Logica Matematica

Sonia L'Innocente
sonia.linnocente@unicam.it

Per la stesura di queste note, si ringraziano

Prof. **Alessandro Andretta** (Università di Torino, Dipartimento di Matematica)
Prof. **Felice Cardone** (Università di Torino, Dipartimento di Matematica)
e il Dipartimento di Informatica dell'Università di Torino.

Indice

CAPITOLO I

Costanti logiche

Le conoscenze alle quali pervengono le scienze esatte si esprimono generalmente in forma di **proposizioni**, frasi dichiarative con il verbo all'indicativo; per esempio:

(1) l'equazione $x^2 = 2$ non ha soluzioni razionali.

Analogamente, in informatica possiamo esprimere la correttezza di un algoritmo a di ordinamento di vettori mediante la proposizione:

(2) per ogni vettore v, l'algoritmo a produce una permutazione degli elementi di v ordinata in ordine crescente.

Una caratteristica delle proposizioni è che hanno un **valore di verità**, cioè possono essere **vere** o **false**. Quindi non considereremo frasi del linguaggio comune che non ammettano un valore di verità definito.

La matematica e l'informatica si differenziano dalle altre discipline scientifiche per il metodo con cui vengono stabiliti i nuovi risultati. Non è sufficiente — e, nella stragrande maggioranza dei casi, neppure necessario — effettuare misurazioni, esperimenti o simulazioni. Nessun esperimento può decidere la verità o falsità di (1), cioè se $\sqrt{2}$ sia o meno un numero razionale: è necessario **dimostrare** che non esistono numeri interi n e m tali che $n^2 = 2m^2$ (vedi Teorema 2.1). Analogamente non è sufficiente aver verificato empiricamente la correttezza dell'algoritmo a di (2) in un numero finito (anche grandissimo) di casi. In alcuni casi, gli esempi e i conti possono fornire *indizi* sulla verità o meno di una congettura, ma questi computi non ci consentono di stabilire la verità o la falsità della congettura. Anzi: a volte, l'evidenza numerica può essere molto fuorviante. Vediamo qualche esempio.

ESEMPI 0.1.(a) Consideriamo i numeri della forma $2^{2^n} + 1$. Per $n = 0, 1, 2, 3$ e 4 si ottengono i numeri

$$2^{2^0} + 1 = 3, \quad 2^{2^1} + 1 - 5, \quad 2^{2^2} + 1 = 17, \quad 2^{2^3} + 1 = 257, \quad 2^{2^4} + 1 = 65537$$

che sono tutti primi. Fermat congetturò che *tutti* i numeri della forma $2^{2^n} + 1$ fossero primi, ma Eulero, un secolo dopo verificò che

$$2^{2^5} + 1 = 4292967297 = 641 \times 6700417.$$

Quindi *non tutti* i numeri della forma $2^{2^n} + 1$ sono primi.

(b) Dmitri Grave congetturò che tutti i numeri della forma $2^{p-1} - 1$ non fossero divisibili per p^2, con p primo. Questa congettura è vera per tutti i primi

$p < 1000$, tuttavia 1093 è primo ma $2^{1092} - 1$ è divisibile per 1093^2. Quindi la congettura è falsa.

(c) La proprietà $P(n)$ definita da "$n^2 - 79n + 1601$ è primo" è vera per $1 \leq n < 80$ ma è falsa per $n = 80$ dato che $80^2 - 79 \times 80 + 1601 = 1681 = 41^2$.

(d) Il primo n per cui $991n^2 + 1$ è un quadrato perfetto è un numero di 29 cifre!

Una **dimostrazione** è un ragionamento che a partire da alcune affermazioni iniziali ci permette di concludere il risultato desiderato. Una dimostrazione ha l'aspetto di una serie di proposizioni concatenate in modo tale che la conclusione (la proposizione da dimostrare) sia fatta dipendere da altre proposizioni mediante **inferenze**. La logica analizza la struttura delle dimostrazioni formalizzandole come **derivazioni**, strutture di formule costruite in accordo con le regole di inferenza opportunamente riformulate in modo da operare su quei particolari oggetti simbolici che sono le formule.

La logica analizza queste proposizioni scomponendole in elementi che appartengono ad un numero ristretto di categorie grammaticali, mettendone in evidenza la struttura mediante una traduzione in **formule** di un opportuno **linguaggio formale**. I linguaggi formali sono necessari per evitare le ambiguità del linguaggio comune (si veda il Capitolo VI). L'uso di un apparato simbolico ci permette di descrivere in modo preciso la struttura delle proposizioni e ci permette di descrivere in maniera sintetica concetti che altrimenti risulterebbero oscuri. È una situazione analoga a quanto avviene in algebra — è molto più semplice enunciare

$$(a + b)^2 = a^2 + 2ab + b^2$$

che dire

> la somma di due numeri moltiplicata per sé stessa è uguale al primo numero moltiplicato per sé stesso sommato al secondo numero moltiplicato per sé stesso e poi ancora sommato al doppio del prodotto dei due numeri.

1. Introduzione alla logica

1.A. Simboli. Quando facciamo matematica fissiamo sempre, in modo implicito o esplicito, un linguaggio in cui i teoremi, le congetture, le dimostrazioni, ecc. sono formulati. Se scorriamo un testo di matematica potremmo imbatterci in vari tipi di simboli.

