{N}$, $\mathbb{N}^p \cap A = \varnothing$ e $A \cap \mathbb{P} = \{11\}$. Quanti insiemi esistono che soddisfano queste condizioni?

Dimostrazione di uguaglianze di insiemi

2.5.2.9 Si dimostrino in modo discorsivo le leggi dell'elemento neutro e la prima legge di distributività a sinistra ($A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$).

2.5.2.10 Utilizzando i diagrammi di Eulero-Venn, dimostrare o confutare le seguenti uguaglianze:

(a) La prima legge di De Morgan: $\overline{(A \cap B)} = \overline{A} \cup \overline{B}$.

(b) $A \cap (B \setminus C) = (A \cap B) \setminus C$.

(c) $(A \cup B) \setminus (B \cap A) = (A \setminus B) \cup (B \setminus A)$.

(d) $A \setminus (B \setminus C) = (A \setminus B) \cup C$.

(e) $A \setminus (B \setminus C) = (A \setminus C) \cup B$.

(f) $A \cap (B \cup A) = B \cup (A \cap B)$.

(g) $\overline{A} \cap (B \cup C) = (B \setminus A) \cup (C \setminus A) \cup (B \cap C)$.

2.5.2.11 Dimostrare in modo discorsivo e in modo grafico che presi due insiemi qualsiasi A, B si ha che:

(a) $A \cup (A \cap B) = A$;

(b) $A \cap (A \cup B) = A$;

(c) se $A \cap B = A \cup B$, allora $A = B$.

2.5.2.12 Dimostrare che presi tre insiemi qualsiasi A, B e C:

(a) se $(A \setminus B) \subseteq C$ allora per ogni elemento $a \in (A \setminus C)$ vale $a \in B$;

(b) se $(A \cap C) \subseteq B$ allora per ogni elemento $a \in C$ vale $a \notin (A \setminus B)$;

(c) se $A \subseteq (B \setminus C)$ allora $A \cap C = \varnothing$;

(d) se $(A \setminus B) \subseteq C$ allora per ogni elemento $a \in (A \setminus C)$ vale $a \in A \cap B$.

2.5.2.13 Si dica se le seguenti proprietà su insiemi sono valide, fornendo una dimostrazione formale in caso positivo oppure un controesempio in caso negativo:

(a) Per ogni A, B tali che $A \subseteq B$ si ha $\overline{B} \subseteq \overline{A}$.

(b) Per ogni A, B tali che $A \subseteq B$ si ha $\overline{A} \subseteq \overline{B}$.

(c) Per ogni A, B tali che $(A \setminus B) \subseteq (B \setminus A)$ si ha $A \subseteq B$.

(d) Per ogni A, B tali che $(A \setminus B) \subseteq (B \setminus A)$ si ha $B \subseteq A$.

(e) Per ogni A, B, C tali che $A \subseteq (B \cup C)$ si ha $A \subseteq B$ oppure $A \subseteq C$.

(f) Per ogni A, B, C tali che $A \subseteq (B \cap C)$ e $B \subseteq (A \cap C)$ e per ogni $a \in (A \cup B)$ si ha $a \in C$.

(g) Per ogni A, B, C tali che $A \subseteq (B \cap C)$ e per ogni $a \in A$ si ha $a \in C$.

(h) Per ogni A, B, C tali che $A \subseteq (B \cup C)$ e per ogni $a \in A$ si ha $a \in B$.

(i) Per ogni A, B, C tali che $A \subseteq C$ e $B \subseteq C$ si ha $(A \cap B) \subseteq C$.

(j) Per ogni A, B, C si ha $(A \setminus (B \cup C)) \subseteq (A \setminus B)$.

(k) Per ogni A, B, C si ha $(A \setminus (B \cap C)) \subseteq (A \setminus B)$.

(l) Per ogni A, B, C tali che $A \subseteq B$ si ha $(C \setminus B) \subseteq (C \setminus A)$.

(m) Per ogni A, B, C tali che $A \subseteq B$ si ha $(C \setminus A) \subseteq (C \setminus B)$.

(n) Per ogni A, B, C tali che $(A \cap B) \subseteq C$ si ha $A \subseteq C$ e $B \subseteq C$.

(o) Per ogni A, B, C, D tali che $A \subseteq B$ e $C \subseteq D$ si ha $(A \cap C) \subseteq (B \cup D)$.

(p) Per ogni A, B, C, D tali che $A \subseteq B$ e $C \subseteq D$ si ha $(A \cap C) \supseteq (B \cap D)$.

(q) Per ogni A, B, C, D tali che $A \subseteq (\overline{B} \cap C)$ e $C \subseteq (B \cup D)$ si ha $A \subseteq D$.

2.5.3 Esercizi che coinvolgono dimostrazioni per sostituzione

2.5.3.1 Dimostrare, per sostituzione, che le leggi su $\varnothing$ e $\mathcal{U}$ elencate nella colonna di sinistra della Proposizione 2 possono essere derivate usando le leggi che compaiono nella colonna di destra.

2.5.3.2 Dimostrare le seguenti uguaglianze di insiemi, utilizzando il principio di sostituzione.

(a) $(A \cup B) \setminus (B \cap A) = (A \setminus B) \cup (B \setminus A)$

(b) $A \setminus \overline{A} = A$

(c) $(A \setminus B) \setminus C = (A \setminus C) \setminus B$

(d) $\overline{A \setminus B} = \overline{A} \cup B$

(e) $\overline{A \cup (\overline{B} \cap C)} = (\overline{C} \cap \overline{A}) \cup (\overline{A} \cap B)$

(f) $(A \cup \overline{B}) \cap C = (C \cap A) \cup (C \setminus B)$

2.5.3.3 Dimostrare in almeno due modi diversi che comunque si scelgano tre insiemi A, B e C vale la seguente uguaglianza tra insiemi, oppure fornire un controesempio:

$$\overline{(A \cap B)} \cup (B \cap C) = \overline{((A \cap B) \setminus C)}$$

2.5.3.4 Dimostrare (sia con i diagrammi di Eulero-Venn che per sostituzione) che presi due insiemi qualsiasi A e B si ha $A \setminus (A \setminus \overline{B}) = A \setminus B$.

2.5.3.5 Dimostrare (sia con i diagrammi di Eulero-Venn che per sostituzione) che comunque si scelgano tre insiemi A, B e C vale la seguente uguaglianza:

$$\overline{C} \setminus (B \cap A) = (\overline{A} \setminus C) \cup (\overline{C} \setminus B)$$

2.5.3.6 Dimostrare (sia con i diagrammi di Eulero-Venn che per sostituzione) che comunque si scelgano tre insiemi A, B e C si ha $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

2.5.3.7 Dimostrare (sia usando i diagrammi di Eulero-Venn che per sostituzione) che comunque si scelgano tre insiemi A, B e C vale la seguente uguaglianza tra insiemi, oppure fornire un controesempio:

$$(A \cup B) \cap (C \setminus A) = (B \cap C) \setminus (A \cap B).$$

2.5.3.8 Dimostrare (sia con i diagrammi di Eulero-Venn che per sostituzione) che presi tre insiemi qualsiasi A, B e C si ha $\overline{C \cup (B \setminus A)} = (A \cup \overline{B}) \setminus C$.

2.5.3.9 [Difficile] Sia $A \triangleleft B$ l'operazione tra insiemi definita da:

$$A \triangleleft B = \overline{(A \setminus B)}$$

Dimostrare (sia con i diagrammi di Eulero-Venn che per sostituzione) o confutare con un controesempio le seguenti asserzioni:

(a) per ogni A, B, C si ha $(A \triangleleft B) \triangleleft C = A \triangleleft (B \triangleleft C)$

(b) per ogni A, B si ha $(A \triangleleft B) \cap (B \triangleleft A) = (A \cup B) \triangleleft (A \cap B)$

Capitolo 3

Il calcolo proposizionale

Il *calcolo proposizionale* (chiamato anche *logica proposizionale*) costituisce il nucleo di tutte le logiche "classiche", in cui le formule possono avere solo due valori di verità: vero o falso. Questo capitolo introduce in forma semplificata il modo di scrivere (la sintassi) e il modo di interpretare (la semantica) le formule proposizionali, e si sofferma sull'uso di questa logica per formalizzare proposizioni espresse in linguaggio naturale in modo da esplicitarne la struttura logica. Questo consentirà di valutare la correttezza di semplici deduzioni espresse in linguaggio naturale, visto che anch'esse sono esprimibili come formule del calcolo proposizionale, sfruttando i connettivi logici che esso mette a disposizione. Successivamente vengono presentate le leggi che descrivono le proprietà dei connettivi logici, e viene discusso come utilizzare le dimostrazioni per sostituzione introdotte nella Sezione 1.4 per dimostrare l'equivalenza logica di formule proposizionali. Questa tecnica può essere usata per dimostrare che certe formule sono tautologie, cioè sempre vere, e quindi per dimostrare la correttezza di semplici inferenze o deduzioni.

Ricordiamo che, nonostante la sua semplicità, il calcolo proposizionale ha svariate applicazioni in informatica, come per esempio le operazioni bit-a-bit e i circuiti binari, il flusso di controllo nella programmazione, le analisi delle specifiche, le interrogazioni su basi di dati, la ricerca booleana nei motori di ricerca, e molte altre ancora che qui non tratteremo ma che incontrerete nel corso di laurea in Informatica.

3.1 Le proposizioni

L'obiettivo della logica non è tanto quello di stabilire la validità assoluta di un certo enunciato, ma piuttosto quello di stabilire quando, assumendo vere certe premesse, si possa affermare la validità di altri enunciati: in questo caso diremo che questi ultimi sono *conseguenze logiche* delle premesse. In sostanza, si può dire che la logica si occupa di stabilire quali ragionamenti siano corretti e quali no.

Data la complessità dell'attività deduttiva e inferenziale degli esseri umani sono state sviluppate diverse logiche che si propongono di catturare aspetti sempre più complessi del ragionamento. Noi ci limitiamo a considerare la *logica classica*, che tratta enunciati che possono assumere uno e uno solo dei valori di verità, detti *booleani*, [1] cioè vero oppure falso, ma non entrambi.[2]

DEFINIZIONE 3.1 (VALORI DI VERITÀ O BOOLEANI)
*I **valori di verità**, chiamati anche **valori booleani**, sono due: in italiano li chiamiamo vero e falso, in inglese true e false.*

A seconda del contesto si usano vari simboli per denotare questi due valori, tra i quali:

vero	*true*	*TT*	*T*	*V*	*1*	$n \in \mathbb{N}^+$	$\top$
falso	*false*	*FF*	*F*	*F*	*0*	*0*	$\bot$

Noi useremo prevalentemente la notazione T e F per la sintassi (cioè per la rappresentazione simbolica dei booleani all'interno di formule) e 1 e 0 per la semantica (cioè per indicare il valore di verità di una formula).

[1] Dal nome di George Boole (1815–1864), importante logico e matematico inglese.

[2] In realtà, molti enunciati in linguaggio naturale non godono di questa proprietà, e sono state sviluppate altre logiche al fine di superare questo limite della logica classica.

DEFINIZIONE 3.2 (PROPOSIZIONI)
*Una **proposizione** è un enunciato dichiarativo (per esempio una frase in linguaggio naturale) che "afferma qualcosa" e per il quale si può dire:*

Principio del terzo escluso: *che è vero oppure è falso (non ci sono altre possibilità)*

Principio di non contradditorietà: *che non è al tempo stesso sia vero che falso.*

Per esempio, *"Quanti sono i numeri primi minori di 100?"* non è una proposizione, perché non "afferma qualcosa". Al contrario, *"Sono biondo naturale"* è una proposizione, che può essere vera o falsa a seconda del soggetto che la legge.

ESEMPIO 3.1 (RICONOSCERE LE PROPOSIZIONI)
Vediamo per ognuna delle frasi seguenti se sono proposizioni oppure no.

1. Firenze è la capitale d'Italia.
   Si tratta di una proposizione, in quanto afferma un fatto che può essere vero o falso, ma non entrambi. In particolare, la proposizione è falsa per il significato usuale che associamo alle parole Firenze, capitale *e* Italia.

2. È possibile che Firenze sia la capitale d'Italia.
   Non afferma qualcosa, ma esprime una valutazione sul fatto che l'enunciato Firenze è la capitale d'Italia *sia vero, pertanto non è una proposizione.*

3. Firenze è la capitale d'Italia?
   Si tratta di un enunciato interrogativo che non afferma qualcosa, quindi non è una proposizione.

4. Firenze è stata la capitale d'Italia.
   È una proposizione perché afferma un fatto che, in particolare, è vero

5. Se solo Firenze fosse la capitale d'Italia!
   È un enunciato che esprime un desiderio ma non afferma qualcosa, quindi non è una proposizione.

6. Probabilmente Firenze è la capitale d'Italia.
   Non è una proposizione per gli stessi motivi della frase 2.

Quando costruiamo un ragionamento (un'inferenza) creiamo una sequenza di proposizioni delle quali alcune si suppone siano vere (come premesse o ipotesi) e altre sono dedotte dalle precedenti applicando delle regole di inferenza. Un tipico esempio è la costruzione della dimostrazione di un teorema. Infatti la matematica non si occupa di verità assolute, ma solo di verità relative ad alcune teorie: come è ben noto, gli enunciati dei teoremi hanno quasi sempre la forma

"se (ipotesi), allora (tesi)"

Le ipotesi sono delle proposizioni che supponiamo essere vere, e la dimostrazione procede costruendo a partire da esse (applicando delle regole di inferenza) delle proposizioni intermedie, e così via fino a ottenere la tesi. Ogni teoria presuppone l'esistenza di un insieme di proposizioni iniziali, dette *assiomi* della teoria, a partire dalle quali è possibile dedurre nuovi teoremi.

Gli aspetti della logica matematica cui siamo interessati in queste note non forniscono strumenti per dimostrare automaticamente dei teoremi o per "creare" ragionamenti o inferenze complesse, ma ci permettono di *analizzare* dimostrazioni, ragionamenti e inferenze per controllare che siano *logicamente corretti*. Per analizzare logicamente un ragionamento occorre *formalizzare* le proposizioni che esso contiene, cioè renderne esplicita la struttura logica: questo serve per controllare se la conclusione è una conseguenza logica delle premesse e per riconoscere ed escludere ragionamenti sbagliati che porterebbero a conclusioni erronee.

La formalizzazione delle proposizioni può essere fatta a vari livelli di approfondimento, che dipendono dal potere espressivo della logica utilizzata. In questo capitolo considereremo il livello più semplice, quello del **calcolo proposizionale**, mentre nel successivo presenteremo la più espressiva **logica dei predicati**.

3.2 Le formule proposizionali e la loro semantica

Le formule del calcolo proposizionale sono ottenute a partire da un insieme di *simboli proposizionali*, che rappresentano dei fatti o enunciati basilari, componendoli in modo arbitrario con le operazioni di negazione, congiunzione, disgiunzione (inclusiva o esclusiva) e implicazione (semplice o doppia).

La semantica di una formula proposizionale, cioè il suo valore di verità, dipende dal valore di verità assegnato ai simboli proposizionali che essa contiene e da come essi sono composti per mezzo dei connettivi logici. Come vedremo le *tabelle di verità* permettono di rappresentare in modo compatto tale semantica, associando ad ogni riga un particolare modo di assegnarei valori ai simboli proposizionali, detto *interpretazione*, e il corrispondente valore booleano della formula.

L'introduzione dei connettivi logici come operatori su formule (in qualche modo analoghi ai ben noti operatori algebrici su espressioni aritmetiche) risale a George Boole, che nel 1854 pubblica "The Laws of Thought" dove spiega (tra le altre cose) come costruire proposizioni complesse a partire da quelle che già abbiamo a disposizione. La costruzione avviene appunto usando i *connettivi logici*, cioè degli operatori che applicati a una o più formule restituiscono una nuova formula.

DEFINIZIONE 3.3 (CONNETTIVI LOGICI)
Siano P e Q due proposizioni.

- *La* ***negazione*** *della proposizione P è la proposizione* $\boxed{\neg P}$*, che è vera se e solo se P è falsa.*
- *La* ***congiunzione*** *di P e Q è la proposizione* $\boxed{P \wedge Q}$*, che è vera se e solo se P e Q sono* **entrambe** *vere.*
- *La* ***disgiunzione (inclusiva)*** *di P e Q è la proposizione* $\boxed{P \vee Q}$*, che è vera se e solo se* **almeno** *una tra P e Q è vera.*
- *La* ***disgiunzione esclusiva*** *di P e Q è la proposizione* $\boxed{P \oplus Q}$*, che è vera se e solo se* **esattamente** *una tra P e Q è vera; equivalentemente, $P \oplus Q$ è vera se e solo se i valori di verità di P e Q sono diversi.*
- *L'****implicazione*** *di Q se P è la proposizione* $\boxed{P \Rightarrow Q}$*, che è vera se e solo se nel caso P sia vera anche Q lo è. Nell'implicazione $P \Rightarrow Q$ la proposizione P è chiamata la* premessa*, mentre Q è la* conseguenza *o* conclusione*.*

  Attenzione: *Sono spesso utili le seguenti definizioni equivalenti dell'implicazione:*

  - *$P \Rightarrow Q$ è vera se e solo se almeno una tra $\neg P$ e Q è vera*
  - *$P \Rightarrow Q$ è falsa se e solo se P è vera e Q è falsa*
- *La* ***doppia implicazione*** *di P e Q è la proposizione* $\boxed{P \Leftrightarrow Q}$ *che è vera se e solo se P e Q hanno lo stesso valore di verità, cioè sono entrambe vere o entrambe false.*

NOTA 3.2 *Talvolta potreste imbattervi nella notazione $P \Leftarrow Q$ che potete leggere come $Q \Rightarrow P$.*

Le *tabelle di verità* che seguono riassumono la semantica della negazione e dei connettivi binari. La prima colonna della tabella di sinistra mostra i possibili valori booleani che può assumere P (si ricordi che 0 rappresenta *falso* e 1 rappresenta *vero*), e la seconda colonna mostra i corrispondenti valori di $\neg P$. Analogamente, in ogni riga della tabella di destra le prime due colonne contengono un possibile assegnamento di valori booleani per P e Q mentre le altre colonne indicano il corrispondente valore della proposizione riportata nella prima riga, ottenuta applicando un connettivo logico a P e Q.

P	$\neg P$
0	1
1	0

P	Q	$P \wedge Q$	$P \vee Q$	$P \oplus Q$	$P \Rightarrow Q$	$P \Leftrightarrow Q$
0	0	0	0	0	1	1
0	1	0	1	1	1	0
1	0	0	1	1	0	0
1	1	1	1	0	1	1

Ogni connettivo logico può essere letto in vari modi, di cui menzioniamo i più comuni (ne incontreremo altri nella Sezione 3.3):

- $\neg P$ può essere letto *"non P"*, *"not P"*, *"non è vero che P vale"*, ...
- $P \wedge Q$ può essere letto *"P e Q"*, *"P and Q"*, *"P e anche Q"*,...
- $P \vee Q$ può essere letto *"P o Q"*, *"P or Q"*, *"P oppure Q"*, ...
- $P \oplus Q$ può essere letto *"P 'o esclusivo' Q"*, *"P xor Q"*, *"o P o Q"*, *"P diverso da Q"*,...
- $P \Rightarrow Q$ può essere letto *"P implica Q"*, *"se P allora Q"*, *"P solo se Q"*, *"Q se P"*, *"Q if P"*, *"P è condizione sufficiente per Q"*, *"Q è condizione necessaria per P"*, ...
- $P \Leftrightarrow Q$ può essere letto *"P sse Q"*, *"P se e solo se Q"*, *"P iff Q"*, *"P equivale a Q"*, *"P è condizione necessaria e sufficiente affinché sia vera Q"*, ...

NOTA 3.3 *Potrebbe non essere ovvio che "condizione sufficiente" e "condizione necessaria" rappresentino forme di implicazioni inverse l'una rispetto all'altra. Dire che P è condizione sufficiente per Q significa che se P è vera allora anche Q deve essere vera ($P \Rightarrow Q$). Però Q può essere vera anche se P è falsa. Invece dire che P è condizione necessaria per Q significa che Q non può essere vera quando P è falsa ($Q \Rightarrow P$).*

Detto questo, quale delle due regole preferireste per l'esame? Perché?

1) "rispondere bene a tutte le domande è condizione sufficiente per prendere 30"

2) "rispondere bene a tutte le domande è condizione necessaria per prendere 30"

Introduciamo finalmente le formule proposizionali, nelle quali i connettivi logici possono essere applicati a sotto-formule arbitrariamente complesse.

DEFINIZIONE 3.4 (FORMULE PROPOSIZIONALI)
Sia dato un insieme $\mathcal{P} = \{P, Q, ...\}$ di ***simboli proposizionali*** *(detto anche* ***alfabeto***[3]*). Le* ***formule proposizionali*** *sono tutte e sole quelle ottenibili con le seguenti regole:*

1. T *("vero") e* F *("falso") sono formule proposizionali*
2. *ogni* $P \in \mathcal{P}$ *è una formula proposizionale*
3. *se A e B sono formule proposizionali, allora anche*

$$\neg A \qquad (A \wedge B) \qquad (A \vee B) \qquad (A \oplus B) \qquad (A \Rightarrow B) \qquad (A \Leftrightarrow B)$$

sono formule proposizionali

Si noti che usiamo P, Q, R, ..., come simboli proposizionali, mentre A, B, C, ..., per denotare generiche formule proposizionali.

ESEMPIO 3.4 (FORMULE PROPOSIZIONALI)
Dalla definizione segue che le seguenti sono formule proposizionali:

$$\mathsf{T} \qquad ((P \wedge Q) \vee \neg R) \qquad ((P \wedge (Q \vee \mathsf{F})) \Rightarrow (\neg P \vee (R \wedge \mathsf{T})))$$

Invece non sono formule proposizionali $(P \wedge \oplus Q)$, $(P \neg Q)$ e $P \neg$, perché non sono ottenibili con le regole della Definizione 3.4. Si noti che anche $P \vee (Q \wedge R)$ non è una formula. La scrittura corretta è $(P \vee (Q \wedge R))$. Spiegheremo più avanti perché richiediamo una coppia di parentesi per ogni connettivo binario.

[3]Per comodità spesso useremo singoli caratteri maiuscoli come simboli proposizionali (per esempio *P*), ma nulla vieta di usare sequenze di caratteri di lunghezza maggiore (per esempio *Piove*).

3.2.1 Interpretare le formule proposizionali

Vista la sintassi delle formule proposizionali, presentata nella Definizione 3.4, ci poniamo ora il problema di stabilire la loro semantica, cioè di come sia possibile assegnare loro un valore di verità.

Come abbiamo visto, una formula proposizionale può contenere T, F, dei simboli proposizionali e dei connettivi logici. T e F hanno come valore di verità 1 e 0, ovviamente. Inoltre i connettivi logici permettono di determinare univocamente il valore di verità della proposizione composta quando si conosca quello degli argomenti, come descritto nella Definizione 3.3. Quindi per determinare il valore di verità di una formula è sufficiente avere un'*interpretazione*, cioè un assegnamento di valori di verità ai simboli proposizionali che compaiono in essa.

DEFINIZIONE 3.5 (INTERPRETAZIONE)
*Data una formula proposizionale A, un'**interpretazione** per A è una funzione che associa un valore di verità ad ogni simbolo proposizionale che compare in A.*

Di seguito usiamo la notazione $\{\ldots, P \mapsto 1, \ldots\}$ (rispettivamente $\{\ldots, P \mapsto 0, \ldots\}$) per indicare un'interpretazione che assegna il booleano vero (rispettivamente falso) al simbolo P.

Consideriamo per esempio la formula $((P \wedge Q) \vee \neg R)$ e l'interpretazione $\{P \mapsto 1, Q \mapsto 0, R \mapsto 0\}$. Una volta assegnati i valori di verità ai simboli P, Q e R, possiamo ricavare i valori di verità associati alle sotto-formule $(P \wedge Q)$ e $\neg R$ e quindi all'intera formula $((P \wedge Q) \vee \neg R)$. Poichè P vale 1 e Q vale 0, dalla Definizione 3.3 sappiamo che $(P \wedge Q)$ vale 0; poiché R vale 0 abbiamo che $\neg R$ vale 1; a questo punto per il significato di $\vee$, visto che $\neg R$ vale 1, l'intera formula vale 1. Possiamo rappresentare questo ragionamento in modo compatto nella seguente tabella:

P	Q	R	$((P$	$\wedge$	$Q)$	$\vee$	$\neg$	$R)$
1	0	0	1	0	0	**1**	1	0
			(1)	(2)	(1)	**(3)**	(2)	(1)

Nella prima riga abbiamo a destra la formula e a sinistra i simboli proposizionali che vi compaiono. Nella seconda riga, sotto i simboli abbiamo il valore fissato dall'interpretazione, e sotto i connettivi logici il risultato determinato dal loro significato. Il valore di verità della formula è quello riportato sotto il *connettivo principale*, cioè l'unico che non compare nella formula come argomento di un altro connettivo: in questo caso è $\vee$. I numeri in parentesi sotto le colonne indicano l'ordine con cui viene compilata la tabella: si parte dalle colonne dei simboli proposizionali e si applicano i connettivi nell'ordine stabilito dalle parentesi. Nel nostro caso l'ordine è il seguente:

P	Q	R	$((P$	$\wedge$	$Q)$	$\vee$	$\neg$	$R)$
1	0	0	**1**		**0**			**0**

P	Q	R	$((P$	$\wedge$	$Q)$	$\vee$	$\neg$	$R)$
1	0	0	1	**0**	0		**1**	0

P	Q	R	$((P$	$\wedge$	$Q)$	$\vee$	$\neg$	$R)$
1	0	0	1	0	0	**1**	1	0

Quante sono le possibili diverse interpretazioni per una formula proposizionale? È facile convincersi che sono 2^n, dove n è il numero di simboli proposizionali distinti che compaiono in essa. Per esempio, per la formula $((P \wedge Q) \vee \neg R)$ abbiamo due possibili valori per P, due per Q e due per R, per un totale di $2^3 = 8$ distinte interpretazioni. Una formula con 10 simboli proposizionali diversi avrebbe $2^{10} = 1024$ interpretazioni.

Una **tabella di verità** per una formula proposizionale elenca, una per riga, tutte le possibili interpretazioni e il corrispondente valore di verità della formula. Nella Definizione 3.3 abbiamo già visto un esempio di tabella di verità, utile per rappresentare in modo compatto il significato dei connettivi logici. Nella Figura 3.1 mostriamo come si può costruire la tabella di verità per la formula $((P \wedge Q) \vee \neg R)$, partendo dall'elenco di tutte le possibili interpretazioni e poi annotando progressivamente i connettivi con i valori calcolati.

0. Possibili assegnamenti di verità ai simboli proposizionali:

P	Q	R	$((P$	$\wedge$	$Q)$	$\vee$	$\neg$	$R)$
0	**0**	**0**						
0	**0**	**1**						
0	**1**	**0**						
0	**1**	**1**						
1	**0**	**0**						
1	**0**	**1**						
1	**1**	**0**						
1	**1**	**1**						

1. Valutazione dei simboli proposizionali nella formula:

P	Q	R	$((P$	$\wedge$	$Q)$	$\vee$	$\neg$	$R)$
0	0	0	**0**		**0**			**0**
0	0	1	**0**		**0**			**1**
0	1	0	**0**		**1**			**0**
0	1	1	**0**		**1**			**1**
1	0	0	**1**		**0**			**0**
1	0	1	**1**		**0**			**1**
1	1	0	**1**		**1**			**0**
1	1	1	**1**		**1**			**1**
			(1)		(1)			(1)

2. Valutazione delle espressioni più annidate ($(P \wedge Q)$ e $\neg R$):

P	Q	R	$((P$	$\wedge$	$Q)$	$\vee$	$\neg$	$R)$
0	0	0	0	**0**	0		**1**	0
0	0	1	0	**0**	0		**0**	1
0	1	0	0	**0**	1		**1**	0
0	1	1	0	**0**	1		**0**	1
1	0	0	1	**0**	0		**1**	0
1	0	1	1	**0**	0		**0**	1
1	1	0	1	**1**	1		**1**	0
1	1	1	1	**1**	1		**0**	1
			(1)	(2)	(1)		(2)	(1)

3. Valutazione delle espressioni più annidate e non ancora valutate:

P	Q	R	$((P$	$\wedge$	$Q)$	$\vee$	$\neg$	$R)$
0	0	0	0	0	0	**1**	1	0
0	0	1	0	0	0	**0**	0	1
0	1	0	0	0	1	**1**	1	0
0	1	1	0	0	1	**0**	0	1
1	0	0	1	0	0	**1**	1	0
1	0	1	1	0	0	**0**	0	1
1	1	0	1	1	1	**1**	1	0
1	1	1	1	1	1	**1**	0	1
			(1)	(2)	(1)	(3)	(2)	(1)

Figura 3.1: Costruzione della tabella di verità della formula $((P \wedge Q) \vee \neg R)$.

NOTA 3.5 *Nella definizione di formule proposizionali abbiamo introdotto una coppia di parentesi ogni volta che si introduce un connettivo logico binario. Questo rende la notazione un po' pesante, ma permette di evitare ambiguità. Infatti, per esempio,* $((P \wedge Q) \Rightarrow Q)$ *e* $(P \wedge (Q \Rightarrow Q))$ *sono due formule sintatticamente corrette, ma per l'interpretazione* $\{P \mapsto 0, Q \mapsto 1\}$ *la prima è vera mentre al seconda è falsa. Se togliessimo le parentesi, da entrambe otterremmo la formula* $P \wedge Q \Rightarrow Q$*, che in mancanza di altre informazioni sarebbe ambigua.*

Una soluzione alternativa all'uso delle parentesi, usata frequentemente (ma non in queste note), consiste nel fissare un ordine di precedenza tra gli operatori: se $\wedge$ *avesse priorità maggiore di* $\Rightarrow$*, allora* $P \wedge Q \Rightarrow Q$ *sarebbe letta come* $(P \wedge Q) \Rightarrow Q$*, risolvendo in questo modo l'ambiguità.*

ESEMPIO 3.6 (TABELLA DI VERITÀ)
Come ulteriore esempio di tabella di verità vediamo quella di una formula leggermente più complessa, dove compaiono anche le costanti T *e* F*:* $((P \wedge (Q \vee \mathsf{F})) \Rightarrow (\neg P \vee (R \wedge \mathsf{T})))$*.*

P	Q	R	$((P$	$\wedge$	$(Q$	$\vee$	$\mathsf{F}))$	$\Rightarrow$	$(\neg$	$P)$	$\vee$	$(R$	$\wedge$	$\mathsf{T})))$
0	0	0	0	0	0	0	0	**1**	1	0	1	0	0	1
0	0	1	0	0	0	0	0	**1**	1	0	1	1	1	1
0	1	0	0	0	1	1	0	**1**	1	0	1	0	0	1
0	1	1	0	0	1	1	0	**1**	1	0	1	1	1	1
1	0	0	1	0	0	0	0	**1**	0	1	0	0	0	1
1	0	1	1	0	0	0	0	**1**	0	1	1	1	1	1
1	1	0	1	1	1	1	0	**0**	0	1	0	0	0	1
1	1	1	1	1	1	1	0	**1**	0	1	1	1	1	1
			(1)	(3)	(1)	(2)	(1)	(4)	(2)	(1)	(3)	(1)	(2)	(1)

Quindi il valore di verità di una formula proposizionale dipende, in generale, dall'interpretazione dei suoi simboli proposizionali. Tuttavia nel calcolo proposizionale ci interessano in particolar modo le *tautologie*, cioè le formule che risultano vere per qualunque interpretazione: esse infatti, come vedremo in seguito, ci permettono di rappresentare schemi di inferenza o di ragionamento corretti.

DEFINIZIONE 3.6 (TAUTOLOGIE, CONTRADDIZIONI, FORMULE SODDISFACIBILI)
Una ***tautologia*** *è una formula proposizionale che è sempre vera, per qualunque interpretazione. Una* ***contraddizione*** *(o* ***formula insoddisfacibile****) è una formula proposizionale che è sempre falsa, per qualunque interpretazione. Una formula proposizionale è* ***soddisfacibile*** *se esiste almeno una interpretazione per la quale è vera.*

Dalla definizione segue che, nella tabella di verità di una formula proposizionale, la colonna sotto il connettivo principale conterrà tutti 1 se la formula è una tautologia, tutti 0 se è una contraddizione, e almeno un 1 se è soddisfacibile.

ESEMPIO 3.7 (TAUTOLOGIE, CONTRADDIZIONI E FORMULE SODDISFACIBILI)
La seguente tabella di verità mostra che la formula $((P \wedge Q) \Rightarrow Q)$ *è una tautologia (e quindi anche soddisfacibile), la formula* $(P \wedge (Q \wedge \neg P))$ *è una contraddizione, mentre la formula* $(P \Rightarrow Q)$ *è soddisfacibile ma non è una tautologia.*

P	Q	$((P$	$\wedge$	$Q)$	$\Rightarrow$	$Q)$	$(P$	$\wedge$	$(Q$	$\wedge$	$\neg$	$P))$	$(P$	$\Rightarrow$	$Q)$
0	0	0	0	0	**1**	0	0	**0**	0	0	1	0	0	**1**	0
0	1	0	0	1	**1**	1	0	**0**	1	1	1	0	0	**1**	1
1	0	1	0	0	**1**	0	1	**0**	0	0	0	1	1	**0**	0
1	1	1	1	1	**1**	1	1	**0**	1	0	0	1	1	**1**	1
		(1)	(2)	(1)	**(3)**	(1)	(1)	**(4)**	(1)	(3)	(2)	(1)	(1)	**(2)**	(1)

Un problema fondamentale del calcolo proposizionale è quello di dimostrare che una data formula è una tautologia. Molti altri problemi interessanti si possono ridurre a questo. Per esempio, se dobbiamo dimostrare che la formula A è una contraddizione, ci basta dimostrare che $\neg A$ è una tautologia; se dobbiamo dimostrare che, assumendo che le formule A e B siano vere, allora anche C è vera, ci basta dimostrare che $((A \wedge B) \Rightarrow C)$ è una tautologia.

Per quanto visto sopra, per vedere se una formula è una tautologia, è sufficiente costruire la sua tabella di verità e controllare che il valore della formula sia 1 su tutte le righe (quindi per ogni interpretazione). Questo procedimento, anche se può essere completamente automatizzato, può richiedere la costruzione di una tabella molto grande (come visto, il numero di righe è 2^n, dove n è il numero di simboli proposizionali della formula) ed è molto soggetto ad errori se fatto a mano. Pertanto nel seguito useremo solo raramente questa tecnica, e vedremo invece come dimostrare che una formula è una tautologia usando le dimostrazioni per sostituzione introdotte nei capitoli precedenti.

Se invece dobbiamo mostrare che una formula è soddisfacibile, non c'è bisogno di costruire tutta la tabella di verità, ma è sufficiente trovare una singola interpretazione che renda la formula vera. Spesso questo può essere fatto in modo abbastanza efficiente ragionando sulla struttura della formula. Analogamente, per mostrare che una formula *non è* una tautologia è sufficiente trovare una interpretazione che renda la formula falsa.

ESEMPIO 3.8 (FORMULA NON TAUTOLOGICA)
Mostriamo, senza costruire la tabella di verità, che la seguente formula non è una tautologia:

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

Sfruttiamo la struttura della formula per costruire un'interpretazione che renda falsa la formula. Per cominciare, osserviamo che il connettivo principale della formula è un'implicazione. L'unico caso in cui un'implicazione è falsa è quando la premessa è vera e la conseguenza è falsa (si veda la Definizione 3.3). Quindi l'interpretazione cercata deve associare 0 *a* Q*, la conseguenza, e* 1 *alla sotto-formula* $((P \Rightarrow \neg Q) \wedge \neg P)$*, la premessa. A sua volta quest'ultima formula ha come connettivo principale una congiunzione, che è vera solo se entrambi gli argomenti sono veri. Quindi in particolare* $\neg P$ *deve valere 1, cioè l'interpretazione deve associare 0 a* P*. Abbiamo quindi individuato l'interpretazione* $\{P \mapsto 0, Q \mapsto 0\}$*, che per il ragionamento fatto è l'unica che potrebbe rendere la formula falsa. Valutando l'intera formula in questa interpretazione otteniamo effettivamente 0 (cioè falso), come si vede dalla seguente tabella:*

P	Q	$(((P$	$\Rightarrow$	$\neg$	$Q)$	$\wedge$	$\neg$	$P)$	$\Rightarrow$	$Q)$
0	0	0	1	1	0	1	1	0	**0**	0
		(1)	(3)	(2)	(1)	(4)	(2)	(1)	**(5)**	(1)

3.3 Formalizzare proposizioni e inferenze

Come anticipato nell'introduzione di questo capitolo, per analizzare logicamente un'inferenza (o un ragionamento, una dimostrazione, ...) al fine di verificarne la correttezza, come primo passo occorre formalizzare le proposizioni che essa contiene, rendendone esplicita la struttura logica. Utilizzeremo quindi le formule proposizionali per formalizzare semplici enunciati in linguaggio naturale.

3.3.1 Formalizzare le proposizioni

In generale il procedimento di estrazione, da una proposizione in italiano, di una formula che la rappresenta non è molto complicato. Seguiamone i passi nel caso della proposizione $\boxed{\textit{"Piove e fa freddo."}}$.

- Come prima cosa occorre introdurre un simbolo proposizionale per ogni proposizione elementare, cioè ogni pezzo della frase che riconosciamo essere una proposizione (ha uno e un solo valore di verità), e che non può essere scomposta in proposizioni più piccole. Nel nostro esempio, fissiamo i simboli proposizionali P per *"piove"* e R per *"fa freddo"*.[4]
- Successivamente si costruisce la formula collegando le occorrenze dei simboli proposizionali con connettivi logici, in modo da rispecchiare fedelmente il significato originale. Nell'esempio, la formula risultante è $\boxed{(P \wedge R)}$, dato che *"e"* rappresenta chiaramente una congiunzione.

La scelta dei connettivi non è sempre ovvia poiché in italiano possono essere resi in molti modi diversi. Inoltre a volte la stessa locuzione viene usata per connettivi diversi, come "oppure" che può rappresentare sia l'*or* $\vee$ che lo *xor* $\oplus$. Nel linguaggio naturale la disambiguazione tra disgiunzione inclusiva ed esclusiva è spesso lasciata al contesto.

[4] Non usiamo il simbolo F per *"fa freddo"* per evitare confusione con F che rappresenta *falso*.

ESEMPIO 3.9 (DA PROPOSIZIONI IN LINGUAGGIO NATURALE A FORMULE PROPOSIZIONALI)
Vediamo come formalizzare altre proposizioni simili.

1. "Piove ma non fa freddo." *Usando i simboli proposizionali appena introdotti, una ragionevole formalizzazione è* $(P \wedge \neg R)$. *Infatti anche* "ma" *rappresenta una congiunzione, anche se con un significato leggermente diverso da* "e".

2. "Se piove o fa freddo allora ci si copre." *Usiamo i simboli* P *e* R *come sopra, e introduciamo* C *per* "ci si copre". *Allora la formula risultante è* $((P \vee R) \Rightarrow C)$. *Infatti* "se ... allora ..." *rappresenta un'implicazione, e* "o" *una disgiunzione inclusiva, dato che può piovere e fare freddo contemporaneamente.*

3. "Se piove non si esce o si prende l'ombrello." *Usiamo* E *per* "si esce" *e* O *per* "si prende l'ombrello". *Una ragionevole formalizzazione è* $(P \Rightarrow (\neg E \oplus O))$. *Infatti in questo caso* "o" *rappresenta una disgiunzione esclusiva: non ha senso prendere l'ombrello e non uscire.*

   Si noti che un'altra formalizzazione possibile, data l'ambiguità della proposizione, sarebbe quella che pone in disgiunzione gli enunciati "Se piove non si esce" e "si prende l'ombrello": $((P \Rightarrow \neg E) \oplus O)$. *Il contesto e il buon senso ci portano a scartare questa possibilità.*

Non sempre la formalizzazione di una proposizione è semplice come negli esempi appena visti. Le principali difficoltà possono essere dovute alla complessità o all'ambiguità della proposizione, ma anche alla corretta interpretazione di certe locuzioni in linguaggio naturale.

ESEMPIO 3.10
Consideriamo le proposizioni elementari "io vado al cinema", *rappresentata dalla variabile proposizionale* V, *e* "tu resti a casa", *rappresentata da* R. *Come possiamo formalizzare la proposizione* "Affinché io vada al cinema è necessario che tu resti a casa"? *La frase dice che* R *è una* condizione necessaria *per* V, *e questo esprime un'implicazione tra le due. Come discusso nella Nota 3.3, la frase può essere formalizzata correttamente con* $V \Rightarrow R$. *Infatti se* R *è falsa ("non resti a casa") anche* V *deve essere falsa ("non vado al cinema").*

3.3.2 Formalizzare le inferenze

Si può sfruttare la formalizzazione di proposizioni per mostrare la correttezza di inferenze o di semplici ragionamenti espressi in linguaggio naturale. Un'inferenza è corretta se la tesi è una conseguenza logica delle ipotesi, e questo si può accertare dimostrando che l'implicazione *(ipotesi)* $\Rightarrow$ *(tesi)* è una tautologia. Vediamo due esempi: un'inferenza corretta e una errata.

ESEMPIO 3.11 (DIMOSTRAZIONE DI CORRETTEZZA DI UN'INFERENZA)
Si dimostri la correttezza della seguente inferenza:

"Studio oggi oppure domani, ma domani non studio, quindi studio oggi"

Per formalizzare la frase, introduciamo un simbolo proposizionale per ogni proposizione elementare, quindi SO *per* "studio oggi" *e* SD *per* "studio domani".

Ora costruiamo una formula proposizionale che usa questi simboli e che esprime il significato inteso della frase:

$$(((SO \vee SD) \wedge \neg SD) \Rightarrow SO)$$

Quindi abbiamo rappresentato "oppure" con la disgiunzione $\vee$, *"non" con la negazione* $\neg$, *"quindi" con l'implicazione* $\Rightarrow$ *e "ma" con la congiunzione "*$\wedge$*". Si noti pure che abbiamo associato in modo abbastanza flessibile le proposizioni della frase alle sotto-formule: "domani" è rappresentato da* SD *poiché sottintende "studio domani", e "domani non studio" da* $\neg SD$.

Ora, dimostrare la correttezza dell'inferenza *significa mostrare che la formula proposizionale ottenuta è una tautologia: il lettore può verificarlo costruendo la tabella di verità. In questo modo si completa la dimostrazione che la proposizione "studio oggi" è una conseguenza logica delle proposizioni "studio oggi o domani" e "non studio domani", e quindi che l'inferenza è corretta.*

Cosa cambia se nella formula sostituiamo la disgiunzione inclusiva con quella esclusiva? Dobbiamo ricostruire l'intera tabella di verità?

Naturalmente non tutte le inferenze sono corrette: vediamo come la formalizzazione logica ci può aiutare a rivelare l'inesattezza di un ragionamento.

ESEMPIO 3.12 (DIMOSTRAZIONE DI NON CORRETTEZZA DI UN'INFERENZA)
È corretta la seguente inferenza?

"Se studio oggi allora domani non studio, ma oggi non studio, quindi domani studierò"

Come nell'esempio precedente possiamo usare i simboli proposizionali SO per "studio oggi" e SD per "studio domani". Una formula proposizionale che rappresenta fedelmente il significato della frase è:

$$(((SO \Rightarrow \neg SD) \wedge \neg SO) \Rightarrow SD)$$

Ma come possiamo dedurre dall'Esempio 3.8 dove abbiamo analizzato una formula con la stessa struttura (anche se con simboli proposizionali diversi), l'interpretazione $\{SO \mapsto 0, SD \mapsto 0\}$ *rende questa formula falsa, pertanto non è una tautologia. Quindi l'inferenza non è corretta, perché "studio domani" non è una conseguenza logica di "se studio oggi allora domani non studio" e di "oggi non studio".*

ESEMPIO 3.13 (CORRETTEZZA DI INFERENZE LOGICHE)
Usando i simboli proposizionali Col per "io sono colpevole" *e Pun per* "io devo essere punito", *valutiamo se le seguenti inferenze sono logicamente corrette:*

1. *[Modus Ponens]* "Se io sono colpevole, allora devo essere punito. Io sono colpevole. Quindi devo essere punito."
   Una possibile formalizzazione è $\boxed{(((Col \Rightarrow Pun) \wedge Col) \Rightarrow Pun)}$*: si verifica facilmente che è una tautologia, quindi l'inferenza è corretta.*

2. "Se io sono colpevole, allora devo essere punito. Io non sono colpevole. Dunque non devo essere punito."
   Una formalizzazione è $\boxed{(((Col \Rightarrow Pun) \wedge \neg Col) \Rightarrow \neg Pun)}$*. Non è una tautologia perché l'interpretazione* $\{Pun \mapsto 1, Col \mapsto 0\}$ *la rende falsa (posso essere punito anche se non sono colpevole); quindi l'inferenza non è corretta.*

3. *[Modus Tollens]* "Se io sono colpevole, allora devo essere punito. Io non devo essere punito. Dunque non sono colpevole."
   Una formalizzazione è $\boxed{(((Col \Rightarrow Pun) \wedge \neg Pun) \Rightarrow \neg Col)}$*, che si verifica essere una tautologia. Quindi l'inferenza è corretta.*

4. "Se io sono colpevole, allora devo essere punito. Io devo essere punito. Quindi sono colpevole".
   Una possibile formalizzazione è $\boxed{(((Col \Rightarrow Pun) \wedge Pun) \Rightarrow Col)}$*, che non è una tautologia: l'interpretazione* $\{Pun \mapsto 1, Col \mapsto 0\}$ *la rende falsa (non posso invertire l'ordine dell'implicazione: la mia colpevolezza implica la punizione ma non necessariamente vale il viceversa). Quindi l'inferenza non è corretta.*

La formalizzazione di proposizioni può essere utile anche per determinare se un enunciato è vero o falso non in generale, ma rispetto a una interpretazione "standard", cioè nella quale a ogni proposizione elementare viene associato un valore di verità determinato dalla nostra comune conoscenza.

ESEMPIO 3.14 (VALUTAZIONE DI PROPOSIZIONI RISPETTO ALL'INTERPRETAZIONE STANDARD)
Consideriamo la seguente domanda:

È vero che "Se la Terra fosse disabitata allora la Luna sarebbe una stella"?

Se indichiamo con TD la proposizione elementare "la Terra è disabitata" *e con LS* "la Luna è una stella", *la frase può essere formalizzata con la formula* $(TD \Rightarrow LS)$*. In questo caso non si chiede se la formula è* sempre vera *(cioè se è una tautologia) ma, implicitamente, se è vera nell'interpretazione (che chiamiamo "standard") in cui sia "la Terra è disabitata" che "la Luna è una stella" sono entrambe ovviamente false. Segue dalla Definizione 3.3 che l'implicazione è vera, poiché sia la premessa che la conseguenza sono false.*

3.4 Dimostrazione di equivalenze logiche

Abbiamo già detto che molti problemi del calcolo proposizionale si possono ridurre alla dimostrazione che una certa formula proposizionale è una tautologia, cioè è vera per qualunque interpretazione delle sue variabili proposizionali. L'obiettivo di questa sezione è di mostrare come anche la tecnica di dimostrazione per sostituzione (introdotta nella Sezione 1.4 per le espressioni aritmetiche, e sfruttata nella Sezione 2.4.5 per dimostrare uguaglianze di insiemi) può essere usata proficuamente anche per dimostrare che certe formule sono tautologie. Come prima cosa vediamo quando due formule sono *logicamente equivalenti*.

DEFINIZIONE 3.7 (EQUIVALENZA LOGICA)
*Due formule proposizionali A e B sono **logicamente equivalenti**, scritto $A \equiv B$, se assumono lo stesso valore di verità per qualunque interpretazione.*

Viceversa, scriviamo $A \not\equiv B$ se esiste un'interpretazione che rende vera una e falsa l'altra.

Segue immediatamente dalla definizione che si può ridurre la dimostrazione che una formula è una tautologia a una dimostrazione di equivalenza logica.

PROPOSIZIONE 3 (TAUTOLOGIE E EQUIVALENZA LOGICA)
Siano A e B formule proposizionali.

- *A è una tautologia se e solo se $A \equiv \mathsf{T}$.*
- *$(A \Leftrightarrow B)$ è una tautologia se e solo se $A \equiv B$.*

Si noti che il secondo punto permette di rappresentare la relazione di equivalenza logica ($\equiv$) all'interno di una formula proposizionale con il connettivo di doppia implicazione $\Leftrightarrow$. Ciò consente di rappresentare tecniche di dimostrazione di equivalenze direttamente come formule proposizionali, e quindi di valutarne la correttezza. Per esempio, consideriamo la seguente tecnica di dimostrazione: *"Per dimostrare che $A \equiv C$ è sufficiente trovare una proposizione B tale che $A \equiv B$ e $B \equiv C$"*. È giusto questo modo di ragionare? Sfruttando la Proposizione 3 possiamo rappresentare questa affermazione con la formula: $(((A \Leftrightarrow B) \wedge (B \Leftrightarrow C)) \Rightarrow (A \Leftrightarrow C))$, che è una tautologia (lasciamo al lettore la dimostrazione). Questo dimostra che la tecnica di dimostrazione descritta, chiamata *transitività dell'equivalenza logica*, è corretta.