- Le lettere x, y, z, ... in genere designano numeri reali arbitrari, mentre le lettere k, m, n, ... denotano numeri naturali.
- Invece certe lettere designano numeri ben specifici — per esempio la lettera π è il rapporto tra la lunghezza del diametro e la lunghezza della circonferenza $\pi = 3{,}14159\ldots$.
- I simboli $+$, $\cdot$ denotano le operazioni binarie di somma e prodotto, che non sono altro che specifiche funzioni da coppie di reali a valori reali.
- Il simbolo $\leq$ denota la relazione d'ordine.

Naturalmente il significato dei simboli $+$, $\cdot$ e $\leq$ può cambiare a seconda del testo in questione. Per esempio $+$ e $\cdot$ potrebbero essere le operazioni di somma e prodotto di matrici, e non di numeri naturali, e il simbolo $\leq$ potrebbe designare un tipo di ordinamento più sofisticato di quello a cui siamo abituati a considerare.... Anche le variabili x, y, z, ... potrebbero denotare un generico elemento nel nostro universo (per esempio una matrice, un vettore, ecc.) piuttosto che un numero reale. Ma se c'è un simbolo sulla cui interpretazione concordiamo tutti, questo è proprio il simbolo di uguaglianza $=$, che asserisce che l'oggetto scritto a sinistra del segno di uguale coincide con l'oggetto scritto a destra.

Ci sono poi alcune espressioni che ricorrono in ogni testo matematico:

- "per ogni x..."
- "c'è almeno un x tale che ..."
- "se... allora ..."
- "... se e solo se ..."
- le particelle "non", "e", "o".

Per scrivere in modo non ambiguo i ragionamenti e le dimostrazioni sono stati introdotti dei simboli noti come **connettivi logici**

$$\neg \qquad \vee \qquad \wedge \qquad \to \qquad \leftrightarrow$$

ed i simboli di **quantificatore**

$$\exists \qquad \forall.$$

I connettivi e i quantificatori si dicono **costanti logiche**, di cui ora vediamo il significato.

- $\neg$ denota la **negazione** e serve per affermare l'opposto di quanto asserisce l'affermazione a cui si applica. Per esempio
$$\neg(x < y)$$
significa che x non è minore di y.
- $\vee$ è la **disgiunzione** e corrisponde al *vel* latino: questo *o* quello *o* eventualmente entrambi. Se asseriamo che
$$(x \text{ è pari}) \vee (x \text{ è un quadrato perfetto})$$
intendiamo dire che il numero x può essere pari (cioè della forma $2n$, per esempio 6), o un quadrato perfetto (cioè della forma n^2, per esempio 9), o magari un numero che è un quadrato perfetto pari (cioè della forma $4n^2$, per esempio 4).
- $\wedge$ è la **congiunzione** e serve per asserire che due fatti valgono contemporaneamente. Per esempio
$$(x \text{ è pari}) \wedge (x \text{ è un quadrato perfetto})$$
significa che il numero x è della forma $4n^2$, per qualche n. Anche le particelle "ma" e "però" sono delle congiunzioni, a cui noi attribuiamo una connotazione avversativa. Resta il fatto che in matematica il significato

di "A ma B" o di "A però B" è lo stesso di "A e B" e quindi si scrivono come "$A \wedge B$".

- $\to$ è l'**implicazione** e corrisponde all'espressione "se... allora ...". Quando in matematica asseriamo che "se A allora B", stiamo affermando che l'unico caso problematico è quando la premessa A vale e la conseguenza B non vale. In particolare, se la premessa è falsa possiamo concludere che l'implicazione vale. Per esempio se vediamo scritto

$$(x > 0) \to (x = y^2 \text{ per qualche } y > 0)$$

siamo d'accordo che questa implicazione vale, dato che o x è positivo e quindi ha una radice positiva, oppure è negativo o nullo e quindi non c'è nulla da dire. Un'implicazione non sottintende nessuna relazione di causalità tra la premessa e la conseguenza — l'unico significato di $A \to B$ è che non è possibile che A valga e B no. Le espressioni "affinché valga A deve valere B" oppure "affinché valga A è necessario che valga B" significano che "se A allora B" e quindi si scrivono $A \to B$, mentre "affinché valga A è sufficiente che valga B" significa che A vale quando B vale, cioè $B \to A$.
- $\leftrightarrow$ è il **bi-condizionale** o **bi-implicazione** e corrisponde all'espressione "se e solo se". Quando asseriamo che "A se e solo se B" intendiamo dire che "se A allora B, e se B allora A". Spesso in matematica "A se e solo se B" lo si scrive, in modo più ampolloso, come "condizione necessaria e sufficiente affinché valga A, è che valga B".
- $\exists$ è il **quantificatore esistenziale**. L'espressione $\exists x A$ si legge: "c'è un x tale che A", ovvero "A vale, per qualche x" e asserisce che c'è *almeno un* ente che gode della proprietà A.
- $\forall$ è il **quantificatore universale**. L'espressione $\forall x A$ si legge: "per ogni x vale A", ovvero "A vale, per tutti gli x" e asserisce che *ogni* ente gode della proprietà A.

1.B. Inferenze. La logica può essere vista come lo studio del ragionamento corretto: vogliamo studiare (tra l'altro) come passare in modo corretto da certe proposizioni (le **premesse**) a certe altre proposizioni (le **conclusioni**) usando **inferenze** logicamente corrette. I passi elementari di questo processo di derivazione di conseguenze sono costituite da **regole** (di inferenza) della forma

$$\frac{A_1 \qquad A_2 \qquad \dots \qquad A_n}{B}$$

dove $A_1, \dots, A_n$ e B sono proposizioni che esprimono il fatto che la conclusione B può essere inferita dalle premesse $A_1, \dots, A_n$.