Per dimostrare che due formule sono logicamente equivalenti possiamo partire dalla prima e cercare di trasformarla nella seconda con una sequenza di passi che costituiscono una dimostrazione per sostituzione. A tal fine abbiamo bisogno di introdurre alcune leggi, che sono delle equivalenze logiche in un certo senso "primitive", da utilizzare come giustificazioni nei passi di dimostrazione. Come il lettore noterà immediatamente, alcune di queste leggi sono analoghe a quelle per l'uguaglianza di insiemi mostrate nella Sezione 2.4.1, facendo corrispondere F all'insieme vuoto $\varnothing$, T all'universo $\mathcal{U}$, la negazione al complemento, la congiunzione all'intersezione, e la disgiunzione all'unione.

PROPOSIZIONE 4 (ALCUNE LEGGI PER L'EQUIVALENZA DEL CALCOLO PROPOSIZIONALE)
Per tutte le formule proposizionali A, B e C valgono le seguenti equivalenze logiche:

Leggi su congiunzione e disgiunzione

$(A \vee \mathsf{F}) \equiv A$	$(A \wedge \mathsf{T}) \equiv A$	*(elemento neutro)*
$(A \vee \mathsf{T}) \equiv \mathsf{T}$	$(A \wedge \mathsf{F}) \equiv \mathsf{F}$	*(elemento assorbente)*
$(A \wedge A) \equiv A$	$(A \vee A) \equiv A$	*(idempotenza)*
$(A \wedge B) \equiv (B \wedge A)$	$(A \vee B) \equiv (B \vee A)$	*(commutatività)*
$(A \wedge (B \wedge C)) = ((A \wedge B) \wedge C)$	$(A \vee (B \vee C)) \equiv ((A \vee B) \vee C)$	*(associatività)*
$(A \vee (B \wedge C)) \equiv ((A \vee B) \wedge (A \vee C))$	$(A \wedge (B \vee C)) \equiv ((A \wedge B) \vee (A \wedge C))$	*(distributività)*

Leggi su negazione

	$\neg \mathsf{T} \equiv \mathsf{F}$	*(T : F)*
	$\neg\neg A \equiv A$	*(doppia negazione)*
	$(A \vee \neg A) \equiv \mathsf{T}$	*(terzo escluso)*
	$(A \wedge \neg A) \equiv \mathsf{F}$	*(contraddizione)*
$\neg(A \vee B) \equiv (\neg A \wedge \neg B)$	$\neg(A \wedge B) \equiv (\neg A \vee \neg B)$	*(De Morgan)*

Leggi di eliminazione di altri connettivi

$(A \Rightarrow B) \equiv (\neg A \vee B)$	*(eliminazione dell'implicazione)*
$\neg(A \Rightarrow B) \equiv (A \wedge \neg B)$	*(eliminazione dell'implicazione negata)*
$(A \Leftrightarrow B) \equiv ((A \wedge B) \vee (\neg A \wedge \neg B))$	*(eliminazione della doppia implicazione)*
$(A \oplus B) \equiv ((A \wedge \neg B) \vee (\neg A \wedge B))$	*(eliminazione dello xor)*

Le equivalenze appena elencate descrivono alcune proprietà algebriche dei connettivi logici (vedi quelle per congiunzione, disgiunzione e negazione), oppure consentono di eliminare un connettivo sostituendolo con una opportuna combinazione di altri connettivi. Ovviamente l'equivalenza è una relazione simmetrica, cioè $A \equiv B$ se e solo se $B \equiv A$, e quindi ogni legge può essere usata in entrambe le direzioni (sostituendo in un certo contesto il membro destro con il sinistro oppure il sinistro con il destro). Tuttavia, nella nostra esperienza, ogni legge viene usata preferibilmente in una direzione, pertanto le abbiamo riportate in modo che tale direzione preferita sia da sinistra verso destra.

Ma come possiamo verificare che le leggi introdotte siano corrette? Si ricordi che per la Proposizione 3, A è logicamente equivalente a B se e solo se $(A \Leftrightarrow B)$ è una tautologia. Quindi per mostrare che una legge del tipo $A \equiv B$ è corretta ci basta costruire la tabella di verità della formula $(A \Leftrightarrow B)$ e controllare che essa sia vera per ogni interpretazione.

ESEMPIO 3.15 (CORRETTEZZA DELLE LEGGI DI DE MORGAN)
Mostriamo che la prima legge di De Morgan è corretta (la dimostrazione per la seconda legge è del tutto analoga). Per quanto appena detto, costruiamo la tabella di verità della formula $(\neg(A \vee B) \Leftrightarrow (\neg A \wedge \neg B))$*:*

A	B	$(\neg$	$(A$	$\vee$	$B)$	$\Leftrightarrow$	$(\neg$	A	$\wedge$	$\neg$	$B))$
0	0	1	0	0	0	**1**	1	0	1	1	0
0	1	0	0	1	1	**1**	1	0	0	0	1
1	0	0	1	1	0	**1**	0	1	0	1	0
1	1	0	1	1	1	**1**	0	1	0	0	1
		(3)	(1)	(2)	(1)	(**4**)	(2)	(1)	(3)	(2)	(1)

Come si vede dalla colonna (4) la formula è una tautologia.

Sfruttando le leggi introdotte siamo ora in grado di impostare delle dimostrazioni per sostituzione che ci permetteranno di provare altre equivalenze logiche. È importante sottolineare che ogni equivalenza dimostrata può essere usata a sua volta come giustificazione in dimostrazioni successive, con un meccanismo simile alla costruzione delle dimostrazioni di teoremi in matematica: se proviamo separatamente alcuni lemmi, essi possono essere utilizzati senza bisogno di ri-dimostrarli nella dimostrazione del teorema principale.

ESEMPIO 3.16 (COMPLEMENTO E ASSORBIMENTO)
Dimostriamo le seguenti equivalenze logiche:

$(A \vee (\neg A \wedge B)) \equiv (A \vee B)$	$(A \wedge (\neg A \vee B)) \equiv (A \wedge B)$	*(complemento)*
$(A \vee (A \wedge B)) \equiv A$	$(A \wedge (A \vee B)) \equiv A$	*(assorbimento)*

Consideriamo la prima legge del complemento. Una buona strategia, che in questo caso funziona, consiste nel partire dalla formula più complessa e nell'usare le leggi per semplificarla finché non si ottiene l'altra. Partiamo quindi da $(A \vee (\neg A \wedge B))$*:*[5]

$$
\begin{aligned}
& (A \vee (\neg A \wedge B)) \\
\equiv \quad & \{ \textit{(distributività)} \} \\
& (\underline{(A \vee \neg A)} \wedge (A \vee B)) \\
\equiv \quad & \{ \textit{(terzo escluso)} \} \\
& (\mathsf{T} \wedge (A \vee B)) \\
\equiv \quad & \{ \textit{(commutatività)} \} \\
& ((A \vee B) \wedge \mathsf{T}) \\
\equiv \quad & \{ \textit{(elemento neutro)} \} \\
& (A \vee B)
\end{aligned}
$$

In modo del tutto analogo si può dimostrare la seconda legge del complemento, nella quale la congiunzione e la disgiunzione giocano un ruolo simmetrico.

Vediamo invece che la stessa strategia non funziona con la prima legge dell'assorbimento, $(A \vee (A \wedge B)) \equiv A$*. Infatti, partendo dal membro sinistro verrebbe naturale applicare le leggi nella sequenza che segue:*

$$
\begin{aligned}
& (A \vee (A \wedge B)) \\
\equiv \quad & \{ \textit{(distributività)} \} \\
& (\underline{(A \vee A)} \wedge (A \vee B)) \\
\equiv \quad & \{ \textit{(idempotenza)} \} \\
& (A \wedge (A \vee B))
\end{aligned}
$$

Si noti che abbiamo ottenuto il membro sinistro della seconda legge del complemento, ed è facile intuire che procedendo allo stesso modo otterremmo la formula da cui eravamo partiti, chiudendo uno sterile ciclo. Quella che segue invece è una dimostrazione corretta della legge, come è facile verificare, ma essa usa in modo non ovvio la legge dell'elemento neutro al contrario.

$$
\begin{aligned}
& (A \vee (A \wedge B)) \\
\equiv \quad & \{ \textit{(elemento neutro), al contrario} \} \\
& ((A \wedge \mathsf{T}) \vee (A \wedge B)) \\
\equiv \quad & \{ \textit{(distributività)} \} \\
& (A \wedge \underline{(\mathsf{T} \vee B)}) \\
\equiv \quad & \{ \textit{(commutatività) e (elemento assorbente)} \} \\
& (A \wedge \mathsf{T}) \\
\equiv \quad & \{ \textit{(elemento neutro)} \} \\
& A
\end{aligned}
$$

Riassumendo, spesso una buona strategia consiste nel partire dalla formula più complessa e nell'usare le leggi per semplificarla fino ad ottenere la formula equivalente cercata. Ma non sempre questa strategia funziona: in tal caso occorre un pizzico di intuizione per impostare una dimostrazione concisa e corretta.

ESEMPIO 3.17 (CONTRONOMINALE)
Dimostriamo la seguente equivalenza logica:

[5] Nelle dimostrazioni che seguono a ogni passaggio sottolineiamo la porzione di formula alla quale viene applicata la legge indicata nella giustificazione, a meno che non sia l'intera formula.

$$(A \Rightarrow B) \equiv (\neg B \Rightarrow \neg A) \qquad \textit{(contronominale)}$$

Partiamo dalla formula più complessa, che in questo caso è il membro destro:

$(\neg B \Rightarrow \neg A)$

$\equiv$ { *(eliminazione dell'implicazione)* }

$(\underline{\neg\neg B} \vee \neg A)$

$\equiv$ { *(doppia negazione)* }

$(B \vee \neg A)$

$\equiv$ { *(commutatività)* }

$(\neg A \vee B)$

$\equiv$ { *(eliminazione dell'implicazione), al contrario* }

$(A \Rightarrow B)$

Nel seguito, come da prassi consolidata, tenderemo a semplificare le dimostrazioni non indicando esplicitamente i passaggi nei quali applichiamo le leggi della commutatività, associatività e idempotenza.

ESEMPIO 3.18 (LE DIMOSTRAZIONI NON SONO UNICHE)
Dimostriamo ora che $\neg(P \vee (\neg P \wedge Q)) \equiv (\neg P \wedge \neg Q)$ *usando il principio di sostituzione. Nei riquadri che seguono mostriamo tre possibili dimostrazioni. Come si vede, scelte diverse delle leggi da applicare nei vari passi portano a dimostrazioni di lunghezza diversa.*

La dimostrazione a sinistra applica in modo sistematico le leggi per semplificare la formula a partire dall'operatore più esterno, la negazione. La dimostrazione in alto a destra invece posticipa l'uso delle leggi di De Morgan, applicandole solo quando la sotto-formula più interna è stata semplificata. Infine nella dimostrazione in basso a destra abbiamo riconosciuto che si può applicare, con una opportuna sostituzione, la legge del complemento dimostrata precedentemente, il che permette di ridurre la dimostrazione a due soli passi.

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

$\equiv$ { *(De Morgan)* }

$(\neg P \wedge \underline{\neg(\neg P \wedge Q)})$

$\equiv$ { *(De Morgan)* }

$(\neg P \wedge (\underline{\neg\neg P} \vee \neg Q))$

$\equiv$ { *(doppia negazione)* }

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

$\equiv$ { *(distributività)* }

$(\underline{(\neg P \wedge P)} \vee (\neg P \wedge \neg Q))$

$\equiv$ { *(contraddizione)* }

$(\mathsf{F} \vee (\neg P \wedge \neg Q))$

$\equiv$ { *(elemento neutro)* }

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

$\neg\underline{(P \vee (\neg P \wedge Q))}$

$\equiv$ { *(distributività)* }

$\neg\big(\underline{(P \vee \neg P)} \wedge (P \vee Q)\big)$

$\equiv$ { *(terzo escluso)* }

$\neg\underline{\big(\mathsf{T} \wedge (P \vee Q)\big)}$

$\equiv$ { *(elemento neutro)* }

$\neg(P \vee Q)$

$\equiv$ { *(De Morgan)* }

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

$\neg\underline{(P \vee (\neg P \wedge Q))}$

$\equiv$ { *(complemento)* }

$\neg(P \vee Q)$

$\equiv$ { *(De Morgan)* }

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

Vediamo ora come si possono usare le dimostrazioni per sostituzione per dimostrare che certe formule sono tautologie. Facendo riferimento alla Proposizione 3 abbiamo due situazioni diverse:

1. La tautologia da dimostrare ha come operatore principale la doppia implicazione, cioè ha la forma $(A \Leftrightarrow B)$. In questo caso è sufficiente dimostrare che A e B sono logicamente equivalenti, come negli esempi visti sopra.

2. Se invece la tautologia da dimostrare non ha quella forma, allora possiamo cercare di dimostrare che è logicamente equivalente a T.

ESEMPIO 3.19 (MODUS PONENS)
Dimostrare che la formula $(((A \Rightarrow B) \wedge A) \Rightarrow B)$, *chiamata* Modus Ponens, *è una tautologia. Mostriamo che è equivalente a* T*:*

$$
\begin{aligned}
& (\underline{(A \Rightarrow B)} \wedge A) \Rightarrow B) \\
\equiv \quad & \{ \textit{(eliminazione dell'implicazione)} \} \\
& (\underline{((\neg A \vee B) \wedge A)} \Rightarrow B) \\
\equiv \quad & \{ \textit{(complemento)} \} \\
& ((B \wedge A) \Rightarrow B) \\
\equiv \quad & \{ \textit{(eliminazione dell'implicazione)} \} \\
& (\underline{\neg(B \wedge A)} \vee B) \\
\equiv \quad & \{ \textit{(De Morgan)} \} \\
& ((\underline{\neg B} \vee \neg A) \underline{\vee B}) \\
\equiv \quad & \{ \textit{(commutatività), (associatività), (terzo escluso)} \} \\
& (\mathsf{T} \vee \neg A) \\
\equiv \quad & \{ \textit{(elemento assorbente)} \} \\
& \mathsf{T}
\end{aligned}
$$

3.5 Esercizi

3.5.1 Esercizi di comprensione

3.5.1.1 Quali delle seguenti sono proposizioni? Se sono proposizioni, sono vere o false nell'interpretazione standard?

(a) "$2+2=4$"
(b) "$3 \times 5 = 10$"
(c) "La capitale dell'Australia è Sydney?"
(d) "La capitale dell'Australia è Sydney"
(e) "A scuola è vietato fumare"
(f) "Non fumare a scuola!"
(g) "Posso fumare a scuola?"
(h) "Non so se posso fumare a scuola"
(i) "Che ore sono?"
(j) "Esiste un valore che sommato a 1 dà 2"
(k) "$x+1=2$"

3.5.1.2 Per ognuna delle seguenti frasi, inclusa questa, dire se nella formalizzazione bisogna impiegare $\vee$ o $\oplus$:

(a) "Per superare l'esame dovete leggere le note o le dispense"
(b) "Se compri la macchina nuova dal mio amico puoi pagare in contanti con lo sconto o a prezzo pieno con rate mensili"
(c) "Per cenare col menù turistico puoi scegliere due portate dalla lista in alto o tre portate da quella in basso"

(d) "La lezione viene annullata se è sciopero o se il docente è malato"

(e) "L'autobus si fermava se qualche persona doveva scendere o salire"

(f) "Quello che ha vinto la corsa era molto forte o aveva preso qualche sostanza proibita"

(g) "Per avere sue notizie chiedi ai genitori o al fratello"

3.5.1.3 Dire con quali connettivi possono essere resi i termini evidenziati nelle seguenti proposizioni:

(a) "Mario è agile, **ma** Rosario è forte"

(b) "Paolo è in campo, **anche se** ha la febbre alta"

(c) "Johnny è in Italia **senza** avere il passaporto"

(d) "Il fantasma appare nel castello **esattamente** a mezzanotte"

3.5.1.4 Quale regola preferireste per l'esame? Perché?

1) "se rispondete bene a tutte le domande allora prendete 30"

2) "prendete 30 solo se rispondete bene a tutte le domande"

Argomentate la risposta formalizzando i due enunciati.

3.5.1.5 Le tabelle di verità, se riempite manualmente, conducono facilmente a errori che sono poi difficili da identificare, inoltre presentano un'esplosione combinatoria all'aumentare dei simboli proposizionali coinvolti. Per convicervene, provate a trovare gli errori nella seguente tabella (se ve ne sono):

P	Q	R	S	$(((P$	$\Rightarrow$	$Q)$	$\oplus$	$R)$	$\Leftarrow$	$\neg$	$S)$
0	0	0	0	0	1	0	1	0	1	1	0
0	0	0	1	0	1	0	1	0	1	0	1
0	0	1	0	0	1	0	0	1	0	1	0
0	0	1	1	0	1	0	0	1	1	0	1
0	1	0	0	0	1	1	1	0	0	1	0
0	1	0	1	0	1	1	1	0	1	0	1
0	1	1	0	0	1	1	0	1	0	1	0
0	1	1	1	0	1	1	0	1	1	0	1
1	0	0	0	1	0	0	0	0	0	1	0
1	0	0	1	1	0	0	0	0	1	0	1
1	0	1	0	1	0	0	1	1	1	1	0
1	0	1	1	1	0	0	1	1	1	0	1
1	1	0	0	1	1	1	1	0	1	1	0
1	1	0	1	1	1	1	1	0	1	0	1
1	1	1	0	1	1	1	0	1	0	1	0
1	1	1	1	1	1	1	0	1	1	0	1
				(1)	(2)	(1)	(3)	(1)	(4)	(2)	(1)

3.5.1.6 [Difficile] Gli operatori binari che abbiamo visto sono quelli più "intuitivi", ma esistono molte altre possibilità di combinare due proposizioni. Ad esempio, per analogia con gli insiemi, si potrebbe definire

$$(P \setminus Q) \equiv (P \wedge \neg Q) \tag{3.1}$$

Oppure si potrebbero definire operatori ternari come

$$(\text{if } P \text{ then } Q \text{ else } R) \equiv (P \wedge Q) \vee (\neg P \wedge R) \tag{3.2}$$

In generale un operatore con n argomenti è determinato da una colonna di una tabella di verità con 2^n righe.

(a) Quanti possibili operatori unari diversi esistono?

(b) Quanti possibili operatori binari diversi esistono?

(c) Quanti possibili operatori n-ari esistono?

(d) Data la colonna che identifica un qualsiasi operatore n-ario, definire una tecnica per costruire una formula equivalente che usi solo i connettivi $\neg$, $\wedge$ e $\vee$.

3.5.2 Esercizi di approfondimento

3.5.2.1 Costruire le tabelle di verità degli operatori $(P \setminus Q)$ e $(\mathsf{if}\ P\ \mathsf{then}\ Q\ \mathsf{else}\ R)$ definiti nei punti (3.1) e (3.2).

3.5.2.2 Costruire le tabelle di verità delle seguenti formule e indicare quali di queste sono tautologie

(a) $((P \vee Q) \Rightarrow P)$
(b) $((P \vee Q) \Rightarrow (P \wedge Q))$
(c) $((P \vee Q) \Leftrightarrow (P \wedge Q))$
(d) $((P \Rightarrow Q) \Rightarrow (Q \Rightarrow P))$
(e) $(P \Rightarrow (Q \Rightarrow (Q \Rightarrow P)))$
(f) $(((P \Rightarrow Q) \Rightarrow Q) \Rightarrow Q)$
(g) $(((P \Rightarrow Q) \Rightarrow Q) \Rightarrow \neg Q)$
(h) $(((P \Rightarrow Q) \Rightarrow Q) \vee \neg Q)$
(i) $((P \oplus Q) \wedge (\neg Q \oplus P))$
(j) $((P \wedge Q) \vee (\neg P \wedge \neg Q))$
(k) $((P \Rightarrow Q) \wedge (\neg P \Rightarrow R))$
(l) $(((P \vee Q) \Leftrightarrow (P \wedge Q)) \Leftrightarrow (P \Leftrightarrow Q))$
(m) $(\neg(P \vee Q) \Rightarrow (\neg Q \vee \neg P))$

3.5.2.3 Costruire le tabelle di verità delle seguenti formule e indicare quali di queste sono tautologie

(a) $((P \wedge (Q \vee R)) \Rightarrow (P \vee (Q \wedge R)))$
(b) $((P \vee (Q \wedge R)) \Rightarrow (P \wedge (Q \vee R)))$
(c) $((P \wedge (Q \Rightarrow R)) \Rightarrow (Q \Rightarrow (P \wedge R)))$
(d) $((Q \Rightarrow (P \wedge R)) \Rightarrow (P \wedge (Q \Rightarrow R)))$
(e) $((P \Rightarrow (Q \vee R)) \Leftrightarrow (Q \Rightarrow (P \vee R)))$
(f) $((\neg(P \wedge Q) \Rightarrow R) \Rightarrow (Q \vee \neg(P \wedge R)))$
(g) $\neg(Q \wedge (R \Rightarrow (P \wedge R)))$
(h) $((Q \wedge R) \vee ((P \wedge Q) \vee (P \wedge R)))$
(i) $\neg((P \vee (Q \vee R)) \Rightarrow (P \wedge (Q \wedge R)))$

3.5.2.4 Per ognuna delle seguenti formule, determinare se è una tautologia oppure no. Se non è una tautologia fornire un'interpretazione che la rende falsa *senza* costruire la tabella di verità, altrimenti costruire la tabella.

(a) $(((P \wedge Q) \vee P) \Leftrightarrow P)$
(b) $(P \Rightarrow (Q \Rightarrow \neg R))$
(c) $(P \Rightarrow (P \vee Q))$
(d) $((P \Rightarrow Q) \Rightarrow \neg P)$

3.5.2.5 Si formalizzino le seguenti proposizioni:

(a) "Aldo va al cinema ma Dario no"

(b) “Luigi andrà al cinema o andrà al teatro”

(c) “Se ho lezione di LMB allora è martedì o è venerdì”

(d) “Non puoi montare sulle montagne russe se sei più basso di un metro e se non hai più di 16 anni”

3.5.2.6 Le seguenti proposizioni in linguaggio naturale esprimono delle implicazioni (semplici o doppie) tra i simboli proposizionali V (*“io vado al cinema”*) e R (*“Tu resti a casa”*). Indicare per ognuna di esse una formula proposizionale che la rappresenta.

(a) “Io vado al cinema se tu resti a casa”

(b) “Io vado al cinema solo se tu resti a casa”

(c) “Io vado al cinema se e solo se tu resti a casa”

(d) “Perché io vada al cinema è necessario che tu resti a casa”

(e) “Perché io vada al cinema è sufficiente che tu resti a casa”

(f) “Condizione necessaria e sufficiente perché io vada al cinema è che tu resti a casa”

3.5.2.7 Siano:

- $V =$ “viaggi a oltre 50 km/h”
- $M =$ “prendi la multa”

Tradurre in formule le seguenti frasi combinando coi connettivi logici le sole proposizioni V ed M:

(a) “non superi i 50 km/h”

(b) “superi i 50 km/h ma non prendi la multa”

(c) “prendi la multa se superi i 50 km/h”

(d) “se non superi i 50 km/h, allora non ti fanno la multa”

(e) “superare i 50 km/h è sufficiente per prendere la multa”

(f) “prendi la multa senza superare i 50 km/h”

(g) “ogni volta prendi la multa proprio quando stai guidando a più di 50 km/h”

3.5.2.8 Aldo, Barbara e Carlo sono tre studenti che hanno sostenuto un esame. Ponendo:

- $A =$ “Aldo ha superato l’esame”
- $B =$ “Barbara ha superato l’esame”
- $C =$ “Carlo ha superato l’esame”

determinare le proposizioni composte che traducono le seguenti proposizioni:

(a) “Solo Carlo ha superato l’esame”

(b) “Solo Aldo non ha superato l’esame”

(c) “Solo uno tra Aldo, Barbara e Carlo ha superato l’esame”

(d) “Almeno uno tra Aldo, Barbara e Carlo ha superato l’esame”

(e) “Almeno due tra Aldo, Barbara e Carlo hanno superato l’esame”

(f) “Al più due tra Aldo, Barbara e Carlo hanno superato l’esame”

(g) “Esattamente due tra Aldo, Barbara e Carlo hanno superato l’esame”

3.5.2.9 Aldo, Barbara e Carlo sono gli unici tre membri di una commissione che vota una proposta. Ponendo:

- $A =$ “Aldo vota a favore”
- $B =$ “Barbara vota a favore”
- $C =$ “Carlo vota a favore”

determinare le proposizioni composte che traducono le seguenti proposizioni:

(a) "La votazione è stata unanime"

(b) "La proposta è passata a maggioranza"

(c) "La proposta è stata respinta, ma non all'unanimità"

3.5.2.10 Facendo riferimento all'Esempio 3.14, per ognuno dei seguenti enunciati si dica se l'enunciato è vero o falso nell'interpretazione standard, motivando la risposta:

(a) "Se il Sole ruotasse attorno alla Terra, allora Marte non apparterrebbe al nostro sistema solare"

(b) "Se la Luna ruotasse attorno alla Terra, allora il Sole sarebbe una stella"

(c) "Se la Terra ruotasse attorno al sole, allora Firenze sarebbe la capitale d'Italia"

(d) "Se la Svizzera fosse un'isola, allora il giglio sarebbe un fiore"

3.5.2.11 Sappiamo che "sono ammesse al concorso le persone che sono laureate e che hanno meno di trent'anni o hanno figli" e che:

- "Aldo non è laureato, ha ventisei anni e un figlio";
- "Barbara è laureata, ha quarant'anni e due figli";
- "Carlo è laureato, ha trentadue anni e non ha figli".

Aldo può partecipare al concorso? E Barbara? E Carlo?

3.5.2.12 Sapendo che "Il colpevole è il cuoco o la cameriera" e che "Il colpevole è l'autista o la cameriera", possiamo concludere che "Il colpevole è il cuoco o l'autista"? Motivare la risposta.

3.5.2.13 Sapendo che "O la ventola è fuori asse o il meccanismo di calibrazione è alterato" e che "Ho controllato l'allineamento della ventola ed è ok", possiamo concludere che "il meccanismo di calibrazione è fuori fase"? Motivare la risposta.

3.5.2.14 Sapendo che "Se oggi nevica, allora domani andremo a sciare" e che "Oggi nevica", possiamo concludere che "Domani andremo a sciare"? Motivare la risposta.

3.5.2.15 Sapendo che "Se oggi nevica, allora domani andremo a sciare" e che "Domani andremo a sciare", possiamo concludere che "Oggi nevica"? Motivare la risposta.

3.5.2.16 Sapendo che "Se oggi nevica, allora domani andremo a sciare" e che "Domani non andremo a sciare", possiamo concludere che "Oggi non nevica"? Motivare la risposta.

3.5.2.17 Sapendo che "Se vinco alla lotteria allora compro una macchina nuova" e che "Ho vinto alla lotteria" possiamo concludere che "Compro una macchina nuova"? Motivare la risposta.

3.5.2.18 Sapendo che "Se vinco alla lotteria allora compro una macchina nuova" e che "Non compro una macchina nuova" possiamo concludere che "Non ho vinto alla lotteria"? Motivare la risposta.

3.5.2.19 Sapendo che "Se risolvete tutti gli esercizi di queste note allora superate l'esame" e che "Superate l'esame" possiamo concludere che "Avete risolto tutti gli esercizi"? Motivare la risposta.

3.5.2.20 Sapendo che "Se risolvete tutti gli esercizi di queste note allora superate l'esame" e che "Non risolvete tutti gli esercizi" possiamo concludere che "Non superate l'esame"? Motivare la risposta.

3.5.2.21 Sapendo che "Risolvete tutti gli esercizi di queste note e superate l'esame" e che "Non risolvete tutti gli esercizi di queste note" possiamo concludere che "Non superate l'esame"? Motivare la risposta.

3.5.2.22 Sapendo che "Risolvete tutti gli esercizi per casa e superate l'esame" e che "Non risolvete tutti gli esercizi per casa" possiamo concludere che "Superate l'esame"? Motivare la risposta.

3.5.3 Esercizi che coinvolgono dimostrazioni per sostituzione

3.5.3.1 Mostrare che le seguenti formule sono tautologie usando dimostrazioni per sostituzione:

(a) $((A \wedge B) \Rightarrow (A \vee B))$
(b) $(A \Rightarrow (B \Rightarrow (A \wedge B)))$
(c) $(A \Rightarrow (\neg A \Rightarrow B))$
(d) $((A \Rightarrow B) \Leftrightarrow \neg(A \wedge \neg B))$
(e) $((A \vee B) \Leftrightarrow (\neg A \Rightarrow B))$
(f) $((A \Rightarrow B) \Rightarrow ((B \Rightarrow C) \Rightarrow (A \Rightarrow C)))$
(g) $((A \Rightarrow (B \Rightarrow C)) \Leftrightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C)))$
(h) $((A \Rightarrow C) \Rightarrow ((B \Rightarrow C) \Rightarrow ((A \vee B) \Rightarrow C)))$

3.5.3.2 Dimostrare le seguenti equivalenze logiche oppure fornire un controesempio:

(a) $((P \vee \neg Q) \equiv (\neg P \wedge Q))$
(b) $((P \vee Q) \Rightarrow (P \wedge Q)) \equiv \mathsf{T}$
(c) $(\neg P \Rightarrow (P \Rightarrow Q)) \equiv \mathsf{T}$
(d) $(P \Rightarrow (Q \Rightarrow R)) \equiv ((P \Rightarrow Q) \Rightarrow R)$
(e) $\big((P \Rightarrow (Q \Rightarrow R)) \Rightarrow \big((P \Rightarrow Q) \Rightarrow (P \Rightarrow R)\big)\big) \equiv \mathsf{T}$
(f) $\big((P \Rightarrow (Q \Rightarrow R)) \Leftrightarrow \big((P \Rightarrow Q) \Rightarrow (P \Rightarrow R)\big)\big) \equiv \mathsf{T}$

3.5.3.3 Per ognuna delle seguenti formule trovare una formula equivalente che usa solo gli operatori $\neg$ e $\wedge$:

(a) $((A \vee B) \vee C)$
(b) $(A \Rightarrow B)$
(c) $(A \Leftrightarrow B)$
(d) $(A \oplus B)$
(e) $((A \wedge (B \Rightarrow C)) \Rightarrow ((\neg C \Rightarrow (A \wedge \neg B))))$

3.5.3.4 Dire se le seguenti formule sono tautologie, contraddizioni o soddisfacibili:

(a) $((P \wedge Q) \Rightarrow (P \vee Q))$
(b) $((P \wedge Q) \Rightarrow P)$
(c) $((P \vee Q) \Rightarrow P)$
(d) $(((P \vee (Q \vee R)) \wedge (\neg P \vee \neg Q)) \wedge ((\neg P \vee \neg R) \wedge \neg(Q \wedge R)))$

3.5.3.5 [Esercizio svolto] Si dica, giustificando tutte le risposte, quali delle seguenti formule proposizionali sono equivalenti, e se sono tautologie, contraddizioni o soddisfacibili:

(a) $(P \Rightarrow Q)$
(b) $(\neg P \Rightarrow \neg Q)$
(c) $(\neg Q \Rightarrow \neg P)$

[Svolgimento] Per prima cosa, semplifichiamo le tre espressioni per confrontarle meglio:

$(P \Rightarrow Q)$

$\equiv$ { *(eliminazione dell'implicazione)* }

$(\neg P \vee Q)$

$(\neg P \Rightarrow \neg Q)$

$\equiv$ { *eliminazione dell'implicazione* }

$(\underline{\neg\neg P} \vee \neg Q)$

$\equiv$ { *doppia negazione* }

$(P \vee \neg Q)$

$(\neg Q \Rightarrow \neg P)$

$\equiv$ { *eliminazione dell'implicazione* }

$(\underline{\neg\neg Q} \vee \neg P)$

$\equiv$ { *doppia negazione* }

$(Q \vee \neg P)$

$\equiv$ { *commutatività* }

$(\neg P \vee Q)$

Quindi la prima e la terza espressione sono chiaramente equivalenti.

Per far vedere che la seconda non è equivalente alle altre due, bisogna dare un'interpretazione che la rende vera ma rende false le altre o, viceversa, che la rende falsa ma rende vere le altre.

L'unica interpretazione tale che $(P \vee \neg Q)$ *è falsa è ovviamente* $\{P \mapsto 0, Q \mapsto 1\}$. *In questo caso si ha che* $(\neg P \vee Q)$ *è vera e quindi abbiamo trovato il controesempio cercato.*

Infine è facile vedere che tutte e tre le formule sono soddisfacibili ma non sono tautologie.

3.5.3.6 Si dica, giustificando tutte le risposte, quali delle seguenti formule proposizionali sono equivalenti, e se sono tautologie, contraddizioni o soddisfacibili. (Procedere in maniera analoga a quanto visto nell'esercizio svolto visto sopra).

(a) $((P \vee Q) \Rightarrow R)$
(b) $((P \Rightarrow R) \wedge (\neg Q \Leftarrow \neg R))$
(c) $((\neg P \Leftarrow \neg R) \vee (Q \Rightarrow R))$

3.5.3.7 Si dica, giustificando tutte le risposte, quali delle seguenti formule proposizionali sono equivalenti, e se sono tautologie, contraddizioni o soddisfacibili.

(a) $(P \Rightarrow (Q \wedge R))$
(b) $((P \Rightarrow Q) \wedge (\neg R \Rightarrow \neg P))$
(c) $((Q \Rightarrow P) \vee (Q \Rightarrow R))$

3.5.3.8 Si dica, giustificando tutte le risposte, quali delle seguenti formule proposizionali sono equivalenti, e se sono tautologie, contraddizioni o soddisfacibili.

(a) $((P \Rightarrow R) \wedge \neg R)$
(b) $\neg(\neg R \Rightarrow P)$
(c) $\neg(\neg P \Rightarrow \neg R)$

3.5.3.9 Si dica, giustificando tutte le risposte, quali delle seguenti formule proposizionali sono equivalenti, e se sono tautologie, contraddizioni o soddisfacibili.

(a) $((P \Rightarrow Q) \Rightarrow R)$

(b) $((P \Rightarrow R) \wedge (Q \Rightarrow (R \wedge P)))$

(c) $((P \vee Q) \Rightarrow (R \wedge P))$

3.5.3.10 Si dica, giustificando tutte le risposte, quali delle seguenti formule proposizionali sono equivalenti, e se sono tautologie, contraddizioni o soddisfacibili.

(a) $(P \vee (Q \Rightarrow (R \wedge P)))$

(b) $(((Q \wedge \neg P) \Rightarrow R) \wedge (Q \Rightarrow P))$

(c) $(P \Rightarrow (Q \Rightarrow R))$

3.5.3.11 Si dica,giustificando le risposte, quali delle seguenti formule sono equivalenti tra loro e si determini se sono tautologie, contraddizioni o soddisfacibili:

(a) $(\neg P \Rightarrow (Q \Rightarrow R))$

(b) $((Q \wedge R) \Rightarrow P)$

(c) $(Q \Rightarrow (\neg R \Rightarrow (P \wedge \neg R)))$

Capitolo 4

Cenni di logica dei predicati

Il calcolo proposizionale introdotto nel capitolo precedente costituisce il nucleo di tutte le logiche classiche, ma ha un potere espressivo alquanto limitato. Infatti anche se consente di formalizzare in modo soddisfacente la struttura logica di proposizioni anche complesse (come inferenze e dimostrazioni) non fornisce strumenti per rappresentare gli elementi del dominio del discorso, le loro proprietà e le relazioni tra di essi. La *logica dei predicati* (o *logica del primo ordine*) arricchisce quella proposizionale con costrutti sintattici che permettono appunto di esprimere predicati su proprietà e relazioni tra specifici elementi del dominio. Inoltre, con i quantificatori, permette di esprimere che una proprietà vale per tutti gli elementi o per almeno un elemento del dominio.

In questo capitolo dopo aver motivato (Sezione 4.1) e introdotto (Sezione 4.2) la sintassi della logica dei predicati, accenneremo nella Sezione 4.3 a come deve essere arricchita la nozione di interpretazione per consentire di associare un valore di verità alle formule di questa logica, senza tuttavia presentare in modo formale il procedimento. Ci limiteremo infatti a considerare tre soli domini di interpretazione, comunque abbastanza rappresentativi: quello dei numeri naturali, quello delle persone e quello degli insiemi. Vedremo poi come questa logica permette di formalizzare in modo adeguato proposizioni ben più complesse di quelle viste nel capitolo precedente (Sezione 4.4). Infine presenteremo alcune leggi per i quantificatori nella Sezione 4.5, mostrando anche per questa logica come le dimostrazioni per sostituzione possono essere utilizzate per mostrare l'equivalenza logica di formule.

4.1 Sull'espressività della logica dei predicati

L'espressività del calcolo proposizionale è abbastanza limitata: nel capitolo precedente siamo stati attenti a scegliere esempi in cui queste limitazioni non emergessero.

Per esempio, pensiamo di voler formalizzare un enunciato che parla di persone, come *"Se Anna è la mamma di Bruno e Bruno ha figli, allora Anna è nonna"*. Usando la tecnica discussa nella Sezione 3.3 dobbiamo introdurre un simbolo per ogni proposizione elementare, per esempio A per *"Anna è la mamma di Bruno"*, B per *"Bruno ha figli"* e C per *"Anna è nonna"*. La formula proposizionale risultante sarebbe $((A \wedge B) \Rightarrow C)$: essa evidenzia correttamente la struttura logica (la congiunzione e l'implicazione) ma poichè le persone coinvolte non hanno una rappresentazione esplicita, la formula non permette di capire che Anna è coinvolta sia nella premessa A che nella conseguenza C dell'implicazione, e che entrambe le premesse A e B parlano di Bruno. Se poi consideriamo la frase *"Maria è la mamma di Giulia"*, questa è una proposizione elementare e quindi dobbiamo rappresentarla con un nuovo simbolo: non abbiamo la possibilità di mettere in evidenza che essa esprime la stessa relazione tra persone della proposizione rappresentata sopra da A.

Quest'analisi rende evidente che, in situazioni molto frequenti, vorremmo poter rappresentare nella sintassi delle formule: (1) le persone coinvolte, (2) le proprietà delle persone (*"aver figli"*, *"essere nonna"*) e (3) le relazioni tra persone (*"essere mamma di"*).

La logica dei predicati permette, grazie a una sintassi più ricca di quella proposizionale, di rappresentare esplicitamente queste entità. Infatti, come vedremo, possiamo formalizzare le frasi viste sopra come

$$((mamma(Anna, Bruno) \wedge haFigli(Bruno)) \Rightarrow èNonna(Anna)) \qquad \text{e} \qquad mamma(Maria, Giulia)$$

in modo di gran lunga più espressivo che con le formule proposizionali.

Naturalmente poter parlare di "persone" è solo un caso particolare: potremmo voler esprimere proprietà e/o relazioni su numeri (*"7 è un numero primo"*, *"6 è il doppio di 3"*), su frutti (*"questa mela è rossa"*), su animali (*"Fido è un bassotto"*), o anche su elementi di tipologie diverse (*"se Fido è il cane di Giorgio allora mangia una mela rossa"*). In generale nella logica dei predicati possiamo rappresentare (con delle *costanti*) gli *elementi* appartenenti a un certo insieme (*dominio*). Di questi elementi possiamo rappresentare delle proprietà e delle relazioni tra essi (con dei *simboli di predicato*).

Negli esempi presentati sopra, abbiamo usato le costanti *"Anna"*, *"Bruno"*, *"Maria"* e *"Giulia"*, i simboli di predicato con un solo argomento (detti *unari*) *"haFigli"* ed *"èNonna"* e il simbolo di predicato a due argomenti (detto *binario*) *"mamma"*.

4.1.1 Quantificazione esistenziale e universale

La possibilità di riferire specifici elementi del dominio di interesse in una formula è solo una premessa necessaria per introdurre i *quantificatori*, l'ingrediente più caratterizzante della sintassi della logica dei predicati.

Nella lingua italiana usiamo comunemente pronomi o aggettivi indefiniti che indicano cose o persone senza specificarne con precisione la quantità, come *"tutti"*, *"qualche"*, *"alcuni"*, *"ogni"*, *"nessuno"*, ecc. Per esempio, parlando di persone, possiamo dire *"tutti gli uomini sono mortali"*, *"nessuno pesa più di 100 chili"*, *"qualcuno è più alto di suo padre"*. Esaminiamone il significato:

- *Tutti* (e sinonimi): permette di asserire che una proprietà vale per tutti gli elementi del dominio o *"universo"*, nessuno escluso. Esprime quindi una *quantificazione universale*.
- *Alcuni* (e sinonimi): permette di affermare che una proprietà vale per uno o più elementi del dominio. Non dice né quanti né quali, ma garantisce l'esistenza di almeno un elemento che la soddisfa. Esprime quindi una *quantificazione esistenziale*.
- *Nessuno* (e sinonimi): permette di asserire che una proprietà non vale per alcun elemento del dominio. Attenzione, è l'opposto di *alcuni*, non è l'opposto di *tutti*! Equivale a dire *tutti ... non ...* e quindi quantifica in maniera universale la negazione di un'enunciato.

La logica dei predicati permette di rappresentare esplicitamente le quantificazioni usando le *variabili* e i *quantificatori*.

Le variabili, di solito chiamate $x, y, z, \ldots$, rappresentano generici elementi del dominio e quindi permettono di rappresentare enunciati parametrici che assumono un valore di verità che dipende da quali elementi vengono sostituiti alle variabili. Per esempio, parlando dei naturali, possiamo scrivere l'enunciato *"x è un numero primo"*, che possiamo rappresentare con la formula della logica dei predicati $primo(x)$. Chiaramente la verità di questa formula dipende da quale elemento sostituiamo a x: $primo(5)$ è vero, mentre $primo(12)$ è falso.

I quantificatori servono per descrivere in che modo una variabile che compare in una formula deve essere sostituita da elementi del dominio, per verificare se l'intera formula è vera o falsa. Essi hanno la seguente forma, dove in generale la formula A contiene una o più occorrenze della variabile x:

Quantificazione esistenziale: $(\exists x\,.\,A)$, che si legge *"esiste un x tale che A vale"*

Quantificazione universale: $(\forall x\,.\,A)$, che si legge *"per ogni x vale A"*

Per esempio, considerando il dominio dei numeri naturali, $(\exists x\,.\,primo(x))$ si legge *"esiste un x tale che* $primo(x)$ *vale"*, e cioè *"esiste un numero naturale che è primo"*. Si noti che mentre $primo(x)$ essendo una formula generica non ha un valore di verità, $(\exists x\,.\,primo(x))$ lo ha: esso vale "vero" *se esiste almeno un elemento nel dominio che sostituito a x rende la formula* $primo(x)$ *vera*. Quindi $(\exists x\,.\,primo(x))$ è vera.

Invece $(\forall x\,.\,primo(x))$ si legge *"per ogni x vale* $primo(x)$*"*, cioè *"ogni numero naturale è primo"*. Quindi $(\forall x\,.\,primo(x))$ è vera se *ogni elemento d del dominio, se sostituito a x, rende la formula* $primo(x)$ *vera*. Poichè ci sono numeri naturali che non sono primi, la formula è falsa (basta considerare la sostituzione di x con 1).

4.2 La sintassi delle formule predicative

La sintassi delle formule proposizionali presentata nella Definizione 3.4 è parametrica rispetto a un insieme di *simboli proposizionali* che, come abbiamo visto, ci servono per rappresentare le proposizioni elementari

del dominio del discorso. Anche per la logica dei predicati la sintassi delle formule è parametrica: useremo simboli di costanti, di predicati e di funzioni presi da un alfabeto fissato a priori. Questi simboli non hanno un significato specifico: quando valuteremo le formule per vedere se sono vere o false su di un *dominio di interpretazione*, dovremo dire qual è il significato di questi simboli.

DEFINIZIONE 4.1 (ALFABETO DEL PRIMO ORDINE)
*Un **alfabeto** del primo ordine $\mathcal{A} = (\mathcal{C}, \mathcal{F}, \mathcal{P}, \mathcal{V})$ è costituito da quattro insiemi:*

1. $\mathcal{C} = \{c, d, ...\}$ *insieme delle **costanti** (per esempio a, b, ..., 0, 1, ..., Mario, Giulia, ...)*
2. $\mathcal{F} = \{f, g, ...\}$ *insieme dei **simboli di funzione**, ognuno con un numero di argomenti fissato (chiamato **arietà**) (per esempio $f(\_,\_,\_)$, $succ(\_)$, $\_ + \_$, $padre(\_)$, ...)*[1]
3. $\mathcal{P} = \{P, Q, ...\}$ *insieme dei **simboli di predicato**, ognuno con la sua arietà (per esempio $p(\_,\_,\_)$, $\_ \leq \_$, $\_ = \_$, $fratello(\_,\_)$, ...)*
4. $\mathcal{V} = \{x, y, ...\}$ *insieme dei **simboli di variabile** (per esempio x, y, n, m, ...)*

DEFINIZIONE 4.2 (TERMINI)
*Fissato un alfabeto $\mathcal{A}$, un **termine** è un'espressione ben formata*[2] *costruita con costanti, variabili e simboli di funzione.*

Si noti che nei termini non compaiono i simboli di predicato, che invece servono a costruire le *formule*.

DEFINIZIONE 4.3 (FORMULE PREDICATIVE)
*Le **formule predicative** (o semplicemente **formule**) sono tutte e sole le espressioni ottenibili mediante le seguenti regole:*

1. T *e* F *sono formule*
2. *se un simbolo di predicato $P \in \mathcal{P}$ ha n argomenti e t_1, t_2, ..., t_n sono termini allora $P(t_1, t_2, ..., t_n)$ è una formula; le formule di questo tipo sono dette **atomiche***
3. *se A_1 e A_2 sono formule allora $\neg A_1$ e $(A_1 \,\mathsf{op}\, A_2)$ sono formule (dove $\mathsf{op} \in \{\wedge, \vee, \oplus, \Rightarrow, \Leftrightarrow\}$ è un qualsiasi connettivo logico binario)*
4. *se A è una formula e $x \in \mathcal{V}$ è una variabile, allora anche $(\forall x.A)$ e $(\exists x.A)$ sono formule*

Si noti che quando un simbolo $P \in \mathcal{P}$ ha 0 argomenti, esso è anche una formula atomica (non deve essere applicato ad argomenti): può essere considerato come un simbolo proposizionale ordinario. Poiché poi si possono costruire formule predicative usando i connettivi logici binari e la negazione, ne segue che tutte le formule del calcolo proposizionale sono anche formule predicative.

Come già anticipato, nel resto del capitolo per semplificare la presentazione useremo un numero limitato di domini: quello dei numeri naturali, quello delle persone, e quello degli insiemi. Per ognuno di essi introduciamo un alfabeto contenente dei simboli che, avendo nomi che suggeriscono un preciso significato, ci renderanno le formule più facili da leggere. Tuttavia da un punto di vista formale è importante ricordare che tali simboli non hanno automaticamente un significato: questo gli viene attribuito successivamente con un'interpretazione (Definizione 4.5). Per esempio, del simbolo di funzione $\_ + \_$ possiamo dire che è binario e infisso, ma solo quando ne forniamo l'interpretazione potremo dire che esso rappresenta l'addizione tra naturali, come atteso, e non un'altra operazione.

DEFINIZIONE 4.4 (ALCUNI ALFABETI DEL PRIMO ORDINE)
*L'**alfabeto dei naturali** $\mathcal{A}_{\mathbb{N}} = (\mathcal{C}_{\mathbb{N}}, \mathcal{F}_{\mathbb{N}}, \mathcal{P}_{\mathbb{N}}, \mathcal{V}_{\mathbb{N}})$ è costituito dai seguenti insiemi (i puntini sospensivi ci permetteranno eventualmente di aggiungere altri simboli nel seguito):*

- *le costanti $\mathcal{C}_{\mathbb{N}} = \mathbb{N} = \{0, 1, 2, ...\}$*

[1] Usiamo un "$\_$" per ogni argomento del simbolo di funzione. Quindi per esempio $f(\_,\_,\_)$ significa che f ha tre argomenti (arietà tre), mentre $\_ + \_$ significa che $+$ ha arietà due ed è infisso, cioè si scrive tra i due argomenti.

[2] Cioè se un simbolo di funzione ha arietà n, allora deve essere applicato a n termini.

- *i simboli di funzione* $\mathcal{F}_{\mathbb{N}} = \{succ(\_), \_+\_, \_\times\_, \_/\_, \_\%\_, \ldots\}$
- *i simboli di predicato* $\mathcal{P}_{\mathbb{N}} = \{\_\leq\_, \_\geq\_, \_<\_, \_>\_, \_=\_, primo(\_), pari(\_), \ldots\}$
- *le variabili* $\mathcal{V}_{\mathbb{N}} = \{x, y, \ldots, n, m, \ldots\}$.