Nelle prossime pagine analizzeremo più in dettagli il significato dei connettivi e dei quantificatori.

2. Connettivi

Il significato dei vari connettivi logici è completamente descritto da delle tabelle note come **tavole di verità**: si introducono due oggetti **V** e **F** che

denotano il *vero* e il *falso*, rispettivamente, e per ogni connettivo si definisce una tabella che lo caratterizza completamente.

Cominciamo col connettivo $\neg$: la sua tavola di verità è

A	$\neg$A
V	**F**
F	**V**

Si vede subito che A e $\neg\neg$A hanno la stessa tavola di verità,

(3)

A	$\neg$A	$\neg\neg$A
V	**F**	**V**
F	**V**	**F**

Quindi da A possiamo ricavare $\neg\neg$A e viceversa:

$$\frac{\text{A}}{\neg\neg\text{A}} \qquad \text{e} \qquad \frac{\neg\neg\text{A}}{\text{A}} .$$

La tavola di verità di $\wedge$ è

A	B	A $\wedge$ B
V	**V**	**V**
V	**F**	**F**
F	**V**	**F**
F	**F**	**F**

Per dimostrare A $\wedge$ B è sufficiente dimostrare A e dimostrare B. Possiamo esprimere graficamente questo così

$$\frac{\text{A} \qquad \text{B}}{\text{A} \wedge \text{B}} .$$

Viceversa, da A $\wedge$ B possiamo dedurre tanto A quanto B, cioè

$$\frac{\text{A} \wedge \text{B}}{\text{A}} \quad \text{e} \quad \frac{\text{A} \wedge \text{B}}{\text{B}} .$$

Il connettivo $\wedge$ è commutativo, nel senso che la tavola di verità di A $\wedge$ B è la medesima di B $\wedge$ A. Quindi asserire A $\wedge$ B è come asserire B $\wedge$ A.

La tavola di verità per $\vee$ è

A	B	A $\vee$ B
V	**V**	**V**
V	**F**	**V**
F	**V**	**V**
F	**F**	**F**

Il connettivo $\vee$ è commutativo, nel senso che la tavola di verità di A $\vee$ B è la stessa di B $\vee$ A. Quindi asserire A $\vee$ B è come asserire B $\vee$ A.

Dimostrato A, possiamo indebolire il nostro risultato asserendo A $\vee$ B, dove B è un'affermazione qualsiasi. Analogamente, da B si deduce A $\vee$ B, per qualsiasi A. In simboli

$$\frac{\text{A}}{\text{A} \vee \text{B}} \qquad \text{e} \qquad \frac{\text{B}}{\text{A} \vee \text{B}} .$$

Invece a partire da $A \vee B$ non possiamo né concludere A né concludere B. D'altra parte, se sappiamo $A \vee B$ e se sappiamo negare una tra le due affermazioni A e B, allora possiamo concludere l'altra, cioè

$$\text{(4)} \qquad \frac{A \vee B \qquad \neg A}{B} \qquad \text{e} \qquad \frac{A \vee B \qquad \neg B}{A}\,.$$

È facile verificare che

$$A \wedge B \text{ e } \neg(\neg A \vee \neg B)$$

hanno la stessa tavola di verità, e così pure per

$$A \vee B \text{ e } \neg(\neg A \wedge \neg B).$$

Quindi:

$$\frac{A \wedge B}{\neg(\neg A \vee \neg B)} \quad \text{e} \quad \frac{A \vee B}{\neg(\neg A \wedge \neg B)}\,.$$

Le formule qui sopra sono note come **Leggi di De Morgan**.

La tavola di verità per l'implicazione è:

A	B	$A \to B$
V	**V**	**V**
V	**F**	**F**
F	**V**	**V**
F	**F**	**V**

È facile verificare che questa è anche la tavola di verità di $\neg A \vee B$, cioè

$$\frac{A \to B}{\neg A \vee B} \qquad \text{e} \qquad \frac{\neg A \vee B}{A \to B}.$$

Per la (3), la regola (4) può essere riformulata per l'implicazione così: da $A \to B$ e A possiamo dedurre B. Questa regola prende il nome di *Modus Ponens*:

$$\text{(MP)} \qquad \frac{A \to B \qquad A}{B}\,.$$

Infine utilizzando la regola della doppia negazione (3) è facile verificare che

$$\frac{A \to B}{\neg B \to \neg A}\,.$$

$\neg B \to \neg A$ si dice il **contrappositivo** di $A \to B$. Osserviamo che, a differenza della congiunzione e dalla disgiunzione, il connettivo $\to$ non commuta, cioè $A \to B$ non ha lo stesso significato di $B \to A$.

Il bi-condizionale $\leftrightarrow$ è definito come la congiunzione di due implicazioni, in simboli

$$\frac{A \leftrightarrow B}{A \to B} \qquad \text{e} \qquad \frac{A \leftrightarrow B}{B \to A}$$

e

$$\frac{A \to B \qquad B \to A}{A \leftrightarrow B}\,.$$

La sua tavola di verità è:

A	B	A $\leftrightarrow$ B
V	**V**	**V**
V	**F**	**F**
F	**V**	**F**
F	**F**	**V**

Il bi-condizionale è commutativo, cioè asserire A $\leftrightarrow$ B è come asserire B $\leftrightarrow$ A.