*L'***alfabeto delle persone** $\mathcal{A}_{\mathcal{P}} = (\mathcal{C}_{\mathcal{P}}, \mathcal{F}_{\mathcal{P}}, \mathcal{P}_{\mathcal{P}}, \mathcal{V}_{\mathcal{P}})$ *è costituito dai seguenti insiemi:*

- *le costanti* $\mathcal{C}_{\mathcal{P}} = \{Aldo, Bruna, io, Barak\ Obama, \ldots\}$
- *i simboli di funzione* $\mathcal{F}_{\mathcal{P}} = \{padre(\_), nonnoMaterno(\_), \ldots\}$
- *i simboli di predicato* $\mathcal{P}_{\mathcal{P}} = \{padre(\_,\_), nonno(\_,\_), figlio(\_,\_), fratelli(\_,\_), \ldots\}$
- *le variabili* $\mathcal{V}_{\mathcal{P}} = \{x, y, \ldots, p, q, \ldots\}$.

*L'***alfabeto degli insiemi** $\mathcal{A}_{\mathcal{S}} = (\mathcal{C}_{\mathcal{S}}, \mathcal{F}_{\mathcal{S}}, \mathcal{P}_{\mathcal{S}}, \mathcal{V}_{\mathcal{S}})$ *è costituito dai seguenti insiemi:*

- *le costanti* $\mathcal{C}_{\mathcal{S}} = \mathbb{N} = \{\varnothing, \mathbb{N}, \mathbb{Z}, \mathbb{N}^+, \ldots, 0, 1, 2 \ldots\}$
- *i simboli di funzione* $\mathcal{F}_{\mathcal{S}} = \{\_\cup\_, \_\cap\_, \_\setminus\_, \bar{\_}\ldots\}$
- *i simboli di predicato* $\mathcal{P}_{\mathcal{S}} = \{isSet(\_), vuoto(\_), \_\in\_, \_\subset\_, \_\subseteq\_, \_\supset\_, \_\supseteq\_, \_=\_, \ldots\}$.
- *le variabili* $\mathcal{V}_{\mathcal{S}} = \{x, y, \ldots, X, Y, \ldots\}$*: useremo le variabili maiuscole per gli insiemi, le minuscole per gli elementi.*

ESEMPIO 4.1 (SINTASSI DI TERMINI E FORMULE)
Si consideri l'alfabeto dei naturali $\mathcal{A}_{\mathbb{N}}$*. Le seguenti espressioni sono sintatticamente corrette, ovvero possono essere ricavate seguendo le regole della Definizione 4.3:*

- 0, 5, 21934, x, n *[sono costanti o variabili, quindi sono* termini*]*
- $3+5$, $succ(x+3)$, $(3+5)\times 0$ *[sono simboli di funzione applicati a un numero di termini pari alla propria arietà, quindi sono* termini*]*
- $x \leq 6$, $pari(42)$, $primo(3\times(5+x))$, $4+x=4-y$ *[sono simboli di predicati applicati a un numero di termini pari alla propria arietà, quindi sono* formule atomiche*]*
- $(x \leq 6 \wedge pari(x))$, (primo(x) $\Rightarrow x>0$), $(\forall x\,.\,x\geq 0)$, $(x>0 \Rightarrow (\exists y\,.\,y<x))$ *[sono connettivi logici oppure quantificatori applicati a formule, quindi sono* formule*]*

Invece le seguenti espressioni non sono sintatticamente corrette, quindi non hanno alcun significato:

- $12+$ *["+" è un simbolo di funzione binario, non può essere applicato a un solo argomento]*
- $(x \leq y) \leq z$ *[il secondo simbolo di predicato "*$\leq$*" è applicato a una formula atomica e a un termine invece che a due termini; questa espressione, sintatticamente non corretta, viene spesso usata come abbreviazione della formula* $(x \leq y) \wedge (y \leq z)$*]*
- $(\forall x\,.\,x+y)$ *[l'espressione quantificata non è una formula ma un termine]*

4.3 Interpretazioni e semantica delle formule predicative

Vediamo ora come determinare la semantica, cioè il valore di verità, di formule predicative su un certo alfabeto del primo ordine. La prima osservazione è che non tutte tali formule possono avere una semantica ben definita. Per esempio, interpretando in modo ovvio il simbolo di predicato $\leq$ come la relazione "minore o uguale" sui naturali, la formula $x \leq 0$ non ha un valore di verità ben determinato: essa vale T se sostituiamo x con 0, e F se sostituiamo x con un qualunque altro naturale. Invece la semantica delle formule $(\exists x\,.\,x \leq 0)$ e $(\forall x\,.\,x \leq 0)$ è ben definita, perché le quantificazioni $\forall x$ e $\exists x$ indicano come deve essere sostituita x per determinare il valore di verità: $(\exists x\,.\,x \leq 0)$ vale T perché c'è almeno un naturale minore o uguale a 0, mentre $(\forall x\,.\,x \leq 0)$ vale F perché non tutti i naturali sono minori o uguali a 0.

Chiameremo una formula come $(\forall x\,.\,x \leq 0)$ *chiusa* perché ogni variabile (in questo caso solo la x) compare nel *campo d'azione* (o *portata* o *scope*) di un quantificatore per la stessa variabile. Il **campo d'azione** della quantificazione $\forall x$ nella formula $(\forall x\,.\,A)$ è l'intera formula A, e analogamente per la quantificazione esistenziale. Nella formula $(\forall x\,.\,A)$, ogni occorrenza di x dentro A viene detta *legata*.

Invece una formula come $x \leq 0$ viene detta *aperta* perché contiene una variabile, la x, che compare nella formula senza essere legata a un corrispondente quantificatore. Una variabile che non è legata a un quantificatore viene detta *libera*.

ESEMPIO 4.2 (CAMPO D'AZIONE, FORMULE APERTE E CHIUSE)
Nella formula seguente le parentesi graffe mostrano il campo d'azione dei due quantificatori. La formula è chiusa perché ogni variabile (le due x e la y) compare nel campo d'azione di un corrispondente quantificatore.

$$(\forall x\,.\,\overbrace{x \leq 0 \Rightarrow (\forall y\,.\,\underbrace{y \geq x}_{\forall y})}^{\forall x})$$

Invece la formula che segue è aperta, perché la seconda x non è nel campo di azione di un $\forall x$ o $\exists x$.

$$(\forall x\,.\,\underbrace{x > 0}_{\forall x}) \Rightarrow (\exists y\,.\,\underbrace{y < \overbrace{x}^{\textit{libera}}}_{\exists y})$$

Per quanto detto sopra considereremo solo la semantica di *formule predicative chiuse*. Data una formula chiusa su un certo alfabeto $\mathcal{A}$, per assegnarle un valore di verità dobbiamo fissare il significato dei simboli di costante, di funzione e di predicato che compaiono in essa, esattamente come per una formula proposizionale dovevamo fissare un valore di verità per ogni simbolo proposizionale. Per far questo fisseremo un *dominio di interpretazione*, cioè un insieme, e un'interpretazione delle costanti come elementi del dominio, e dei simboli di funzione e di predicato come opportune funzioni o relazioni sul dominio.

Quindi il concetto di interpretazione, già visto nel caso più semplice del calcolo proposizionale, viene arricchito nel modo seguente.

DEFINIZIONE 4.5 (INTERPRETAZIONE PER ALFABETO DEL PRIMO ORDINE)
*Un'**interpretazione** I per un alfabeto del primo ordine $\mathcal{A} = (\mathcal{C}, \mathcal{F}, \mathcal{P}, \mathcal{V})$ è una coppia $(\mathcal{D}_I, \alpha_I)$ dove $\mathcal{D}_I$ è il **dominio (di interpretazione)** (un insieme di valori), mentre α_I è un'**associazione** che assegna:*

- *a ogni simbolo di costante $\mathsf{c} \in \mathcal{C}$ un elemento $\alpha_I(\mathsf{c}) \in \mathcal{D}_I$ (talvolta scritto più semplicemente c^I)*
- *a ogni simbolo di funzione $f \in \mathcal{F}$ di arietà n una funzione $\alpha_I(f) : \mathcal{D}_I^n \to \mathcal{D}_I$, cioè un'operazione che presi n valori di $\mathcal{D}_I$ restituisce come risultato un altro valore di $\mathcal{D}_I$ (spesso scriveremo f^I per $\alpha_I(f)$)*
- *a ogni simbolo di predicato $P \in \mathcal{P}$ di arietà n (cioè con n argomenti) una funzione $\alpha_I(P) : \mathcal{D}_I^n \to \{0,1\}$, cioè un'operazione che presi n valori di $\mathcal{D}_I$ restituisce vero o falso[3] (spesso scriveremo P^I per $\alpha_I(P)$)*

Una volta fissata un'interpretazione per un alfabeto $\mathcal{A}$ possiamo utilizzarla per associare un valore di verità (la semantica) a ogni formula chiusa scritta con simboli in $\mathcal{A}$.

[3] Ricordiamo che una funzione n-aria $f : X^n \to \{0,1\}$ è anche chiamata una *relazione n-aria* sull'insieme X.

Ma prima di vedere come si fa, introduciamo le interpretazioni per i tre alfabeti della Definizione 4.4, in modo da poter poi presentare degli esempi. Queste sono le interpretazioni standard che ci aspettiamo, tuttavia necessarie per collegare le entità sintattiche (i simboli degli alfabeti) con la corrispondente semantica definita sul dominio di interpretazione.

DEFINIZIONE 4.6 (ESEMPI DI INTERPRETAZIONI)

- *L'*interpretazione (standard) *per l'alfabeto dei naturali* $\mathcal{A}_{\mathbb{N}} = (\mathcal{C}_{\mathbb{N}}, \mathcal{F}_{\mathbb{N}}, \mathcal{P}_{\mathbb{N}}, \mathcal{V}_{\mathbb{N}})$ *(Definizione 4.4) è la coppia* $I_{\mathbb{N}} = (\mathcal{D}_{I_{\mathbb{N}}}, \alpha_{I_{\mathbb{N}}})$ *dove il dominio* $\mathcal{D}_{I_{\mathbb{N}}}$ *è costituito dall'insieme dei naturali* $\mathbb{N}$*, mentre* $\alpha_{I_{\mathbb{N}}}$ *assegna:*
  - *a ogni costante* $\mathsf{c} \in \mathcal{C}_{\mathbb{N}} = \mathbb{N}$ *se stessa, vista come elemento del dominio;*
  - *a ogni simbolo di funzione in* $\mathcal{F}_{\mathbb{N}}$ *la corrispondente funzione sui naturali; per esempio* $succ^{I_{\mathbb{N}}}$ *è la funzione* successore*, che mappa ogni numero* x *su* $x+1$*;* $+^{I_{\mathbb{N}}}$ *è l'addizione su naturali:* $/^{I_{\mathbb{N}}}$ *è la divisione intera (es.* $10/^{I_{\mathbb{N}}}3 = 3$*); e* $\%^{I_{\mathbb{N}}}$ *è il resto della divisione intera (es.* $10\%^{I_{\mathbb{N}}}3 = 1$*);*
  - *a ogni simbolo di predicato in* $\mathcal{P}_{\mathbb{N}}$ *la corrispondente relazione sui naturali di uguale arietà, per esempio per tutti i naturali* $n,m \in \mathbb{N}$*,* $n \leq^{I_{\mathbb{N}}} m = 1$ *se e solo se* n *è minore o uguale a* m*; mentre* $primo^{I_{\mathbb{N}}}(n) \equiv 1$ *se e solo se* n *è un numero primo.*
- *L'interpretazione (standard)* $I_{\mathcal{P}}$ *dell'alfabeto delle persone* $\mathcal{A}_{\mathcal{P}} = (\mathcal{C}_{\mathcal{P}}, \mathcal{F}_{\mathcal{P}}, \mathcal{P}_{\mathcal{P}}, \mathcal{V}_{\mathcal{P}})$ *ha come dominio appunto l'insieme di tutte le persone. Le costanti e i simboli di funzione e di predicato sono associati nel modo ovvio a persone e a funzioni o relazioni definite su persone. Per esempio,* $Aldo^{I_{\mathcal{P}}}$ *è una determinata persona di nome Aldo;* $(Barack\ Obama)^{I_{\mathcal{P}}}$ *è un politico americano, attualmente Presidente degli USA;* $padre^{I_{\mathcal{P}}}$ *è la funzione che associa ogni persona al suo padre naturale; e* $fratelli^{I_{\mathcal{P}}}(p,q)$ *è vera se e solo se le persone* p *e* q *sono fratelli.*
- *Infine l'interpretazione (standard) dell'alfabeto degli insiemi ha come dominio un insieme che ha come elementi sia gli insiemi di nostro interesse (come* $\mathbb{N}$*,* $\mathbb{Z}$*, ecc.) che i loro elementi. Le costanti e i simboli di funzione e di predicato elencati nella Definizione 4.4 sono associati in modo ovvio rispettando la usuale notazione matematica.*

4.3.1 Semantica di formule chiuse

Vediamo ora come si può valutare la semantica di una formula predicativa chiusa rispetto a una data interpretazione. Come primo passo, osserviamo che data un'interpretazione $I = (\mathcal{D}_I, \alpha_I)$ possiamo associare, in maniera univoca, ogni termine chiuso (cioè senza variabili) t con un particolare elemento $[\![t]\!]^I$ del dominio usando le seguenti regole:

(R1) se t è una costante $\mathsf{c} \in \mathcal{C}$ allora $[\![t]\!]^I = \mathsf{c}^I$;

(R2) se invece t è della forma $f(t_1,...,t_n)$ e sappiamo che $[\![t_1]\!]^I = v_1$, ..., $[\![t_n]\!]^I = v_n$ allora $[\![t]\!]^I = f^I(v_1,...,v_n)$.

ESEMPIO 4.3 (DA TERMINI A ELEMENTI DEL DOMINIO)
Consideriamo l'alfabeto dei naturali $\mathcal{A}_{\mathbb{N}}$*. Esempi di termini chiusi sono* 5*,* $7+4$*, e* $succ((3\times 4)/5)$*. I corrispondenti valori del dominio rispetto all'interpretazione standard* $I_{\mathbb{N}}$ *sono*

- $[\![5]\!]^{I_{\mathbb{N}}} = 5^{I_{\mathbb{N}}} = 5$
- $[\![7+4]\!]^{I_{\mathbb{N}}} = [\![7]\!]^{I_{\mathbb{N}}} +^{I_{\mathbb{N}}} [\![4]\!]^{I_{\mathbb{N}}} = 7^{I_{\mathbb{N}}} +^{I_{\mathbb{N}}} 4^{I_{\mathbb{N}}} = 7 +^{I_{\mathbb{N}}} 4 = 11$
- $[\![succ((3\times 4)/5)]\!]^{I_{\mathbb{N}}} = 3$.

A questo punto siamo in grado di associare un valore di verità alle formule atomiche chiuse. Scriveremo $I \models A$ se la formula A è vera rispetto ad I, altrimenti $I \not\models A$. Data un'interpretazione $I = (\mathcal{D}_I, \alpha_I)$ e una formula atomica chiusa $P(t_1,...,t_n)$ con $[\![t_1]\!]^I = v_1$, ..., $[\![t_n]\!]^I = v_n$ diciamo che:

(S1) $I \models P(t_1,...,t_n)$ se e solo se $P^I(v_1,...,v_n) = 1$.

(S1 bis) (quindi $I \not\models P(t_1,...,t_n)$ se e solo se $P^I(v_1,...,v_n) = 0$).

ESEMPIO 4.4 (SEMANTICA DI FORMULE ATOMICHE)
Assumendo l'interpretazione standard dei naturali $I_{\mathbb{N}}$, possiamo valutare la semantica di alcune formule atomiche sui naturali come $0 \leq 1$, $1 \leq 0$, e $primo(7)$.

- *Vediamo che $I_{\mathbb{N}} \models 0 \leq 1$.*
  Infatti $I_{\mathbb{N}} \models 0 \leq 1$ se e solo se $[\![0]\!]^{I_{\mathbb{N}}} \leq^{I_{\mathbb{N}}} [\![1]\!]^{I_{\mathbb{N}}}$ se e solo se $0 \leq^{I_{\mathbb{N}}} 1$, e questo è vero perché $\leq^{I_{\mathbb{N}}}$ è la relazione di minore o uguale sui naturali. Analogamente si vede che $I_{\mathbb{N}} \not\models 1 \leq 0$.
- *Abbiamo $I_{\mathbb{N}} \models primo(7)$. Infatti $primo^{I_{\mathbb{N}}}([\![7]\!]^{I_{\mathbb{N}}}) = primo^{I_{\mathbb{N}}}(7) = 1$, poiché 7 è un numero primo.*

Ci resta da vedere come valutare la semantica di formule chiuse non atomiche. Per le formule ottenute con connettivi logici e negazione il valore si ottiene come nel caso del calcolo proposizionale, valutando prima le sottoformule e poi applicando le tabelle di verità dei connettivi (si veda la Sezione 3.2). Per esempio, $I \models (A \wedge B)$ se e solo se $I \models A$ e $I \models B$.

Ci rimane da considerare le formule ottenute con i quantificatori. Per valutare una formula chiusa del tipo $(\forall x.A)$ (oppure $(\exists x.A)$) non sempre è possibile valutare prima A perché potrebbe contenere occorrenze di x legate al quantificatore in questione e quindi libere in A (che risulterebbe una formula aperta). Per esempio, per valutare la formula $(\forall x.primo(x))$ nell'interpretazione standard dei naturali non possiamo valutare direttamente $primo(x)$ perché è una formula aperta.

Per procedere dobbiamo prima introdurre il concetto di *sostituzione*, che ci servirà per istanziare le occorrenze libere di x in A con opportuni valori del dominio.

DEFINIZIONE 4.7 (SOSTITUZIONE)
*La **sostituzione** di una variabile x con t in un'espressione E (che può essere un termine o una formula) è l'espressione $E\{x \mapsto t\}$, ottenuta rimpiazzando in E tutte le occorrenze libere della variabile x con t.*

L'uso corretto delle sostituzioni richiede una certa attenzione perché la stessa variabile potrebbe comparire nella formula in più di una quantificazione. Un altro problema può essere dato dalla presenza di variabili nell'espressione E che dopo la sostituzione potrebbero in parte risultare legate a quantificatori e in parte no. Per semplicità ignoreremo questi problemi, evitando di considerare formule e sostituzioni che siano problematiche da questo punto di vista.

Possiamo ora descrivere la semantica delle formule quantificate. Data un'interpretazione $I = (\mathcal{D}_I, \alpha_I)$ e una formula quantificata chiusa si ha che

(S2) $I \models (\forall x.A)$ se e solo se $I \models A\{x \mapsto v\}$ per ogni $v \in \mathcal{D}_I$.

(S3) $I \models (\exists x.A)$ se e solo se $I \models A\{x \mapsto v\}$ per almeno un elemento $v \in \mathcal{D}_I$.

ESEMPIO 4.5 (SEMANTICA DI FORMULE CON QUANTIFICATORI)
Vediamo quali delle seguenti formule sono vere rispetto all'interpretazione standard dei naturali $I_{\mathbb{N}}$.

1. *$(\forall x.(0 \leq 1))$: è banalmente vera in $I_{\mathbb{N}}$, visto che x non compare nella formula $(0 \leq 1)$ e $I_{\mathbb{N}} \models (0 \leq 1)$.*
2. *$(\forall x.(x \leq 1))$: non è vera in $I_{\mathbb{N}}$ perché, per esempio, considerando la sostituzione $\{x \mapsto 2\}$ abbiamo $(x \leq 1)\{x \mapsto 2\} = (2 \leq 1)$, e chiaramente $I_{\mathbb{N}} \not\models (2 \leq 1)$)*
3. *$(\exists x.(x \leq 1))$: è vera in $I_{\mathbb{N}}$ perché per la sostituzione $\{x \mapsto 1\}$ vale $I_{\mathbb{N}} \models (x \leq 1)\{x \mapsto 1\}$.*
4. *$(\exists x.(1 \leq x \wedge pari(x)))$: Per la regola **(S3)**, dobbiamo trovare un valore $n \in \mathbb{N}$ tale che*

$$I_{\mathbb{N}} \models (1 \leq n \wedge pari(n))$$

Per il significato della congiunzione, n deve essere tale da soddisfare sia $I_{\mathbb{N}} \models 1 \leq n$ che $I_{\mathbb{N}} \models pari(n)$.

Procediamo per tentativi:

- *per $n = 0$ si ha che $I_{\mathbb{N}} \not\models 1 \leq 0$, quindi dobbiamo tentare con un altro valore;*
- *per $n = 1$ si ha che $I_{\mathbb{N}} \models 1 \leq 1$ ma $I_{\mathbb{N}} \not\models pari(1)$, quindi non va bene;*
- *per $n = 2$ si ha che $I_{\mathbb{N}} \models 1 \leq 2$ e anche $I_{\mathbb{N}} \models pari(2)$, e quindi abbiamo finito: la formula esistenziale è vera rispetto a $I_{\mathbb{N}}$.*

4.4 Formalizzazione di frasi

Con la logica predicativa siamo in grado di formalizzare molte frasi in maniera più espressiva di quanto fosse possibile con il calcolo proposizionale. Vediamo alcuni esempi, basati sugli alfabeti degli interi e delle persone.

1. *"Esiste un numero che è sia pari che primo"*
   Ovviamente rappresentiamo *"Esiste"* con una quantificazione esistenziale, e sfruttiamo i simboli di predicato $primo(\_)$ e $pari(\_)$. La formula risultante è

   $$(\exists x\,.\,(pari(x) \wedge primo(x)))$$

2. *"Tutti gli uomini sono mortali"*
   Estendiamo l'alfabeto $\mathcal{A}_{\mathcal{P}}$ con il simbolo di predicato $mortale(\_)$, e l'interpretazione standard $I_{\mathcal{P}}$ in modo da associare a *mortale* la funzione

   $$mortale^{I_{\mathcal{P}}}(p) = 1 \text{ se e solo se } p \text{ è mortale}$$

   Inoltre rappresentiamo *"Tutti"* con una quantificazione universale. La formula risultante è:

   $$(\forall x\,.\,mortale(x))$$

3. *"Tutti i numeri naturali dispari sono maggiori di zero"*
   In questo caso la quantificazione universale non è su tutti i naturali, ma è ristretta a un sottoinsieme: i naturali dispari. Un modo naturale di formalizzarla è di riconoscere che c'è un'implicazione implicita: *"Per ogni naturale vale che se è dispari allora è maggiore di zero"*. La formula risultante è

   $$(\forall x\,.\,(dispari(x) \Rightarrow (x > 0))$$

4. *"Esiste un numero naturale dispari che è minore o uguale a zero"*
   Anche qui la quantificazione è ristretta ai numeri dispari, ma è una quantificazione esistenziale e possiamo leggerla come *"Esiste un numero che è dispari ed è minore o uguale a zero"*. Quindi può essere formalizzata con

   $$(\exists x\,.\,(dispari(x) \wedge (x \leq 0))) \tag{4.1}$$

   Si noti che l'uso di un'implicazione (come nel caso precedente) sarebbe errata: la formula

   $$(\exists x\,.\,(dispari(x) \Rightarrow (x \leq 0))) \tag{4.2}$$

   ha un significato diverso. Infatti la formula (4.1) è falsa nell'interpretazione standard sui naturali (così come è falso l'enunciato originale), mentre la formula (4.2) è vera, poiché il numero 34 (e qualunque altro numero pari) soddisfa $(dispari(34) \Rightarrow (34 \leq 0))$.

5. *"Ogni persona in questa classe ha un amico che parla inglese o francese"*
   Estendiamo l'alfabeto delle persone con i simboli di predicato unari *questaClasse*, *parlaENG* e *parlaFR* e con il simbolo di predicato binario *amico*, con la seguente interpretazione:

   - $questaClasse^{I_{\mathcal{P}}}(p) = 1$ se e solo se la persona p appartiene a questa classe
   - $parlaENG^{I_{\mathcal{P}}}(p) = 1$ se e solo se la persona p parla inglese
   - $parlaFR^{I_{\mathcal{P}}}(p) = 1$ se e solo se la persona p parla francese
   - $amico^{I_{\mathcal{P}}}(p,q) = 1$ se e solo se le persone p e q sono amiche.

   Quella che segue è una possibile formalizzazione della frase:

   $$(\forall x\,.\,(questaClasse(x) \Rightarrow (\exists y\,.\,(amico(x,y) \wedge (parlaENG(y) \vee parlaFR(y))))))$$

   Abbiamo usato di nuovo un'implicazione per restringere la quantificazione universale a un sottoinsieme delle persone. Che cosa succede se spostiamo la quantificazione esistenziale fuori dall'implicazione?

   $$(\forall x\,.\,(\exists y\,.\,(questaClasse(x) \Rightarrow (amico(x,y) \wedge (parlaENG(y) \vee parlaFR(y))))))$$

Il significato è rimasto invariato. E se scambiamo l'ordine dei quantificatori?

$$(\exists y\,.\,(\forall x\,.\,(questaClasse(x) \Rightarrow (amico(x,y) \wedge (parlaENG(y) \vee parlaFR(y))))))$$

Adesso invece la formula ha un significato diverso.

6. *"Ogni persona felice ha un solo amico del cuore"*
   Estendiamo l'alfabeto delle persone con i simboli di predicato $felice(\_)$ e $amiciDelCuore(\_,\_)$ con l'ovvia interpretazione. Come primo tentativo, proviamo a formalizzare la frase così:

$$(\forall x\,.\,(\exists y\,.\,(felice(x) \Rightarrow amiciDelCuore(x,y))))$$

   Tuttavia questa formula non coglie il concetto di *unicità*! La seguente formula invece lo cattura in modo corretto:

$$(\forall x\,.\,(\exists y\,.\,(felice(x) \Rightarrow (amiciDelCuore(x,y) \wedge (\forall z\,.\,(amiciDelCuore(x,z) \Rightarrow y = z))))))$$

NOTA 4.6 (ESISTE UNICO) *In matematica è frequente esprimere delle proprietà che riguardano non solo l'esistenza di un certo elemento, ma anche la sua unicità, come nell'esempio appena visto. In questo caso si usa la notazione* $\boxed{(\exists!x.\ P(x))}$ *al posto della più complessa formula* $(\exists x.\ P(x) \wedge (\forall y.\ (P(y) \Rightarrow x = y)))$*, che presuppone la presenza del simbolo di predicato* $=$ *per confrontare l'identità degli elementi del dominio.*

4.4.1 Formalizzazione di enunciati sulla teoria degli insiemi

Nel Capitolo 2 abbiamo introdotto le principali relazioni e operazioni tra insiemi in modo preciso ma discorsivo, usando il linguaggio naturale. Un utile esercizio di formalizzazione consiste nel riformulare quelle definizioni usando formule predicative. La formalizzazione risulta particolarmente utile quando tali definizioni devono essere manipolate in qualche modo: vedremo più avanti (Esempio 4.13) la soluzione dell'Esercizio 1. Nel resto di questa sezione useremo l'alfabeto per gli insiemi $\mathcal{A}_S$ introdotto nella Definizione 4.4.

ESEMPIO 4.7 (FORMALIZZAZIONE DI RELAZIONI TRA INSIEMI)
Con formule predicative basate sull'alfabeto degli insiemi $\mathcal{A}_S$ *possiamo definire in modo rigoroso alcune delle relazioni tra insiemi introdotte nella Definizione 2.2. Siano* A *e* B *due generici insiemi:*

Inclusione: "A è un **sottoinsieme** di B, scritto $A \subseteq B$, se e solo se ogni elemento di A è anche elemento di B"

$$(A \subseteq B \quad \Leftrightarrow \quad (\forall x\,.\,(x \in A \Rightarrow x \in B))) \tag{4.3}$$

Disguaglianza: "A e B sono **diversi**, scritto $A \neq B$, se e solo se esiste almeno un elemento che è contenuto in uno dei due insiemi ma non nell'altro"

$$(A \neq B \quad \Leftrightarrow \quad (\exists x\,.\,((x \in A \ \wedge\ x \notin B) \vee (x \notin A \ \wedge\ x \in B)))) \tag{4.4}$$

Inclusione stretta: "A è un **sottoinsieme stretto** di B, scritto $A \subset B$, se e solo se $A \subseteq B$ e $A \neq B$"

$$(A \subset B \quad \Leftrightarrow \quad (A \subseteq B \ \wedge\ A \neq B)) \tag{4.5}$$

Naturalmente possiamo anche formalizzare le classiche operazioni su insiemi.

ESEMPIO 4.8 (FORMALIZZAZIONE DI OPERAZIONI SU INSIEMI)
Definiamo con formule predicative basate sull'alfabeto degli insiemi le operazioni su insiemi, introdotte nella Definizione 2.3, e in particolare la relazione di appartenenza ($\in$) *per insiemi ottenuti come risultato di queste operazioni. Siano* A *e* B *due generici insiemi:*

Intersezione:	$(x \in A \cap B$	$\Leftrightarrow$	$(x \in A \ \wedge\ x \in B))$
Unione:	$(x \in A \cup B$	$\Leftrightarrow$	$(x \in A \ \vee\ x \in B))$
Complemento (rispetto a $\mathcal{U}$)	$(x \in \overline{A}$	$\Leftrightarrow$	$(x \in \mathcal{U} \ \wedge\ x \notin A))$
Differenza:	$(x \in A \setminus B$	$\Leftrightarrow$	$(x \in A \ \wedge\ x \notin B))$

4.4.2 Formalizzazione e soluzione del Wason selection task

Come anticipato nel Capitolo 1, adesso abbiamo tutti gli strumenti che servono per formalizzare e risolvere il problema dell'Esercizio 1.3, il Wason selection task. Per praticità, ne ripetiamo il testo:

> Un poliziotto entra in un locale della Florida dove un grande cartello ricorda ai clienti che
>
> *per bere birra devi avere più di 16 anni*
>
> Nel locale ci sono altri quattro clienti: un ragazzo (che chiameremo Aldo) che sta bevendo acqua, una ragazza (Barbara) che sta bevendo birra, un'anziana signora (Carla) e un adolescente di 15 anni (Dante) che tengono i loro bicchieri racchiusi tra le mani.
>
> Quali clienti deve controllare il poliziotto per verificare che la regola sia rispettata?

Con riferimento al dominio delle persone, la regola sul cartello può essere formalizzata con la formula

$$C \equiv (\forall x\,.\,(bar(x) \Rightarrow (birra(x) \Rightarrow mag16(x))))$$

dove il simbolo di predicato $bar(x)$ indica se la persona x è nel bar oppure no, $birra(x)$ se sta bevendo birra e $mag16(x)$ se ha più di 16 anni. Possiamo inoltre formalizzare le informazioni disponibili sui quattro clienti con la formula

$$R \equiv (\neg birra(Aldo) \wedge birra(Barbara) \wedge mag16(Carla) \wedge \neg mag16(Dante))$$

Il poliziotto deve individuare tutte le persone p il cui comportamento potrebbe essere in contraddizione con la regola $(bar(p) \Rightarrow (birra(p) \Rightarrow mag16(p)))$. Trattandosi di un'implicazione, se p non è nel bar il predicato è soddisfatto banalmente. Quindi dobbiamo controllare solo le quattro persone che sono nel bar. Per ciascuna di queste, dato che la premessa $bar(p)$ è vera, affinché l'implicazione $(bar(p) \Rightarrow (birra(p) \Rightarrow mag16(p)))$ sia vera, occorre che la conclusione $(birra(p) \Rightarrow mag16(p))$ sia vera.

1. Per *Aldo*, sapendo che $birra(Aldo)$ è falso possiamo concludere che $(birra(Aldo) \Rightarrow mag16(Aldo))$ è vero, come si vede dalla seguente tabella:

$birra(Aldo)$	$mag16(Aldo)$	$(birra(Aldo) \Rightarrow mag16(Aldo)$
0	0	1
0	1	1

   Formalmente, ci chiediamo se è vera la formula

$$(\neg birra(Aldo) \Rightarrow ((birra(Aldo) \Rightarrow mag16(Aldo))))$$

   La seguente dimostrazione, che usa solo leggi del calcolo proposizionale, è un modo alternativo alla tabella di verità per verificare che la formula è vera:

$(\neg birra(Aldo) \Rightarrow ((birra(Aldo) \Rightarrow mag16(Aldo))))$
$\equiv$ { (eliminazione dell'implicazione) e (doppia negazione) }
$(birra(Aldo) \vee (\underline{(birra(Aldo) \Rightarrow mag16(Aldo))}))$
$\equiv$ { (eliminazione dell'implicazione) }
$(\underline{birra(Aldo)} \vee ((\neg birra(Aldo) \vee mag16(Aldo))))$
$\equiv$ { (associatività), (terzo escluso) }
$(\mathsf{T} \vee mag16(Aldo))$
$\equiv$ { (elemento assorbente) }
T

   Quindi Aldo soddisfa la regola e controllare l'età di *Aldo* è superfluo per il poliziotto:

2. Per *Barbara* sappiamo solo che $birra(Barbara)$ è vero, quindi a seconda che $mag16(Barbara)$ sia vero o falso, l'implicazione $(birra(Barbara) \Rightarrow mag16(Barbara))$ è vera o falsa, rispettivamente:

$birra(Barbara)$	$mag16(Barbara)$	$(birra(Barbara) \Rightarrow mag16(Barbara)$
1	0	0
1	1	1

   Il poliziotto deve quindi accertare l'età di *Barbara*.

3. Per *Carla*, l'anziana signora, sapendo che $mag16(Carla)$ è vero possiamo concludere che $(birra(Carla) \Rightarrow mag16(Carla))$ è vero:

$birra(Carla)$	$mag16(Carla)$	$(birra(Carla) \Rightarrow mag16(Carla)$
0	1	1
1	1	1

   Anche in questo caso si può dimostrare, come per *Aldo*, che vale la seguente implicazione, di cui lasciamo la verifica per esercizio:

$$(mag16(Carla) \Rightarrow (birra(Carla) \Rightarrow mag16(Carla)))$$

   Quindi controllare la consumazione di *Carla* è superfluo per il poliziotto.

4. Infine per *Dante* sappiamo solo che $mag16(Dante)$ è falso, quindi a seconda che $birra(Dante)$ sia vero o falso, l'implicazione $(birra(Dante) \Rightarrow mag16(Dante))$ è falsa o vera, rispettivamente:

$birra(Dante)$	$mag16(Dante)$	$(birra(Dante) \Rightarrow mag16(Dante)$
0	0	1
1	0	0

   Il poliziotto deve controllare la consumazione di *Dante* per far rispettare la legge.

Per concludere solo *Barbara* e *Dante* devono essere controllati.

4.5 Equivalenza logica e dimostrazioni per sostituzione

Nella Sezione 4.3 abbiamo visto come, fissata un'interpretazione I per un alfabeto del primo ordine $\mathcal{A}$, si può assegnare un valore di verità a ogni formula predicativa chiusa contenente simboli dell'alfabeto.

DEFINIZIONE 4.8
Analogamente al calcolo proposizionale:

- *una formula chiusa si dice* ***valida*** *se e solo se è vera in ogni interpretazione (corrisponde al concetto di tautologia);*
- *una formula chiusa si dice* ***insoddisfacibile*** *se e solo se è falsa in ogni interpretazione (corrisponde al concetto di contraddizione);*
- *una formula chiusa si dice* ***soddisfacibile*** *se e solo se esiste almeno un'interpretazione che la rende vera;*
- *due formule A e B si dicono* ***logicamente equivalenti*** *(scritto $A \equiv B$) se e solo se hanno lo stesso valore di verità rispetto a ogni possibile interpretazione.*

Rispetto al calcolo proposizionale il problema principale è che le interpretazioni possibili da considerare generalmente sono infinite. Inoltre, anche se fissiamo un'interpretazione, il dominio dei valori da considerare potrebbe essere infinito. Questo rende i problemi della soddisfacibilità e dell'equivalenza logica estremamente più complicati. Infatti non esiste per la logica dei predicati una tecnica analoga a quella delle tabelle di verità.

Fortunatamente, il principio di sostituzione e tutte le leggi relative ai connettivi logici che abbiamo visto per il calcolo proposizionale continuano a valere. Per cui anche nel caso della logica predicativa possiamo dimostrare l'equivalenza di formule sfruttando altre equivalenze già note. Inoltre ci sono delle equivalenze importanti che riguardano i quantificatori.

TEOREMA 5 (ALCUNE LEGGI SUI QUANTIFICATORI)
Valgono le seguenti equivalenze logiche su formule quantificate chiuse:

Leggi sui quantificatori		
$\neg(\exists x\,.\,A) \equiv\ (\forall x\,.\,\neg A)$	$\neg(\forall x\,.\,A) \equiv\ (\exists x\,.\,\neg A)$	*(De Morgan)*
$(\exists x\,.\,(A \vee B)) \equiv\ ((\exists x\,.\,A) \vee (\exists x\,.\,B))$	$(\forall x\,.\,(A \wedge B)) \equiv\ ((\forall x\,.\,A) \wedge (\forall x\,.\,B))$	*(distributività)*
$(\exists x\,.\,(\exists y\,.\,A)) \equiv\ (\exists y\,.\,(\exists x\,.\,A))$	$(\forall x\,.\,(\forall y\,.\,A)) \equiv\ (\forall y\,.\,(\forall x\,.\,A))$	*(commutatività)*

La dimostrazione di queste equivalenze va al di là degli obiettivi di queste note, ma possiamo mostrare, usando le dimostrazioni per sostituzione, che in ogni coppia di equivalenze sulla stessa riga della tabella l'una è conseguenza logica dall'altra.

ESEMPIO 4.9 (DIMOSTRAZIONI PER SOSTITUZIONE: $\neg(\forall x\,.\,A) \equiv\ (\exists x\,.\,\neg A)$)
Vediamo per esempio come la seconda legge di De Morgan può essere dimostrata usando la prima:

$\neg(\forall x\,.\,\underline{A})$
$\equiv$ { *(doppia negazione)* }
$\neg\underline{(\forall x\,.\,\neg\neg A)}$
$\equiv$ { *prima legge (De Morgan), applicata da destra verso sinistra sostituendo A con* $\neg A$ }
$\neg\neg(\exists x\,.\,\neg A)$
$\equiv$ { *(doppia negazione)* }
$(\exists x\,.\,\neg A)$

ESEMPIO 4.10 (DIMOSTRAZIONI PER SOSTITUZIONE: $(\forall x\,.\,(A \wedge B)) \equiv\ ((\forall x\,.\,A) \wedge (\forall x\,.\,B))$)
In modo analogo al caso precedente, possiamo dimostrare la seconda legge di distributività usando la prima:

$(\forall x\,.\,(A \wedge B))$
$\equiv$ { *(doppia negazione)* }
$\neg\neg\underline{(\forall x\,.\,(A \wedge B))}$
$\equiv$ { *(De Morgan) per* $\forall$ }
$\neg(\exists x\,.\,\underline{\neg(A \wedge B)})$
$\equiv$ { *(De Morgan) per* $\wedge$ }
$\neg\underline{(\exists x\,.\,(\neg A \vee \neg B))}$
$\equiv$ { *(distributività) per* $\exists$ }
$\neg(\underline{(\exists x\,.\,\neg A)} \vee \underline{(\exists x\,.\,\neg B)})$
$\equiv$ { *(De Morgan) per* $\forall$*, due volte* }
$\neg\underline{(\neg(\forall x\,.\,A) \vee \neg(\forall x\,.\,B))}$

$\equiv$ { *(De Morgan)* }

$\neg\neg((\forall x.A) \wedge (\forall x.B))$

$\equiv$ { *(doppia negazione)* }

$((\forall x.A) \wedge (\forall x.B))$

Relativamente alle leggi di distributività per i quantificatori, è bene riflettere sul fatto che il quantificatore esistenziale distribuisce *solo* rispetto alla disgiunzione, mentre quello universale *solo* rispetto alla congiunzione. Infatti in generale non è vero che $(\forall x.(A \vee B)) \equiv ((\forall x.A) \vee (\forall x.B))$, anche se in alcuni casi può esser vero.

ESEMPIO 4.11 (CONTROESEMPIO PER $(\forall x.(A \vee B)) \equiv ((\forall x.A) \vee (\forall x.B))$)
Come controesempio consideriamo l'alfabeto dei naturali con la corrispondente interpretazione $I_{\mathbb{N}}$, e le due formule

$$(\forall x.(pari(x) \vee dispari(x))) \qquad ((\forall x.pari(x)) \vee (\forall x.dispari(x)))$$

Chiaramente $I_{\mathbb{N}} \models (\forall x.(pari(x) \vee dispari(x)))$, perché è vero che ogni numero naturale o è pari o è dispari. Però abbiamo $I_{\mathbb{N}} \not\models (\forall x.pari(x))$, perché non è vero che tutti i naturali sono pari, e analogamente $I_{\mathbb{N}} \not\models (\forall x.dispari(x))$. Quindi abbiamo $I_{\mathbb{N}} \not\models ((\forall x.pari(x)) \vee (\forall x.dispari(x)))$.

Analogamente, in generale non è vero che $(\exists x.(A \wedge B)) \equiv ((\exists x.A) \wedge (\exists x.B))$, cioè la quantificazione esistenziale non distribuisce rispetto alla congiunzione, anche se in alcuni casi può esser vero. Il lettore è invitato a trovare un controesempio a questa equivalenza, magari sfruttando quello visto precedentemente.

Concludiamo quest'analisi delle leggi per i quantificatori osservando che l'ultima legge, la commutatività, vale solo per coppie di quantificatori dello stesso tipo.

In generale infatti non vale $(\exists x.(\forall y.A))) \equiv (\forall y.(\exists x.A))$, anche se in alcuni casi può essere vero.

Intuitivamente, la formula $(\exists x.(\forall y.A))$ asserisce che esiste (almeno) un particolare valore di x che rende valida A indipendentemente dall'y considerato. La formula $(\forall y.(\exists x.A))$ invece asserisce che per ciascun valore y possiamo trovare un valore x che rende vera A, ma per valori di y diversi potrebbero servire valori di x diversi.

ESEMPIO 4.12 (CONTROESEMPIO PER $(\exists x.(\forall y.A))) \equiv (\forall y.(\exists x.A)))$)
È facile costruire un controesempio, usando il dominio dei naturali. Abbiamo che $I_{\mathbb{N}} \models (\forall y.(\exists x.y < x))$, perché la formula asserisce che per ogni naturale possiamo trovarne uno strettamente più grande, cosa che è ovviamente vera. Ma $I_{\mathbb{N}} \not\models (\exists x.(\forall y.y < x))$: infatti questa formula asserisce che esiste un naturale più grande di tutti gli altri, cosa che è chiaramente falsa. Quindi le due formule non sono logicamente equivalenti.

ESEMPIO 4.13 (DIMOSTRAZIONI SU INSIEMI)
Nell'Esempio 4.7 abbiamo visto come formalizzare alcune delle relazioni tra insiemi introdotte nella Definizione 2.2. Vediamo ora come si possono usare le dimostrazioni per sostituzione sia per controllare la correttezza di concetti derivati da definizioni date, sia per risolvere semplici problemi.

Nell'Esempio 4.7 abbiamo formalizzato con la seguente formula la relazione di inclusione stretta *tra due insiemi:*

$$(A \subset B \quad \Leftrightarrow \quad (A \subseteq B \ \wedge \ A \neq B))$$

D'altra parte dopo la Definizione 2.2 avevamo affermato che "per dimostrare che $A \subset B$ si può mostrare che ogni elemento di A appartiene a B, ma che esiste un elemento di B che non appartiene ad A". *Traducendo la frase in una formula predicativa otteniamo:*

$$(((\forall x.(x \in A \Rightarrow x \in B) \ \wedge \ (\exists x.(x \notin A \ \wedge \ x \in B))) \quad \Rightarrow \quad A \subset B)$$

Vediamo che questo è vero, mostrando che premessa e conseguenza sono anzi logicamente equivalenti:

$A \subset B$

$\equiv$ { *formula (4.5) dell'Esempio 4.7, ricordando che $(P \Leftrightarrow Q)$ se e solo se $P \equiv Q$* }

$(A \subseteq B \ \wedge \ A \neq B)$

$\equiv$ { *formula (4.3) dell'Esempio 4.7* }

$$
\begin{array}{ll}
 & ((\forall x.(x \in A \Rightarrow x \in B)) \wedge \underline{A \neq B}) \\
\equiv & \quad \{ \textit{ formula (4.4) dell'Esempio 4.7 } \} \\
 & ((\forall x.(x \in A \Rightarrow x \in B)) \wedge \underline{(\exists x.((x \in A \wedge x \notin B) \vee (x \notin A \wedge x \in B)))}) \\
\equiv & \quad \{ \textit{ (distributività) di } \exists \textit{ su } \vee \} \\
 & ((\forall x.(x \in A \Rightarrow x \in B)) \wedge ((\exists x.(x \in A \wedge x \notin B)) \vee (\exists x.(x \notin A \wedge x \in B)))) \\
\equiv & \quad \{ \textit{ (distributività) di } \wedge \textit{ su } \vee \} \\
 & (((\forall x.(x \in A \Rightarrow x \in B)) \wedge \underline{(\exists x.(x \in A \wedge x \notin B))}) \vee ((\forall x.(x \in A \Rightarrow x \in B)) \wedge (\exists x.(x \notin A \wedge x \in B)))) \\
\equiv & \quad \{ \textit{ (doppia negazione) e (De Morgan) } \} \\
 & (((\forall x.(x \in A \Rightarrow x \in B)) \wedge \neg(\forall x.\underline{\neg(x \in A \wedge x \notin B)})) \vee ((\forall x.(x \in A \Rightarrow x \in B)) \wedge (\exists x.(x \notin A \wedge x \in B)))) \\
\equiv & \quad \{ \textit{ (De Morgan) e (eliminazione implicazione) al contrario } \} \\
 & (\underline{((\forall x.(x \in A \Rightarrow x \in B)) \wedge \neg(\forall x.(x \in A \Rightarrow x \in B)))} \vee ((\forall x.(x \in A \Rightarrow x \in B)) \wedge (\exists x.(x \notin A \wedge x \in B)))) \\
\equiv & \quad \{ \textit{ (contraddizione) } \} \\
 & (\mathsf{F} \vee ((\forall x.(x \in A \Rightarrow x \in B)) \wedge (\exists x.(x \notin A \wedge x \in B)))) \\
\equiv & \quad \{ \textit{ (elemento neutro) } \} \\
 & ((\forall x.(x \in A \Rightarrow x \in B)) \wedge (\exists x.(x \notin A \wedge x \in B)))
\end{array}
$$

Cerchiamo ora di esplicitare, come richiesto nell'Esercizio 2.5.2.1c, come si può dimostrare che $A \not\subset B$. Abbiamo:

$$
\begin{array}{ll}
 & A \not\subset B \\
\equiv & \quad \{ \textit{ per la dimostrazione appena fatta } \} \\
 & \neg((\forall x.(x \in A \Rightarrow x \in B)) \wedge (\exists x.(x \notin A \wedge x \in B))) \\
\equiv & \quad \{ \textit{ (De Morgan) per } \wedge \} \\
 & (\underline{\neg(\forall x.(x \in A \Rightarrow x \in B))} \vee \underline{\neg(\exists x.(x \notin A \wedge x \in B))}) \\
\equiv & \quad \{ \textit{ (De Morgan), due volte } \} \\
 & ((\exists x.\underline{\neg(x \in A \Rightarrow x \in B)}) \vee (\forall x.\underline{\neg(x \notin A \wedge x \in B)})) \\
\equiv & \quad \{ \textit{ (eliminazione implicazione) e (De Morgan) } \} \\
 & ((\exists x.\underline{\neg(\neg(x \in A) \vee x \in B)}) \vee (\forall x.\underline{(x \in A \vee \neg(x \in B))})) \\
\equiv & \quad \{ \textit{ (De Morgan), (doppia negazione) e (eliminazione implicazione) al contrario } \} \\
 & ((\exists x.(x \in A \wedge x \notin B)) \vee (\forall x.(x \in B \Rightarrow x \in A)))
\end{array}
$$

Rileggendo questa formula in italiano possiamo concludere che *"per dimostrare che $A \not\subset B$ si può mostrare che esiste un elemento di A che non appartiene a B, oppure che ogni elemento di B appartiene ad A"*.

4.6 Esercizi[4]

4.6.1 Esercizi di comprensione

4.6.1.1 Qual è la differenza tra termini e formule atomiche?

4.6.1.2 Qual è la differenza tra formule aperte e formule chiuse?

[4] Alcuni esercizi sono tratti da materiale liberamente accessibile sul web, preparato da Dario Palladino.

4.6.1.3 Considerando l'alfabeto dei naturali $\mathcal{A}_{\mathbb{N}}$, quali delle seguenti espressioni sono termini?

(a) $x+0$
(b) $7+$
(c) $1+1$
(d) $x \leq 0$
(e) $(\forall x\,.\,x \leq 0)$
(f) $x++$

4.6.1.4 Considerando l'alfabeto dei naturali $\mathcal{A}_{\mathbb{N}}$, quali delle seguenti espressioni sono formule atomiche?

(a) $x+0$
(b) $x \leq 0$
(c) $(\forall x\,.\,(x \leq 0))$
(d) $x \leq\leq 0$

4.6.1.5 Considerando l'alfabeto dei naturali $\mathcal{A}_{\mathbb{N}}$, quali delle seguenti espressioni sono formule? Quali formule sono chiuse?