La **disgiunzione esclusiva** (corrispondente al latino *aut* e usualmente chiamata in informatica *xor*) "A oppure B, ma non entrambe", è denotata con

$$A \oplus B$$

e non è altro che un'abbreviazione di $(A \vee B) \wedge \neg(A \wedge B)$. La sua tavola di verità è:

A	B	A $\oplus$ B
V	**V**	**F**
V	**F**	**V**
F	**V**	**V**
F	**F**	**F**

È spesso più comodo utilizzare i simboli 1 e 0 invece dei simboli **V** e **F**. In questo caso le tavole di verità per la negazione ha la seguente forma

A	$\neg$A
0	1
1	0

e le tavole dei connettivi binari si scrivono così

A	B	A $\wedge$ B	A $\vee$ B	A $\rightarrow$ B	A $\leftrightarrow$ B	A $\oplus$ B
0	0	0	0	1	1	0
0	1	0	1	1	0	1
1	0	0	1	0	0	1
1	1	1	1	1	1	0

2..1. *Tautologie e conseguenza logica.* Ora che abbiamo visto i connettivi e le loro tavole logiche possiamo provare ad analizzare proposizioni più complesse. Fissiamo una famiglia di proposizioni elementari, che non possono essere ulteriormente analizzate mediante i connettivi. Queste proposizioni sono indicate con le lettere $A, B, C, \ldots$ eventualmente decorate con apici o pedici. Possiamo calcolare la tavola di verità di ciascuna proposizione costruita a partire dalle lettere — per esempio la tavola di verità di $(B \rightarrow A) \wedge ((B \vee C) \leftrightarrow A)$ è ottenuta a partire dalle tavole di verità di $B \rightarrow A$,

di $B \vee C$, e di $(B \vee C) \leftrightarrow A$:

A	B	C	$B \to A$	$B \vee C$	$(B \vee C) \leftrightarrow A$	$(B \to A) \wedge ((B \vee C) \leftrightarrow A)$
0	0	0	1	0	1	1
0	0	1	1	1	0	0
0	1	0	0	1	0	0
0	1	1	0	1	0	0
1	0	0	1	0	0	0
1	0	1	1	1	1	1
1	1	0	1	1	1	1
1	1	1	1	1	1	1

ESEMPIO 2.1. La tavola di verità di $(A \wedge \neg A) \to B$ è

A	B	$\neg A$	$A \wedge \neg A$	$(A \wedge \neg A) \to B$
0	0	1	0	1
0	1	1	0	1
1	0	0	0	1
1	1	0	0	1

ESEMPIO 2.2. Se P è $A \vee C \to \neg A \wedge (B \to C)$, la sua tavola di verità è:

A	B	C	$\neg A$	$B \to C$	$\neg A \wedge (B \to C)$	$A \vee C$	P
0	0	0	1	1	1	0	1
0	0	1	1	1	1	1	1
0	1	0	1	0	0	0	1
0	1	1	1	1	1	1	1
1	0	0	0	1	0	1	0
1	0	1	0	1	0	1	0
1	1	0	0	0	0	1	0
1	1	1	0	1	0	1	0

ESEMPIO 2.3. Le tavole di verità di $A \vee (B \wedge C)$ e $(A \vee B) \wedge (A \vee C)$ coincidono. Infatti

A	B	C	$B \wedge C$	$A \vee (B \wedge C)$	$A \vee B$	$A \vee C$	$(A \vee B) \wedge (A \vee C)$
1	1	1	1	1	1	1	1
1	1	0	0	1	1	1	1
1	0	1	0	1	1	1	1
1	0	0	0	1	1	1	1
0	1	1	1	1	1	1	1
0	1	0	0	0	1	0	0
0	0	1	0	0	0	1	0
0	0	0	0	0	0	0	0

Vediamo come le tavole di verità ci aiutino a risolvere alcuni rompicapo logici.

ESEMPIO 2.4. **Problema:** Consideriamo le seguenti proposizioni, dove le parentesi servono a chiarire la struttura:

- Né Alberto né Carlo sono buoni studenti;
- (Alberto è un buon studente se Davide lo è), oppure, (se (Davide oppure Elisabetta sono buoni studenti) allora (Carlo è un buon studente se e solo se Davide lo è)).

Nella situazione descritta dalle proposizioni qui sopra, Davide è un buon studente?

Soluzione: Abbreviamo con A, C, D ed E le proposizioni Alberto è un buon studente, ..., Elisabetta è una buona studentessa. Sappiamo che

$$\neg A \wedge \neg C \quad \text{e} \quad (D \to A) \vee ((D \vee E) \to (C \leftrightarrow D))$$

sono proposizioni vere. Dalla prima vediamo che A e C sono false. Supponiamo D sia vera: allora $D \vee E$ sarebbe vera e $C \leftrightarrow D$ falsa e quindi $(D \vee E) \to (C \leftrightarrow D)$ è falsa. D'altra parte $D \to A$ è falsa, quindi $(D \to A) \vee ((D \vee E) \to (C \leftrightarrow D))$ è falsa, contro la nostra ipotesi. Ne segue che D è falsa.

Una relazione di capitale importanza per la logica è quella di **conseguenza logica**. Per definirla, introduciamo una serie di nozioni utili per descrivere classi notevoli di proposizioni.

Definizione 2.5. Una **tautologia** o **proposizione logicamente vera** è una proposizione che è vera per ogni assegnazione di valori di verità alle lettere che contiene.

Una **contraddizione proposizionale** o **contraddizione** è una proposizione che è falsa per ogni assegnazione di valori di verità alle lettere che contiene.

In altre parole, una tautologia è una proposizione il cui valore di verità è sempre 1, in qualsiasi riga della tavola di verità, e A è una tautologia se e soltanto se $\neg A$ è una contraddizione proposizionale.

Definizione 2.6. Una proposizione è **soddisfacibile** se è vera per *qualche* assegnazione di valori di verità alle lettere che contiene.

Esempi 2.7. $\neg A \vee A$ è una tautologia, $\neg A \wedge A$ è una contraddizione, mentre $A \to B$ è soddisfacibile.

Definizione 2.8. Una proposizione B è **conseguenza tautologica** o, più semplicemente, **conseguenza logica** di proposizioni $A_1, \ldots, A_n$ se la proposizione

$$(A_1 \wedge \cdots \wedge A_n) \to B$$

è una tautologia.

Abbiamo un criterio per dire quando una regola di inferenza è logicamente corretta: la regola di inferenza

$$\frac{A_1 \qquad A_2 \qquad \ldots \qquad A_n}{B}$$

è **logicamente corretta** se e solo se B è una conseguenza logica di $A_1, \dots, A_n$. Per quanto detto prima, questo equivale a dire che la proposizione

$$(A_1 \wedge \cdots \wedge A_n) \to B$$

è una tautologia. Per esempio, la regola di inferenza del Modus Ponens

$$\frac{A \to B \qquad A}{B}$$

è logicamente corretta, dato che $((A \to B) \wedge A) \to B$ è una tautologia.

Le tautologie, in particolare quelle che sono nella forma di equivalenze o implicazioni, sono dette anche **leggi logiche**.

Un elenco di leggi logiche notevoli è presentato nella seguente lista:

legge dell'identità: $A \to A$
legge della doppia negazione: $A \leftrightarrow \neg\neg A$
commutatività di $\wedge$: $A \wedge B \leftrightarrow B \wedge A$
associatività di $\wedge$: $(A \wedge B) \wedge C \leftrightarrow A \wedge (B \wedge C)$
commutatività di $\vee$: $A \vee B \leftrightarrow B \vee A$
associatività di $\vee$: $(A \vee B) \vee C \leftrightarrow A \vee (B \vee C)$
idempotenza di $\wedge$: $A \wedge A \leftrightarrow A$
idempotenza di $\vee$: $A \vee A \leftrightarrow A$
eliminazione di $\wedge$: $A \wedge B \to A$
introduzione di $\vee$: $A \to A \vee B$
distributività: $A \wedge (B \vee C) \leftrightarrow (A \wedge B) \vee (A \wedge C)$
distributività: $A \vee (B \wedge C) \leftrightarrow (A \vee B) \wedge (A \vee C)$
legge di assorbimento: $A \wedge (A \vee B) \leftrightarrow A$
legge di assorbimento: $A \vee (A \wedge B) \leftrightarrow A$
legge di De Morgan: $\neg(A \wedge B) \leftrightarrow (\neg A \vee \neg B)$
legge di De Morgan: $\neg(A \vee B) \leftrightarrow (\neg A \wedge \neg B)$
legge del terzo escluso: $\neg A \vee A$
legge di non contraddizione: $\neg(A \wedge \neg A)$
legge di contrapposizione: $A \to B \leftrightarrow \neg B \to \neg A$
legge di Lewis, o *ex falso quodlibet*: $A \wedge \neg A \to B$
affermazione del conseguente: $A \to (B \to A)$
negazione dell'antecedente: $\neg A \to (A \to B)$
legge di riduzione all'assurdo: $(A \to B \wedge \neg B) \to \neg A$
riduzione all'assurdo debole: $(A \to \neg A) \to \neg A$
***consequentia mirabilis*:** $(\neg A \to A) \to A$
legge di Peirce: $((A \to B) \to A) \to A$
legge di Dummett: $(A \to B) \vee (B \to A)$
***modus ponens*:** $A \to ((A \to B) \to B)$
scambio antecedenti: $A \to (B \to C) \leftrightarrow B \to (A \to C)$
distinzione di casi: $(A \to C) \wedge (B \to C) \leftrightarrow A \vee B \to C$
distinzione di casi: $(A \to B) \wedge (\neg A \to B) \to B$
distributività di $\to$: $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$
transitività di $\to$: $(A \to B) \wedge (B \to C) \to (A \to C)$
importazione delle premesse: $A \to (B \to C) \leftrightarrow (A \wedge B) \to C$

Per verificare queste leggi, dove $\mathrm{A}, \mathrm{B}, \ldots$ sono qualunque, si devono prima verificare le stesse nel caso particolare che $\mathrm{A}, \mathrm{B}, \ldots$ siano atomiche (ad esempio $p \to p$ per la legge dell'identità), e poi sfruttare il fatto che se $\mathrm{A}[p]$ è una tautologia e B è qualunque, allora anche il risultato della sostituzione di B a p in A è una tautologia (vedi esercizi).

Per le leggi che nella tabella sono scritte come condizionali e non bicondizionali, si vedrà in seguito che l'implicazione inversa in generale non sussiste (salvo alcuni casi, ad esempio per l'inverso della riduzione all'assurdo debole, cioè $\neg\mathrm{A} \to (\mathrm{A} \to \neg\mathrm{A})$, che rientra nell'affermazione del conseguente).