(a) $x+0$
(b) $x \leq 0$
(c) $(\forall x\,.\,(x \leq 0))$
(d) $\forall x\,.\,(x \leq 0)$
(e) $(\forall x\,.\,(\exists y\,.\,(y \leq x)))$
(f) $(\forall x\,.\,(\exists x\,.\,(x \leq x)))$
(g) $(\forall x\,.\,(x+1))$
(h) $(x \leq y) \leq z$
(i) $((x \leq y) \wedge (y \leq z))$
(j) $(x \leq y) + (y \leq z)$

4.6.1.6 In cosa i simboli di predicato sono trattati diversamente dai simboli di funzione?

4.6.1.7 Quali delle seguenti affermazioni sono vere?

(a) *"Una formula predicativa chiusa ha un solo valore di verità"*.
(b) *"Una formula predicativa chiusa ha un solo valore di verità rispetto a una data interpretazione"*.
(c) *"Una formula predicativa aperta ha un solo valore di verità"*.
(d) *"Una formula predicativa aperta ha un solo valore di verità rispetto a una data interpretazione"*.

4.6.1.8 Dire se le seguenti affermazioni sono vere o false, motivando la risposta:

(a) *"Tutti i quantificatori distribuiscono sulla congiunzione"*.
(b) *"Tutti i quantificatori distribuiscono sulla disgiunzione"*.
(c) *"Tutti i quantificatori distribuiscono sulla congiunzione e sulla disgiunzione"*.
(d) *"Tutti i quantificatori distribuiscono sulla congiunzione o sulla disgiunzione"*.
(e) *"Esiste un quantificatore che distribuisce sulla congiunzione e sulla disgiunzione"*.
(f) *"Esiste un quantificatore che distribuisce sulla congiunzione o sulla disgiunzione"*.
(g) *"Esiste un quantificatore che distribuisce sulla congiunzione e uno che distribuisce sulla disgiunzione"*.

4.6.1.9 Quali delle seguenti formule basate sui consueti simboli di costante, di funzione e di predicato sono ben formate? Perché?

(a) $(\forall x\,.\,(x+7))$.
(b) $(\exists x\,.\,(x \leq (\forall y\,.\,y \leq 5)))$
(c) $(\forall x\,.\,(\exists y\,.\,x \leq y))$
(d) $(\forall x\,.\,(\exists y\,.\,xy))$
(e) $(\forall x\,.\,(\exists y\,.\,x^y = y^x))$
(f) $(((\forall x\,.\,x)+5) \leq 10)$

4.6.1.10 Assumendo l'interpretazione standard sul dominio dei numeri naturali $\mathbb{N}$, descrivere a parole il significato delle seguenti formule:

(a) $(\forall x\,.\,x \leq 2x)$
(b) $(\forall x\,.\,\neg(\exists y\,.\,x+y<x))$
(c) $(\exists x\,.\,(\forall y\,.\,(\exists z\,.\,z=xy)))$
(d) $(\forall x\,.\,(\forall y\,.\,(\exists z\,.\,z=xy)))$
(e) $(\exists x\,.\,(\exists n\,.\,(\forall z\,.\,x=z^n)))$
(f) $(\forall x\,.\,(\exists y\,.\,(\forall z\,.\,y<x+z)))$

4.6.2 Esercizi di approfondimento

4.6.2.1 Dire se le seguenti formule sono vere oppure no rispetto all'interpretazione standard $I_{\mathbb{N}}$ sul dominio dei naturali $\mathbb{N}$:

(a) $(\exists x\,.\,(\exists y\,.\,(x\leq y)))$
(b) $(\exists x\,.\,(\forall y\,.\,(x\leq y)))$
(c) $(\forall y\,.\,(\exists x\,.\,(x\leq y)))$
(d) $(\forall y\,.\,(\forall x\,.\,(x\leq y)))$
(e) $(\forall x\,.\,(\forall y\,.\,(\exists z\,.\,z=xy)))$
(f) $(\forall x\,.\,(\exists y\,.\,(\forall z\,.\,y<x+z)))$

4.6.2.2 Dire se le formule dell'esercizio precedente sono vere oppure no rispetto all'ovvia interpretazione standard $I_{\mathbb{Z}}$ sul dominio degli interi $\mathbb{Z}$.

4.6.2.3 Dire se le seguenti formule sono vere oppure no rispetto all'interpretazione standard sui naturali:

(a) $(\forall x\,.\,(x^2\geq 0))$
(b) $(\exists x\,.\,(x^2=2))$
(c) $(\forall x\,.\,(x^2\geq x))$
(d) $(\forall x\,.\,(\exists y\,.\,(x^2<y)))$
(e) $(\exists x\,.\,(\forall y\,.\,(x<y^2)))$
(f) $(\forall x\,.\,(\exists y\,.\,(x+y=0)))$
(g) $(\exists x\,.\,(\forall y\,.\,(x\times y=0)))$
(h) $(\exists x\,.\,(\exists y\,.\,(x^2+y^2=5)))$
(i) $(\exists x\,.\,(\exists y\,.\,(x^2+y^2=6)))$
(j) $(\exists x\,.\,(\exists y\,.\,(x+y=4\ \wedge\ x-y=1)))$
(k) $(\forall x\,.\,(\forall y\,.\,(\exists z\,.\,(z=(x+y)/2))))$

4.6.2.4 Si formalizzino le seguenti frasi usando e/o estendendo le interpretazioni introdotte nella Definizione 4.6 e i rispettivi alfabeti

(a) [Esercizio svolto] *"Se una persona è di sesso femminile ed è genitore allora è la madre di almeno una persona"*

[Svolgimento] Estendiamo l'alfabeto delle persone $\mathcal{A}_{\mathcal{P}}$ e la rispettiva interpretazione $I_{\mathcal{P}}$ con i seguenti simboli: (1) i simboli di predicato unari femmina e genitore tali che $femmina^{I_{\mathcal{P}}}(p)$ è vera se e solo se la persona p è donna e $genitore^{I_{\mathcal{P}}}(p)$ è vera se e solo se la persona p ha figli; (2) il simbolo di funzione unario madre tale che $madre^{I_{\mathcal{P}}}(p)=q$ se e solo se q è la madre di p. Allora la frase può essere formalizzata con: $(\forall x\,.\,((femmina(x)\wedge genitore(x))\Rightarrow(\exists y\,.\,x=madre(y))))$

(b) *"Ogni persona conosce un solo idraulico e un solo elettricista"*

(c) *"I numeri pari sono tutti e soli quelli divisibili per due"*
(Si sfrutti il simbolo funzionale $\_\%\_$ che viene interpretato come il resto della divisione intera.)

(d) *"Esiste almeno un numero che è divisibile per tutti i numeri minori di 10"*

(e) *"I numeri primi sono tutti e soli quei numeri maggiori di* 1 *e divisibili solo per* 1 *e per se stessi"*

4.6.2.5 Si formalizzino gli enunciati enunciati dell'Ultimo Teorema di Fermat (Sezione 1.5.1) e della Congettura di Goldbach (Sezione 1.5.3), utilizzando l'alfabeto e l'interpretazione standard dei naturali.

4.6.2.6 Sia $\mathcal{A}$ l'alfabeto del primo ordine contenente i predicati unari $italiano(x)$, $onesto(x)$ e $beneducato(x)$ con l'ovvia interpretazione sul dominio delle persone. Formalizzare i seguenti enunciati:

(a) [Esercizio svolto] *"Qualche italiano è onesto e beneducato"*.
[Svolgimento] $(\exists x\,.\,(italiano(x) \wedge onesto(x) \wedge beneducato(x)))$

(b) *"Qualche italiano è onesto solo se è stato educato bene"*.

(c) *"Qualche italiano è onesto se è stato educato bene"*.

(d) *"Ogni italiano è onesto se è stato educato bene"*.

(e) *"Ogni italiano è stato educato bene se è onesto"*.

(f) *"Ogni italiano è stato educato bene se e solo se è onesto"*.

(g) *"Solo gli italiani beneducati sono onesti"*.

(h) *"Solo gli italiani onesti sono stati educati bene"*.

(i) *"Qualche italiano è onesto anche se non è stato educato bene"*.

(j) *"Qualche italiano che non è stato educato bene non è onesto"*.

(k) *"Qualche italiano non è né onesto né beneducato"*.

(l) *"Nessun italiano che sia stato educato bene può non essere onesto"*.

4.6.2.7 Sia $\mathcal{A}$ l'alfabeto del primo ordine contenente la costante *Angelo* e il predicato binario $rispetta(x,y)$ con l'ovvia interpretazione sul dominio delle persone. Formalizzare i seguenti enunciati:

(a) [Esercizio svolto] *"Angelo rispetta tutti"*.
[Svolgimento] $(\forall x\,.\,rispetta(Angelo,x))$

(b) *"Angelo è rispettato da tutti"*.

(c) *"Chi rispetta Angelo, rispetta tutti"*.

(d) *"Chi rispetta qualcuno, rispetta Angelo"*.

(e) *"Tutti si rispettano a vicenda"*.

(f) *"Tutti rispettano qualcuno"*.

(g) *"Chiunque rispetta sé stesso, rispetta Angelo"*.

(h) *"Se c'è qualcuno che rispetta sé stesso, quello è Angelo"*.

(i) *"Qualcuno è rispettato da tutti"*.

(j) *"Qualcuno rispetta solo sé stesso"*.

(k) *"C'è qualcuno che solo Angelo rispetta"*.

4.6.2.8 Formalizzare i seguenti enunciati introducendo opportune costanti e simboli di predicato interpretati sul dominio delle persone.

(a) *"Stefano è più alto di Carlo"*.

(b) *"Stefano è alto e Carlo è basso"*.

(c) *"Tutti sono più alti di Carlo"*.

(d) *"Non tutti sono più alti di Carlo"*.

(e) *"Se Carlo ha rubato la marmellata sarà punito"*.

(f) *"Chiunque ha rubato la marmellata sarà punito"*.

(g) *"Carlo e chiunque ha rubato la marmellata sarà punito"*.

(h) *"Se un ragazzo è bugiardo nessuno gli crederà"*.

(i) *"Nessuno ama qualcuno se non ama sè stesso"*.

(j) *"Ogni uomo ha qualche amico, ma nessun uomo è amico di tutti"*.

(k) *"C'è un venditore dal quale tutti comprano"*.

(l) *"Ognuno compra da un venditore"*.

(m) *"Qualche persona compra da un solo venditore"*.

(n) *"Qualche persona compra da tutti i venditori"*.

(o) *"Nessuno compra da tutti i venditori"*.

(p) *"Se c'è uno che comprerebbe da tutti i venditori quello è Carlo"*.

4.6.2.9 Formalizzare i seguenti enunciati usando i consueti simboli di funzione e di predicato interpretati sul dominio dei naturali, negarli e scriverne la descrizione in linguaggio naturale:

(a) *"Ogni numero è minore di un altro numero"*.

(b) *"Esiste un numero che divide tutti gli altri numeri"*.

(c) *"Ogni numero è esprimibile come il prodotto di due numeri più piccoli"*.

(d) *"Per ogni numero esiste un numero più grande"*.

(e) *"Esiste un numero più grande di un altro numero"*.

(f) *"Esiste un numero più grande di tutti i numeri per i quali esiste un numero più piccolo"*.

4.6.2.10 Sulla falsariga dell'Esempio 4.7, si formalizzino le relazioni di uguglianza e disgiunzione di insiemi introdotte nella Definizione 2.2.

4.6.3 Esercizi che coinvolgono dimostrazioni per sostituzione

4.6.3.1 Sulla falsariga dell'Esempio 4.13, riprendendo l'Esercizio 2.5.2.1,

(a) descrivere informalmente come si può dimostrare che (1) $A \neq B$, e (2) $A \not\subseteq B$;

(b) formalizzare gli enunciati del punto precedente nella logica del primo ordine;

(c) dimostrare per sostituzione che le formule ottenute implicano rispettivamente (1) e (2).

4.6.3.2 Dimostrare le seguenti equivalenze logiche:

(a) $((\forall x\,.\,P(x)) \Rightarrow (\exists x\,.\,Q(x))) \equiv (\exists x\,.\,(P(x) \Rightarrow Q(x)))$

(b) $(\neg(\exists x\,.\,P(x)) \wedge (\forall x\,.\,Q(x))) \equiv (\forall x\,.\,\neg(Q(x) \Rightarrow P(x)))$

(c) $(\neg(\exists x\,.\,(P(x) \wedge Q(x))) \Rightarrow (\exists x\,.\,\neg Q(x))) \equiv (\exists x\,.\,(Q(x) \Rightarrow P(x)))$

(d) $((\forall x\,.\,P(x)) \;\Rightarrow\; (\exists x\,.\,Q(x))) \equiv (\exists x\,.\,(\neg Q(x) \;\Rightarrow\; \neg P(x)))$

4.6.3.3 Dimostrare che le seguenti formule sono valide:

(a) $((\forall x\,.\,(P(x) \vee \neg Q(x))) \Leftrightarrow \neg(\exists x\,.\,(\neg P(x) \wedge Q(x))))$

(b) $(\neg(\forall x\,.\,\neg(P(x) \Rightarrow (\exists y\,.\,Q(y)))) \Leftrightarrow (\exists x\,.\,\neg(P(x) \wedge (\forall y\,.\,\neg Q(y)))))$

(c) $(((\forall x\,.\,P(x)) \wedge (\exists x\,.\,Q(x))) \Rightarrow (\exists x\,.\,(P(x) \Rightarrow Q(x))))$

4.6.3.4 Fornire un controesempio alle seguenti implicazioni definendo un'opportuna interpretazione, sul dominio delle persone, dei simboli di predicato che vi compaiono. [**Suggerimento**: usare il principio di sostituzione per semplificare le formule prima di cercare il controesempio)]

(a) $(\forall x\,.\,(\forall y\,.\,P(x,y) \Rightarrow P(y,x)))$

(b) $(\forall x\,.\,(\exists y\,.\,P(x,y))) \Leftrightarrow (\exists y\,.\,(\forall x\,.\,P(x,y)))$

(c) $(((\forall x\,.\,P(x)) \wedge (\exists x\,.\,Q(x))) \Rightarrow (\forall x\,.\,(P(x) \Rightarrow Q(x))))$

(d) $(((\forall x\,.\,P(x)) \Rightarrow (\exists x\,.\,Q(x))) \Rightarrow (\forall x\,.\,(P(x) \;\Rightarrow\; Q(x))))$

(e) $(((\exists x\,.\,(\forall y\,.\,(P(x,y) \Rightarrow \neg Q(y,x)))) \wedge (\forall x\,.\,(\exists y\,.\,Q(y,x)))) \Rightarrow (\exists x\,.\,\neg P(x,x)))$

(f) $(((\exists x\,.\,(\forall y\,.\,(P(x,y) \Rightarrow \neg Q(y,x)))) \wedge (\forall x\,.\,(\exists y\,.\,Q(y,x)))) \Rightarrow (\forall x\,.\,(\forall y\,.\,\neg P(x,y))))$

4.6.3.5 Con riferimento alla notazione della Sezione 4.4.2, sulla formalizzazione del Wason selection task, dimostrare per sostituzione che la formula $(mag16(Carla) \Rightarrow (birra(Carla) \Rightarrow mag16(Carla)))$ è valida.

Capitolo 5

Le espressioni regolari

I capitoli precedenti trattavano alcuni argomenti classici della matematica e della logica che i lettori avevano sicuramente incontrato in precedenza, anche se non approfondito. Questo capitolo introduce invece un argomento classico dell'informatica che ha trovato largo impiego in applicazioni pratiche: le *espressioni regolari*.

Le espressioni regolari permettono di definire una particolare classe di linguaggi formali. Senza anticipare in queste note i concetti fondamentali di quell'area, come grammatiche e automi, le espressioni regolari offrono un ulteriore esempio per applicare il bagaglio di nozioni e tecniche viste nei capitoli precedenti:

- Un linguaggio formale è un *insieme* L di sequenze formate da simboli presi da un alfabeto A fissato (usando la notazione che abbiamo introdotto nel Capitolo 2 possiamo cioè scrivere $L \subseteq A^*$). In gergo informatico, le sequenze di simboli presi dall'alfabeto A sono chiamate *stringhe*.
- La classe dei linguaggi associati alle espressioni regolari soddisfa importanti proprietà che la rendono particolarmente significativa. Senza poterci addentrare troppo nell'argomento, una di queste proprietà è la cosiddetta *chiusura* rispetto alle operazioni su insiemi. Questo significa che l'intersezione, l'unione, la differenza e il complemento di linguaggi regolari risultano essere ancora linguaggi regolari.[1]
- Le sequenze che appartengono a un certo linguaggio sono solitamente caratterizzate da alcune *proprietà logiche* che possiamo descrivere con la notazione introdotta nei Capitoli 3 e 4.
- Così come a ogni espressione aritmetica è associato un valore intero e a ogni formula logica è associato un valore booleano, ad ogni espressione regolare è associato un particolare insieme di sequenze e due espressioni regolari che definiscono lo stesso linguaggio sono considerate *semanticamente equivalenti*.
- Le espressioni regolari sono costruite con un insieme ristretto di operatori, dal significato immediato, e sono manipolabili algebricamente grazie ad un numero ridotto di leggi che preservano l'equivalenza semantica mediante il *principio di sostituzione* con il quale abbiamo familiarizzato nei capitoli precedenti.

Una diffusa applicazione delle espressioni regolari è quella per la ricerca e sostituzione di testo. A partire da questa, nelle sezioni successive introdurremo la nozione di linguaggio formale e relative operazioni, spiegheremo come comporre e interpretare le espressioni regolari e ne descriveremo alcune leggi algebriche.

5.1 La ricerca di stringhe

Riconoscere gli schemi è qualcosa di abbastanza naturale per gli uomini. Le espressioni regolari offrono un modo, privo di ambiguità, per indicare alla macchina qual è lo schema che ci interessa, ma per farlo dobbiamo riuscire a formalizzarlo senza errori. Come descrivereste la parte indirizzo su una busta? E le sequenze di numeri che rappresentano dei numeri telefonici per chiamare apparecchi fissi? Come sappiamo che una certa sequenza rappresenta un indirizzo e-mail? Sicuramente ognuno di noi è in grado di riconoscere sequenze dei tipi descritti sopra. Più difficile è trovare un modo sistematico per enucleare le regole *formali* che applichiamo inconsapevolmente nel farlo.

[1] Per maggior precisione, la classe dei linguaggi regolari è chiusa anche rispetto alle operazioni di concatenazione e stella di Kleene, per le quali rimandiamo alla Definizione 5.5.

ESEMPIO 5.1 (TROVARE E SOSTITUIRE)
Immaginiamo di voler comporre una lunga relazione a partire dalla versione elettronica di note raccolte in periodi precedenti e di altro materiale raccolto in forma di testo elettronico, magari scaricato dalla rete e organizzato su documenti diversi. Supponiamo anche di voler articolare la relazione in capitoli e che per questo motivo ci troviamo di fronte all'esigenza di dover chiamare "Capitolo" ogni parte che prima era invece chiamata "Sezione". Fare questa operazione a mano sarebbe un compito ingrato e soggetto ad errori. Come sappiamo, ogni elaboratore di testi mette a disposizione una funzionalità che ci permette di impostare velocemente la ricerca e la sostituzione di stringhe (ovvero sequenze di simboli). Lo stesso accade per il sistema operativo, che mette a disposizione funzionalità analoghe per applicare automaticamente la ricerca con sostituzione su più documenti. Questi sistemi sono basati sulle espressioni regolari *(*regular expressions*) e permettono di definire degli* schemi *(*patterns*) da ricercare in un testo: la ricerca avviene confrontando ogni porzione del testo di riferimento con lo schema che stiamo ricercando per vedere se vi è corrispondenza.*

Nel nostro esempio il compito consiste nel cercare tutte le occorrenze della stringa "Sezione", per poi sostituirle con la stringa "Capitolo". A prima vista l'operazione non sembra così complicata, ma soffermiamoci a osservarla più attentamente. Cosa succede se da qualche parte nel testo appare la stringa "sezione"? Distinguiamo le maiuscole dalle minuscole? E ancora, cosa succede se questa distinzione non la prevediamo e la stringa "sezione" possiamo trovarla all'interno di una stringa più lunga? Per esempio, se avessimo applicato la sostituzione in modo disattento al testo che compone queste note avremmo potuto finire con l'introdurre varie volte nel testo la parola "intercapitolo" al posto di "intersezione".

Le espressioni regolari sono utili per descrivere una classe di schemi e modificarne con facilità la descrizione. Esistono poi sistemi per tradurre le espressioni regolari ed implementare i corrispondenti riconoscitori.

ESEMPIO 5.2 (RICONOSCERE UN INDIRIZZO DI POSTA ELETTRONICA)
Come si identifica un indirizzo e-mail corretto? Sappiamo che sicuramente ad un certo punto nella stringa dovrà comparire il simbolo "@". E probabilmente dopo questo simbolo troveremo una stringa che al suo interno contiene almeno un punto. Sappiamo inoltre che le varie sotto-stringhe contengono caratteri alfanumerici. Vediamo di comporre una possibile espressione regolare che ci permetta di codificare quanto detto. Esistono notazioni diverse per esprimere le stesse espressioni regolari. Per il momento ci limiteremo a descrivere lo schema in linguaggio naturale e poi tradurremo la descrizione nella notazione adottata dal linguaggio Javascript, un linguaggio di programmazione orientato agli oggetti tra i più usati nella programmazione di siti web.

Ogni sequenza di caratteri che forma un indirizzo di posta elettronica dovrebbe:[2]

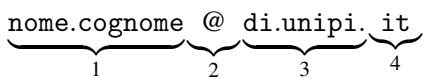
1. *iniziare con una stringa non vuota composta da soli caratteri alfanumerici (lettere minuscole e maiuscole dell'alfabeto inglese e cifre decimali), underscore (o trattino basso) e punti; questa parte dell'indirizzo è quella che precede il simbolo della chiocciola* '`@`' *o* a commerciale *(si legge come l'inglese "at");*

2. *proseguire con una singola occorrenza del simbolo* '`@`'*; questo simbolo separa il nome che corrisponde all'account di posta elettronica (la parte iniziale descritta in precedenza) dal dominio a cui l'account appartiene (la parte descritta nei punti successivi);*

3. *comprendere, dopo la chiocciola, una o più stringhe, separate con il punto* '`.`'*;*

4. *concludersi con una sequenza di caratteri che descrive il cosiddetto* dominio di primo livello*; questa sequenza ha solitamente una lunghezza ridotta che varia dai 2 ai 4 caratteri nella maggior parte dei casi, ma che può arrivare a 6 caratteri (domini* `museum` *e* `travel`*).*

Per esempio gli indirizzi dei docenti del nostro dipartimento di informatica hanno la forma



che può essere ricondotta allo schema sopra mediante la corrispondenza illustrata.

Tanto per avere un'idea di come sia possibile formalizzare la descrizione data sopra, vediamo adesso l'espressione regolare corrispondente (nella notazione Javascript):

[2] Per semplicità trascuriamo volutamente la presenza di simboli quali il trattino − o la percentuale % nell'indirizzo.

$$\underbrace{[\backslash w \backslash .]+}_{1}\ \underbrace{@}_{2}\ \underbrace{[\backslash w \backslash .]+}_{3}\ \underbrace{\backslash .[\backslash w]\{2,6\}}_{4}$$

Andiamo ora a spiegarne il significato, analizzando parte per parte l'espressione.

- *Con* `\w` *si indica un qualunque carattere alfanumerico e il trattino basso* _.[3]
- *Con* `\.` *si indica il punto.*[4]
- *Con le parentesi quadrate* `[ ]` *si indica la presenza di un singolo carattere tra quelli contenuti nelle parentesi. Quindi* `[\w\.]` *indica un qualsiasi carattere o il punto.*
- *Con l'operatore* `+` *si indica che dal blocco che lo precede possiamo scegliere consecutivamente* uno o più *simboli. Quindi l'espressione* `[\w\.]+` *indica una qualsiasi stringa non vuota composta di caratteri e punto.*
- *Il simbolo* `@` *indica il carattere chiocciola.*
- *Le parentesi graffe permettono di specificare la lunghezza minima e massima della stringa definita dal blocco che le precede. Quindi* `[\w]{2,6}` *indica una qualsiasi stringa composta di simboli alfanumerici la cui lunghezza è compresa tra 2 e 6 (estremi inclusi).*

Il linguaggio associato all'espressione regolare appena vista è formato da tutte e sole le stringhe che sono conformi allo schema, cioè tutti gli indirizzi di posta elettronica che erano stati individuati nella descrizione in linguaggio naturale.

Adesso che abbiamo un'idea degli schemi che ci piacerebbe riuscire a descrivere, possiamo addentrarci nel definire in modo puntuale le regole di composizione delle espressioni regolari. Ci accorgeremo che la loro definizione ci conduce alla determinazione di una vera e propria algebra, nella quale si definiscono le espressioni elementari e le operazioni con le quali comporre termini via via più complessi.