L'associatività della congiunzione giustifica che si possa scrivere senza ambiguità, indipendentemente dalle convenzioni sulle parentesi, $\mathrm{A} \wedge \mathrm{B} \wedge \mathrm{C}$ per (indifferentemente) $\mathrm{A} \wedge (\mathrm{B} \wedge \mathrm{C})$ o $(\mathrm{A} \wedge \mathrm{B}) \wedge \mathrm{C}$, o in generale $\mathrm{A}_1 \wedge \ldots \wedge \mathrm{A}_n$ (e lo stesso per la disgiunzione). $\mathrm{A} \wedge (\mathrm{B} \wedge \mathrm{C})$ e $(\mathrm{A} \wedge \mathrm{B}) \wedge \mathrm{C}$ sono diverse (si disegni il loro albero sintattico) ma si dice che sono uguali **a meno di** equivalenza logica.

Anche le seguenti sono leggi logiche:

$$\mathrm{A} \to \mathrm{B} \leftrightarrow \neg\mathrm{A} \vee \mathrm{B}$$
$$(\mathrm{A} \leftrightarrow \mathrm{B}) \leftrightarrow (A \to \mathrm{B}) \wedge (\mathrm{B} \to \mathrm{A})$$
$$\mathrm{A} \oplus \mathrm{B} \leftrightarrow (\mathrm{A} \wedge \neg\mathrm{B}) \vee (\mathrm{B} \wedge \neg\mathrm{A})$$
$$\mathrm{A} \oplus \mathrm{B} \leftrightarrow (\mathrm{A} \vee \mathrm{B}) \wedge \neg(\mathrm{A} \wedge \mathrm{B}).$$

Si noti che le due leggi per $\oplus$ forniscono un esempio di come una particella logica possa essere espressa con diversi giri di frase equivalenti; queste equivalenze in genere mostrano cosa significa che frasi diverse vogliono dire la stessa cosa.

2.A. Esercizi.

Esercizio 2.9. Costruire la tavola di verità delle proposizioni:

- $(\mathrm{A} \to \mathrm{A}) \to \mathrm{A}$
- $\mathrm{A} \to (\mathrm{A} \to \mathrm{A})$
- $\mathrm{A} \vee \mathrm{B} \to \mathrm{A} \wedge \mathrm{B}$
- $\mathrm{A} \vee \mathrm{B} \wedge \mathrm{C} \to \mathrm{A} \wedge \mathrm{C} \vee \mathrm{D}$
- $(\mathrm{A} \vee \mathrm{B}) \wedge \mathrm{C} \to \mathrm{A} \wedge (\mathrm{C} \vee \mathrm{D})$
- $\mathrm{A} \to (\mathrm{B} \to \mathrm{A})$.

Esercizio 2.10. Verificare che $\mathrm{A} \wedge (\mathrm{B} \vee \mathrm{C})$ e $(\mathrm{A} \wedge \mathrm{B}) \vee (\mathrm{A} \wedge \mathrm{C})$ hanno le medesime tavole di verità.

Esercizio 2.11. Se Alberto ordina un caffè altrettanto fa Bice; Bice o Carlo, ma non entrambi, ordinano un caffè; Alberto o Carlo, o entrambi, ordinano un caffè. Se Carlo ordina un caffè, altrettanto fa Alberto. Chi ordina un caffè?

Esercizio 2.12. $(\mathrm{A} \to \mathrm{B}) \to (\mathrm{B} \to \mathrm{A})$ non è una tautologia, quindi

$$\frac{\mathrm{A} \to \mathrm{B}}{\neg\mathrm{A} \to \neg\mathrm{B}}$$

non è una regola di inferenza.

Invece

$$\frac{\mathrm{A} \to \mathrm{B}}{\neg \mathrm{B} \to \neg \mathrm{A}}$$

è una regola di inferenza.

3. Quantificatori

Lo studio dei quantificatori è essenzialmente più complesso dello studio dei connettivi. In particolare non c'è nessun analogo delle tavole di verità.

Quando scriviamo un'affermazione del tipo $\exists x\mathrm{A}$ o $\forall x\mathrm{A}$ implicitamente intendiamo che A stia affermando qualche proprietà di x. Se, per esempio, A è l'equazione $x^2+x=0$, l'espressione $\exists x\mathrm{A}$ dice che l'equazione data ammette una soluzione. Invece $\forall x\mathrm{A}$ dice che ogni numero è soluzione di A! Se invece A non dice nulla della variabile x, il significato di $\exists x\mathrm{A}$ e di $\forall x\mathrm{A}$ coincide con quello di A — per esempio $\exists x\exists y\left(y^2+y=0\right)$ e $\forall x\exists y\left(y^2+y=0\right)$ sono entrambe equivalenti a $\exists y\left(y^2+y=0\right)$. Negare $\forall x\mathrm{A}$ significa dire che non tutti gli x godono della proprietà descritta da A, cioè c'è almeno un x per cui si può asserire $\neg\mathrm{A}$. Viceversa, se neghiamo $\exists x\mathrm{A}$ allora vuol dire che non si dà il caso che ci sia un x per cui vale A, cioè per ogni x deve valere $\neg\mathrm{A}$. In simboli

$$\frac{\neg\forall x\mathrm{A}}{\exists x\neg\mathrm{A}} \qquad \text{e} \qquad \frac{\neg\exists x\mathrm{A}}{\forall x\neg\mathrm{A}}\,.$$

Quando scriviamo $\forall x\forall y\mathrm{A}$ intendiamo dire che in qualsiasi modo si scelgano gli elementi x e y vale A, e questo è la stessa cosa che dire $\forall y\forall x\mathrm{A}$. Analogamente $\exists x\exists y\mathrm{A}$ ha lo stesso significato di $\exists y\exists x\mathrm{A}$. Quindi

$$\frac{\exists x\exists y\mathrm{A}}{\exists y\exists x\mathrm{A}} \qquad \text{e} \qquad \frac{\forall x\forall y\mathrm{A}}{\forall y\forall x\mathrm{A}}\,.$$

Supponiamo $\exists x\forall y\mathrm{A}$ valga: questo vuol dire che c'è un $\bar{x}$ tale che per ogni y vale A. Quindi se scegliamo un y arbitrario possiamo sempre trovare un x tale che A: basta prendere l'elemento $\bar{x}$ di prima. In altre parole

$$\frac{\exists x\forall y\mathrm{A}}{\forall y\exists x\mathrm{A}}\,.$$

Questa regola non può essere invertita: da $\forall y\exists x\mathrm{A}$ non possiamo concludere $\exists x\forall y\mathrm{A}$ — per convincersi di questo basta considerare le affermazioni sui numeri naturali $\forall y\exists x(y<x)$ e $\exists x\forall y(y<x)$.

Il quantificatore esistenziale si distribuisce rispetto alla disgiunzione nel seguente senso: dire che "c'è un x per cui A oppure c'è un x per cui B" è la stessa cosa che dire "c'è un x per cui A o B", in simboli

$$\frac{(\exists x\mathrm{A})\vee(\exists x\mathrm{B})}{\exists x(\mathrm{A}\vee\mathrm{B})} \qquad \text{e} \qquad \frac{\exists x(\mathrm{A}\vee\mathrm{B})}{(\exists x\mathrm{A})\vee(\exists x\mathrm{B})}\,.$$

Per quanto riguarda il quantificatore esistenziale e la congiunzione abbiamo solo una regola: se "c'è un x tale che A e B" allora "c'è un x tale che A, e c'è

un x tale che B", cioè

$$\frac{\exists x(\mathrm{A} \wedge \mathrm{B})}{(\exists x\mathrm{A}) \wedge (\exists x\mathrm{B})} .$$

Il viceversa non vale: dal fatto che ci sia un numero pari e ci sia un numero dispari non possiamo concludere che esista un numero che è tanto pari quanto dispari.

Analogamente, il quantificatore universale si distribuisce rispetto alla congiunzione

$$\frac{(\forall x\mathrm{A}) \wedge (\forall x\mathrm{B})}{\forall x\,(\mathrm{A} \wedge \mathrm{B})} \qquad \text{e} \qquad \frac{\forall x\,(\mathrm{A} \wedge \mathrm{B})}{(\forall x\mathrm{A}) \wedge (\forall x\mathrm{B})} ,$$

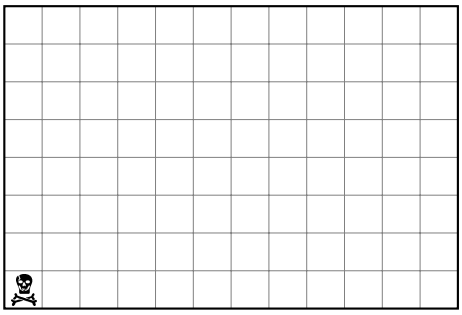
ma solo parzialmente rispetto alla disgiunzione

$$\frac{(\forall x\mathrm{A}) \vee (\forall x\mathrm{B})}{\forall x\,(\mathrm{A} \vee \mathrm{B})} .$$

Questo parallelismo tra il quantificatore esistenziale e la disgiunzione, da un lato, e il quantificatore universale e la congiunzione, dall'altro, non è così sorprendente, visto che i quantificatori possono essere visti come disgiunzioni e congiunzioni generalizzate: dire che vale $\exists x P(x)$ in $\mathbb{N}$ equivale ad asserire $P(0) \vee P(1) \vee P(2) \vee \ldots$ mentre dire che vale $\forall x P(x)$ in $\mathbb{N}$ equivale ad asserire $P(0) \wedge P(1) \wedge P(2) \wedge \ldots$

3.A. Affermazioni esistenziali. Per asserire un'affermazione del tipo $\exists x\mathrm{A}$ non si richiede di esibire esplicitamente un testimone x che renda vera A. Per esempio, per dimostrare $\exists x\mathrm{A}$ è possibile procedere per assurdo, cioè dimostrare che l'affermazione $\forall x\neg\mathrm{A}$ porta ad una contraddizione. Molti risultati profondi sui numeri naturali sono di questo tipo — si dimostra che deve esistere un numero che gode di una certa proprietà, ma spesso non si riesce neppure a stabilire un limite superiore a tale numero. Vediamo ora un esempio molto concreto in teoria dei giochi di questo fenomeno.