Prima di iniziare è utile introdurre alcuni concetti elementari relativi ai linguaggi formali.

5.2 Le stringhe e i linguaggi

DEFINIZIONE 5.1 (ALFABETI)
Un ***alfabeto*** Σ *è un insieme finito e non vuoto. Gli elementi di un alfabeto sono chiamati* ***simboli****.*

ESEMPIO 5.3 (ALFABETI DI INTERESSE)

- *L'alfabeto occidentale è* $\Sigma_A = \{a, b, c, \ldots, z\}$*, cioè l'insieme di tutte le lettere (minuscole, per semplicità).*
- *L'alfabeto binario è* $\Sigma_{\mathbb{B}} = \{0, 1\}$

DEFINIZIONE 5.2 (STRINGHE)
Dato un alfabeto Σ*, una* ***stringa*** *su* Σ *è una sequenza finita, anche vuota, di simboli appartenenti a* Σ*. La* ***stringa vuota*** *è indicata con* ε*.*

Di seguito usiamo $a, b, \ldots$ per indicare i simboli di Σ e $u, v, w, \ldots$ per indicare le stringhe su Σ.

ESEMPIO 5.4 (STRINGHE)

- *Ogni parola (senza lettere accentate, per semplicità) è una stringa sull'alfabeto* Σ_A*.*
- *La codifica binaria su 8 bit del valore* 12 *è la stringa* 00001100 *sull'alfabeto* $\Sigma_{\mathbb{B}}$*.*

La notazione usata per indicare il numero di simboli in una stringa è analoga a quella usata per indicare la cardinalità di un insieme: data la stringa $u \in \Sigma$ indichiamo con $|w|$ la sua lunghezza.

[3] Le sequenze che iniziano col simbolo del *backslash* o *barra rovesciata* \ sono dette sequenze di escape. La barra rovesciata viene usata per indicare che il simbolo immediatamente successivo, in questo caso il carattere '`w`', deve essere interpretato in modo speciale.

[4] Nelle espressioni Javascript quando il punto non è preceduto dalla barra rovesciata viene interpretato come un carattere speciale che sta ad indicare "qualunque carattere".

ESEMPIO 5.5 (LUNGHEZZA DI STRINGHE)
- *L'unica stringa di lunghezza* 0 *è la stringa vuota:* $|\varepsilon| = 0$
- *Data la stringa "matematica"* $\in \Sigma_A$ *si ha* $|\text{matematica}| = 10$.
- *Data la stringa* $00001100 \in \Sigma_{\mathbb{B}}$ *si ha* $|00001100| = 8$.

DEFINIZIONE 5.3 (POTENZE DI UN ALFABETO)
Dato un alfabeto Σ *e un numero naturale* $k \in \mathbb{N}$*, chiamiamo:*

- Σ^k *l'insieme delle stringhe di lunghezza* k *su* Σ*;*
- Σ^* *l'insieme di tutte le stringhe su* Σ*, cioè* $\Sigma^* = \Sigma^0 \cup \Sigma^1 \cup \Sigma^2 \cup \Sigma^3 \cup \cdots$
- Σ^+ *l'insieme di tutte le stringhe non vuote su* Σ*, cioè* $\Sigma^+ = \Sigma^1 \cup \Sigma^2 \cup \Sigma^3 \cup \cdots$

Dalla definizione data segue ovviamente che $\Sigma^* = \Sigma^0 \cup \Sigma^+$

ESEMPIO 5.6 (POTENZE DELL'ALFABETO BINARIO)
Se consideriamo l'alfabeto binario abbiamo, per esempio:

- $\Sigma^0_{\mathbb{B}} = \{\varepsilon\}$.
- $\Sigma^1_{\mathbb{B}} = \{0, 1\}$.
- $\Sigma^2_{\mathbb{B}} = \{00, 01, 10, 11\}$.

DEFINIZIONE 5.4 (LINGUAGGI)
Un linguaggio L *sull'alfabeto* Σ *è un sottoinsieme* $L \subseteq \Sigma^*$ *delle stringhe su* Σ.

Il linguaggio vuoto, scritto $\varnothing$, è diverso dal linguaggio che comprende la sola stringa vuota, scritto $\{\varepsilon\}$.

ESEMPIO 5.7 (LINGUAGGI)
- *L'insieme delle parole italiane è un linguaggio sull'alfabeto* Σ_A.
- *L'insieme delle parole inglesi è un linguaggio sull'alfabeto* Σ_A.
- *L'insieme delle stringhe che comprendono un numero pari di* 0 *e un numero pari di* 1 *è un linguaggio sull'alfabeto* $\Sigma_{\mathbb{B}}$.

$$\{\varepsilon, 00, 11, 0011, 0101, 0110, 1100, 1010, 1001, 001111, 000011, \ldots\}$$

- *L'insieme delle stringhe che comprendono lo stesso numero di* 0 *e di* 1 *è un linguaggio sull'alfabeto* $\Sigma_{\mathbb{B}}$.

$$\{\varepsilon, 01, 10, 0011, 0101, 0110, 1100, 1010, 1001, 000111, \ldots\}$$

Dato che i linguaggi sono insiemi, possiamo applicare loro tutte le operazioni su insiemi viste nel Capitolo 2: intersezione, unione, differenza e complemento. Ovviamente, il risultato dell'applicazione di operazioni insiemistiche a linguaggi su Σ è ancora un linguaggio su Σ. In particolare, il complemento di un linguaggio $L \subseteq \Sigma^*$ è definito rispetto all'universo $\mathcal{U} = \Sigma^*$.

Ci sono altre operazioni specifiche dei linguaggi basate sul concetto di **concatenazione di stringhe**: date due stringhe $u, v \in \Sigma^*$, indichiamo con (uv) la stringa ottenuta per giustapposizione di u e v, la cui lunghezza è $|(uv)| = |u| + |v|$. Più precisamente, se $u = a_1 a_2 \ldots a_h$ e $v = b_1 b_2 \ldots b_k$ allora $(uv) = c_1 c_2 \ldots c_{h+k}$ con

$$c_i = \begin{cases} a_i & \text{se } 1 \leq i \leq h \\ b_{i-h} & \text{se } h < i \leq h+k \end{cases}$$

ESEMPIO 5.8 (CONCATENAZIONE DI STRINGHE BINARIE)
Date le stringhe $u = 01101$ *e* $v = 110$ *su* $\Sigma_{\mathbb{B}}$ *si ha* $uv = 01101110$ *e* $vu = 11001101$*. Inoltre* $u\varepsilon = 01101 = \varepsilon u$.

DEFINIZIONE 5.5 (OPERAZIONI SU LINGUAGGI)
Siano L e M due linguaggi sullo stesso alfabeto Σ.

- *La **concatenazione** di L con M, scritta $L \cdot M$, è il linguaggio che comprende tutte e sole le stringhe ottenute concatenando una stringa di L con una di M. In formule, $L \cdot M = \{ w \mid \exists u \in L.\ \exists v \in M.\ w = (uv) \}$.*
- *La **potenza k-esima** di L, scritta L^k, è il linguaggio che comprende tutte e sole le stringhe ottenute concatenando k stringhe di L. In formule, $L^k = \{ w \mid \exists u_1, u_2, \ldots, u_k \in L.\ w = (u_1(u_2(\ldots u_k))) \}$. In particolare si ha: $L^0 = \{\varepsilon\}$, $L^1 = L$ e $L^{k+1} = L \cdot L^k$ per ogni $k \geq 0$.*
- *La **chiusura di Kleene** di L, scritta L^*, è il linguaggio che comprende tutte e sole le stringhe ottenute concatenando un numero arbitrario, anche nullo, di stringhe di L, cioè $L^* = L^0 \cup L^1 \cup L^2 \cup \ldots$*
- *L^+ è il linguaggio che comprende tutte e sole le stringhe ottenute concatenando un numero arbitrario, non nullo, di stringhe di L, cioè $L^+ = L^1 \cup L^2 \cup \ldots$*

ESEMPIO 5.9 (OPERAZIONI SU LINGUAGGI)
Vediamo alcuni esempi dell'applicazione degli operatori di concatenazione e di chiusura di Kleene:

- $\varnothing \cdot \{0,1,01\} = \varnothing$
- $\{\varepsilon\} \cdot \{0,1,01\} = \{0,1,01\}$
- $\{\varepsilon,1\} \cdot \{0,1,01\} = \{0,1,01,10,11,101\}$
- $\{\varepsilon,0,1\}^2 = \{0,1,00,01,10,11\}$
- $\{0\}^* = \{\varepsilon,0,00,000,\ldots\}$
- $\{0\}^+ = \{0,00,000,\ldots\}$

5.3 Le espressioni regolari

Le *espressioni regolari* sono espressioni simboliche che servono a rappresentare un particolare tipo di linguaggi, chiamati *linguaggi regolari*. Ad esempio il linguaggio delle stringhe di parentesi bilanciate non è regolare. Preso un linguaggio $L \subseteq \Sigma^*$, non sarà dunque sempre possibile esprimerlo sempre mediante un'espressione regolare. La classe dei linguaggi regolari comprende, per esempio, il linguaggio vuoto $\varnothing$, il linguaggio formato dalla sola stringa vuota $\{\varepsilon\}$, tutti i linguaggi che contengono un numero finito di stringhe, e anche alcuni linguaggi infiniti, come mostrato nell'Esempio 5.11.

Le espressioni regolari sono formate a partire dai simboli dell'alfabeto Σ di riferimento più $\varnothing$ e ε utilizzando le operazioni di unione, concatenazione e chiusura di Kleene. Intuitivamente:

- ciascun simbolo $a \in \Sigma$ rappresenta il linguaggio con un solo elemento $\{a\}$;
- il simbolo $\varnothing$ rappresenta il linguaggio vuoto;
- il simbolo ε rappresenta il linguaggio singoletto $\{\varepsilon\}$;
- l'operatore $+$ rappresenta l'unione di linguaggi;
- la giustapposizione di espressioni rappresenta la concatenazione di linguaggi;
- la stella di Kleene rappresenta l'operazione di chiusura di Kleene.

DEFINIZIONE 5.6 (ESPRESSIONI REGOLARI)
*Dato un alfabeto Σ, le **espressioni regolari** su Σ sono tutte e sole quelle ottenibili con le seguenti regole:*

1. *ε e $\varnothing$ sono espressioni regolari.*
2. *Se $a \in \Sigma$, allora a è un'espressione regolare.*

3. *Se e e f sono espressioni regolari, allora*

$$(e+f) \qquad (ef) \qquad (e^\star)$$

sono espressioni regolari.

A ciascuna espressione regolare e viene associato un linguaggio $L(e)$, calcolato seguendo le regole elencate sotto che ispezionando la natura dell'espressione e indicano come calcolare il risultato:

$$\begin{array}{rcl} L(\{\varepsilon\}) & = & \{\varepsilon\} \\ L(\varnothing) & = & \varnothing \\ L(a) & = & \{a\} \\ L(f+g) & = & L(f) \cup L(g) \\ L(fg) & = & L(f) \cdot L(g) \\ L(f^*) & = & L(f)^* \end{array}$$

ESEMPIO 5.10 (LINGUAGGI ASSOCIATI AD ALCUNE ESPRESSIONI REGOLARI)
Di seguito mostriamo i linguaggi che corrispondono ad alcune semplici espressioni regolari su $\Sigma_{\mathbb{B}}$:

- $L(0+1) = \{0,1\}$
- $L((\varepsilon+1)(0+1)) = \{0,1,10,11\}$
- $L(01) = \{01\}$
- $L((0^*)+(1^*)) = \{\varepsilon,0,1,00,11,000,111,...\}$
- $L((01)^*) = \{\varepsilon,01,0101,010101,...\}$

ESEMPIO 5.11 (IL LINGUAGGIO FORMATO DA TUTTE LE STRINGHE BINARIE DOVE SI ALTERNANO 0 E 1)
Supponiamo di voler caratterizzare con un'espressione regolare il linguaggio formato da tutte le stringhe binarie dove si alternano 0 e 1. Cioè vogliamo trovare un'espressione regolare e tale che:

$$L(e) = \{\, u \mid u \in \Sigma_{\mathbb{B}}^* \text{ con 0 e 1 che si alternano in } u\}$$

Cerchiamo di arrivare alla soluzione per passi successivi, costruendo delle espressioni regolari che si avvicinano ogni volta di più a catturare esattamente il linguaggio cercato:

- $e_1 = (01)^*$ *non va del tutto bene, perché anche se comprende solo sequenze ammissibili, scarta tutte le sequenze che iniziano con 1: per esempio $10 \notin L(e_1)$.*
- $e_2 = (0+1)(0+1)^*$ *non va assolutamente bene, perché oltre a sequenze corrette comprende anche sequenze dove 0 e 1 non si alternano: per esempio $00 \in L(e_2)$.*
- $e_3 = (e_1 + (1e_1)) = (((01)^*) + (1((01)^*)))$ *non va ancora bene, perché anche se comprende solo sequenze ammissibili, scarta le sequenze che terminano con 0: per esempio $0 \notin L(e_3)$ e $010 \notin L(e_3)$.*
- $e_4 = (e_3 + (e_3 0)) = ((((01)^*) + (1((01)^*))) + ((((01)^*) + (1((01)^*)))0))$ *cattura esattamente il linguaggio cercato.*

L'espressione e_4 non è però l'unica espressione che offre una soluzione corretta al problema. Per esempio, l'espressione

$$e_5 = (((\varepsilon+1)((01)^*))(\varepsilon+0))$$

è tale che $L(e_5) = L(e_4)$.

NOTA 5.12 (ORDINE DI PRECEDENZA PER GLI OPERATORI) *Le espressioni regolari offrono un modo di descrivere un linguaggio regolare con una notazione compatta. La presenza di parentesi appesantisce troppo la notazione. Al fine di migliorare la leggibilità delle espressioni, in seguito ipotizzeremo che la chiusura abbia precedenza sulle altre operazioni e che la concatenazione abbia precedenza sull'unione. Per esempio, in questo modo potremo scrivere semplicemente 01^*+1 invece che $((0(1^*))+1)$. Questa convenzione è del tutto analoga a quella delle espressioni aritmetiche, con l'elevamento a potenza che gioca il ruolo della stella di Kleene, del prodotto che gioca il ruolo della concatenazione e della somma che gioca il ruolo dell'unione.*

Nella pratica ci si trova spesso a scrivere espressioni regolari del tipo "una o nessuna istanza di e", "una o più istanze consecutive di e", "esattamente n istanze consecutive di e", o "un numero di istanze consecutive di e che varia tra n e m", per una data espressione e e naturali n e m. Questi casi sono talmente frequenti che è stata introdotta una notazione *ad hoc* basata su operatori derivati.

DEFINIZIONE 5.7 (OPERATORI DERIVATI)
Data un'espressione e e due naturali n,m usiamo le seguenti abbreviazioni:

- $e^? = \varepsilon + e$ *(una o nessuna istanza di e).*
- $e^+ = e(e^*)$ *(una o più istanze consecutive di e).*
- $e^n = \underbrace{ee...e}_{n \text{ volte}}$ *(esattamente n istanze consecutive di e).*
- $e^{\{n,m\}} = e^n + e^{n+1} + ... + e^m$ *(un numero di istanze consecutive di e che varia tra n e m).*

5.4 Dimostrare uguaglianze delle espressioni regolari

Come per le espressioni aritmetiche, insiemi e predicati, esistono delle leggi algebriche molto utili anche per le espressioni regolari. In questo caso le leggi devono preservare il linguaggio associato all'espressione: in accordo al principio di sostituzione questo ci permetterà di semplificare delle espressioni sostituendo uguali con uguali e senza alterare il linguaggio associato.

DEFINIZIONE 5.8 (EQUIVALENZA SEMANTICA DELLE ESPRESSIONI REGOLARI)
*Due espressioni regolari e e f sono **equivalenti**, scritto $e = f$, se e solo se $L(e) = L(f)$.*

PROPOSIZIONE 6 (ALCUNE LEGGI PER L'EQUIVALENZA DI ESPRESSIONI REGOLARI)
Per tutte le espressioni regolari e, f e g valgono le seguenti equivalenze:

Leggi su unione e concatenazione		
$e + \varnothing = e$	$\varepsilon e = e \quad e\varepsilon = e$	*(elemento neutro)*
$e + e = e$	$\varnothing e = \varnothing \quad e\varnothing = \varnothing$	*(idempotenza e elemento assorbente)*
$e + f = f + e$		*(commutatività)*
$e + (f + g) = (e + f) + g$	$e(fg) = (ef)g$	*(associatività)*
$e(f + g) = ef + eg$	$(e + f)g = eg + fg$	*(distributività)*

Leggi su stella di Kleene		
$\varnothing^* = \varepsilon$	$\varepsilon^* = \varepsilon$	*(chiusure notevoli)*
$(e^*)^* = e^*$	$ee^* = e^*e$	*(idempotenza e scambio)*
$e^* = \varepsilon + e^*e$	$(\varepsilon + e)^* = e^* \quad e^*e^* = e^*$	*(unfolding e assorbimento)*

ESEMPIO 5.13 (PRECEDENZA DEGLI OPERATORI E NOTAZIONE COMPATTA)
Sfruttando la precedenza degli operatori e le leggi di associatività e commutatività, le espressioni regolari e_4 e e_5 dell'esempio 5.11 possono essere trascritte come:

$$e_4 = (01)^* + 1(01)^* + (01)^*0 + 1(01)^*0 \qquad e_5 = (\varepsilon + 1)(01)^*(\varepsilon + 0)$$

ESEMPIO 5.14 (PROVE DI EQUIVALENZA DI ESPRESSIONI REGOLARI)
Dimostriamo per sostituzione che $(\varepsilon + 1)(01)^*(\varepsilon + 0) = (01)^* + 1(01)^* + (01)^*0 + 1(01)^*0$

$$
\begin{array}{ll}
 & \underline{(\varepsilon+1)(01)^*}(\varepsilon+0) \\
= & \quad \{ \textit{(distributività)} \} \\
 & (\underline{\varepsilon(01)^*}+1(01)^*)(\varepsilon+0) \\
= & \quad \{ \textit{(elemento neutro)} \} \\
 & ((01)^*+1(01)^*)(\varepsilon+0) \\
= & \quad \{ \textit{(distributività)} \} \\
 & \underline{((01)^*+1(01)^*)\varepsilon}+((01)^*+1(01)^*)0 \\
= & \quad \{ \textit{(elemento neutro)} \} \\
 & ((01)^*+1(01)^*)+\underline{((01)^*+1(01)^*)0} \\
= & \quad \{ \textit{(distributività) e (associatività)} \} \\
 & (01)^*+1(01)^*+(01)^*0+1(01)^*0
\end{array}
$$

5.5 Espressioni regolari in Javascript

Senza pretesa di completezza, ecco alcune delle notazioni e delle classi di caratteri esprimibili in modo compatto in Javascript, alcune già anticipate nel capitolo:

- il simbolo . rappresenta un *qualunque carattere dell'alfabeto*, cioè è l'espressione regolare che cattura il linguaggio che comprende (tutte e sole) le stringhe di lunghezza 1;
- la coppia di parentesi quadre applicata a una sequenza di simboli $[\mathtt{a_1a_2...a_k}]$ rappresenta l'espressione regolare $a_1+a_2+...+a_k$, alla quale corrisponde il linguaggio $\{a_1,a_2,,a_k\}$;
- esistono anche notazioni *ad hoc* per esprimere le classi di caratteri più comuni:
  - \w rappresenta la classe di tutti i caratteri alfanumerici e il trattino basso,
  - \d rappresenta la classe di tutte le cifre numeriche,
  - _ rappresenta la classe di tutti i caratteri di spaziatura;
- $\mathtt{e_1}|\mathtt{e_2}$ indica l'espressione regolare e_1+e_2, cioè il linguaggio ottenuto dall'unione dei linguaggi di e_1 e e_2;
- $\mathtt{e_1e_2}$ indica l'espressione regolare e_1e_2, cioè il linguaggio ottenuto dalla concatenazione dei linguaggi di e_1 e e_2;
- e{n} denota il pattern composto da n copie del pattern e, ed equivale quindi all'espressione regolare e^n;
- e{n,m} denota il pattern composto da un minimo di n ad un massimo di m copie del pattern exp, ed equivale quindi all'espressione regolare $e^{\{n,m\}}$;
- e? denota il pattern composto da *zero oppure una* copia del pattern e, ed equivale quindi all'espressione regolare $e+\varepsilon$;
- e$*$ denota il pattern composto da *zero oppure più di una* copia del pattern e, ed equivale quindi all'espressione regolare e^*;
- e+ denota il pattern composto da *una oppure più di una* copia del pattern e, ed equivale quindi all'espressione regolare e^+.

ESEMPIO 5.15 (SPERIMENTAZIONE CON LA RICERCA DI ESPRESSIONI REGOLARI)
Potete adesso sperimentare con le espressioni regolari Javascript collegandovi, ad esempio, alla pagina

http://regexpal.com/

5.6 Esercizi

5.6.1 Esercizi di comprensione

5.6.1.1 Quante stringhe ci sono in $\Sigma_{\mathbb{B}}^3$? Qual è la loro lunghezza?

5.6.1.2 È vero che $\varepsilon \in \Sigma_{\mathbb{B}}^1$?

5.6.1.3 È vero che $\varepsilon \in \Sigma_{\mathbb{B}}^+$?

5.6.1.4 È vero che $\varepsilon \in \Sigma_{\mathbb{B}}^*$?

5.6.1.5 Quante stringhe ci sono in $\Sigma^1 \cap \Sigma^2 \cap \ldots$?

5.6.1.6 Dato un alfabeto Σ che contiene n simboli e dato $k \in \mathbb{N}$, quante stringhe contiene la potenza Σ^k di Σ?

5.6.1.7 È vero che ogni linguaggio regolare contiene solo un numero finito di stringhe?

5.6.1.8 È vero che tutti i linguaggi sono regolari?

5.6.1.9 È vero che ogni linguaggio regolare è identificato da un'unica espressione regolare?

5.6.1.10 È vero che un'espressione regolare può generare tanti linguaggi diversi?

5.6.1.11 È vero che la stringa vuota appartiene al linguaggio vuoto? ($\varepsilon \in \varnothing$?)

5.6.2 Esercizi di approfondimento

5.6.2.1 Quali sono i linguaggi associati alle seguenti espressioni regolari su $\Sigma_{\mathbb{B}}$?

(a) $\varnothing^* + \varepsilon^*$
(b) $0(1+0)^*$
(c) $(0^* + 1^* + 01)0^*1^*(0^* + 1^* + 10)$
(d) $((\varnothing^* + 0)^* + 0)^*$
(e) $1(\varepsilon + 0 + 1)1$

5.6.2.2 Scrivere le espressioni regolari su $\Sigma_{\mathbb{B}}$ per rappresentare i seguenti linguaggi di stringhe binarie:

(a) il linguaggio di tutte e sole le stringhe senza 0
(b) il linguaggio di tutte e sole le stringhe dove 0 non precede mai 1
(c) il linguaggio di tutte e sole le stringhe senza due 0 consecutivi
(d) il linguaggio di tutte e sole le stringhe con almeno tre 1
(e) il linguaggio di tutte e sole le stringhe dove 0 non segue mai 1.

5.6.2.3 Scrivere le espressioni regolari necessarie per descrivere:

(a) il codice fiscale di una persona
(b) una URL
(c) una data in formato dd/mm/aaaa
(d) tutti i numeri naturali divisibili per due o per cinque
(e) tutti i numeri naturali divisibili per due e per cinque.

5.6.3 Esercizi che coinvolgono dimostrazioni per sostituzione

5.6.3.1 Dimostrare che per ogni espressione regolare e, f, g valgono le seguenti equivalenze:

(a) $L(e^*) = L(\varepsilon + e + e^*)$

(b) $L(ef^*g) = L(eg + ef^*fg)$

(c) $L((f^* + g^*)e) = L(e + ge + f^*e + g^*e)$

(d) $L(f(\varepsilon + e)^*) = L(f(e^*)^*)$

5.6.3.2 Dimostrare le seguenti equivalenze usando il principio di sostituzione e le leggi delle espressioni regolari (ipotizziamo che l'alfabeto di riferimento sia $\Sigma_{\mathbb{B}}$):

(a) $\varnothing^*\varepsilon + \varepsilon\varepsilon^* = \varepsilon$

(b) $0(0^* + 1^*(0^* + 1^*))0^* = 0^*0 + 01^*0^* + 01^*0^*$

(c) $(01^* + 10^*)(0^* + 1^*) = 01^*0^* + 10^* + 01^* + 10^*1^*$

(d) $\varepsilon(0^* + 1(0^* + 1^*)) = (\varepsilon + 1)(1 + \varepsilon)(0^* + 1^*)$