Esempio 3.1. Consideriamo il seguente gioco. Fissiamo una tavoletta di cioccolata rettangolare

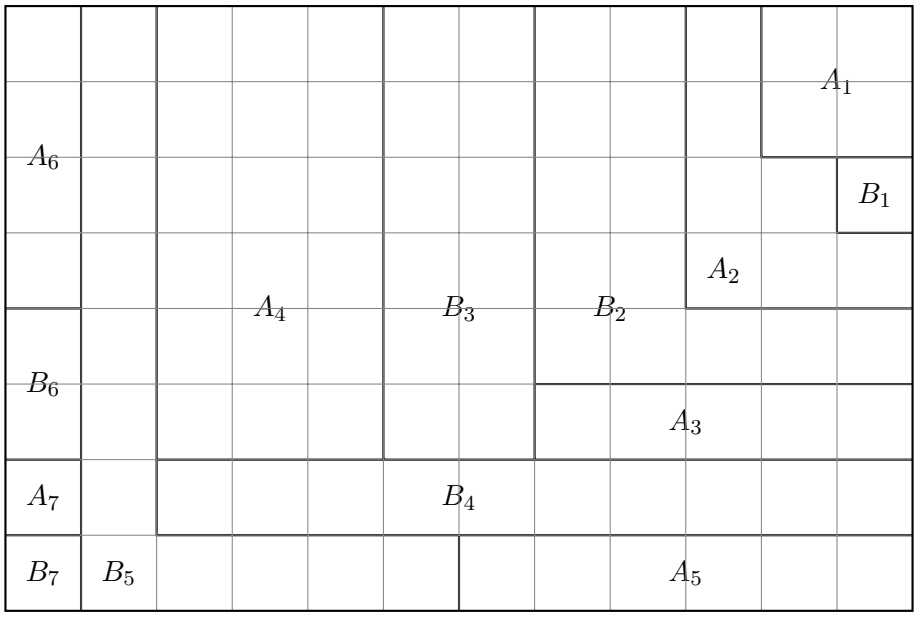


Due giocatori, che convenzionalmente chiameremo Alice e Bob, a turno prendono dei pezzi della tavoletta seguendo la seguente regola

> si sceglie un quadretto di coordinate (i, j) e si prendono tutti i quadretti rimanenti che hanno coordinate (i', j') con $i \leq i'$ e $j \leq j'$.

Alice comincia per prima. Il giocatore che prende il quadretto ☠ di coordinate $(0, 0)$ *perde*. Per la regola, chi prende ☠ prende anche tutti gli altri quadretti che sono rimasti.

Una partita di questo gioco consiste di una stringa mosse (cioè pezzi di cioccolato) della forma $A_1, B_1, A_2, B_2, \ldots$. Dato che la tavoletta ha $n \times m$ quadretti, la stringa ha lunghezza $\leq nm$. Qui sotto riportiamo una partita su una tavoletta 8×12 in cui Alice vince.



CAPITOLO II

Tecniche di dimostrazione

Prima di studiare formalmente le derivazioni, consideriamo in modo ancora informale alcuni esempi di schemi di dimostrazione.

1. Dimostrazione diretta

Consideriamo il problema di dimostrare un enunciato della forma

$$\mathrm{A} \to \mathrm{B}. \tag{5}$$

Una strategia generica che si può applicare in questo caso consiste nel dimostrare B avendo assunto A. Da un punto di vista operativo, assumere A significa poter usare A nella dimostrazione di B. Da un punto di vista semantico, assumere A significa supporre che A sia vera. Questo tipo di dimostrazione di $\mathrm{A} \to \mathrm{B}$ viene chiamata anche **dimostrazione diretta**. Graficamente, una dimostrazione diretta può essere rappresentata così:

$$\begin{array}{|l} \mathrm{A\ (assunzione)} \\ \vdots \\ \mathrm{B} \\ \hline \mathrm{A} \to \mathrm{B\ (conclusione)} \end{array}$$

In questa rappresentazione di una dimostrazione, trascriviamo i passaggi che la compongono uno per riga; le barre verticali servono a delimitare il campo di azione di una assunzione. In questo caso, l'assunzione A si estende per tutte le righe della dimostrazione tranne l'ultima riga, in cui l'assunzione viene **scaricata**: mentre l'enunciato B dipende ancora da A, l'enunciato $\mathrm{A} \to \mathrm{B}$ non ne dipende più, quindi si trova all'esterno della barra orizzontale, che evidentemente rappresenta la struttura d'innestamento dei campi di azione delle assunzioni.

Spesso si vuole dimostrare una proposizione A per tutti i valori di una **variabile** x scelti in un certo insieme, vale a dire si vuole dimostrare $\forall x\mathrm{A}$. Una strategia che può essere adottata in questi casi consiste nel dimostrare la proposizione A per un valore generico di x: poiché niente distingue il valore generico scelto per x da tutti gli altri, la proposizione vale allora per tutti i valori di x. Non sempre questa strategia è sufficiente: vedremo che per dimostrare una proprietà per tutti i numeri naturali è spesso necessario ricorrere al principio di induzione.

Si ricordi che un numero intero n è pari se $n = 2k$ per qualche intero k. Analogamente, n è dispari se $n = 2l + 1$ per qualche l. Vediamo una dimostrazione diretta dell'enunciato seguente:

> Per tutti i numeri interi n ed m, se n è dispari e m è pari, allora $n + m$ è dispari

ovvero

$$\forall n\, \forall m \left(\underbrace{\boxed{n \text{ è dispari}}}_{\text{A}} \wedge \underbrace{\boxed{m \text{ è pari}}}_{\text{B}} \to \underbrace{\boxed{n + m \text{ è dispari}}}_{\text{C}} \right)$$

Per la dimostrazione: siano n ed m interi qualsiasi, ed assumiamo $\text{A} \wedge \text{B}$, cioè: n è dispari e m è pari. Bisogna dimostrare C, cioè: $n + m$ è dispari. Per definizione $n = 2l + 1$ per qualche intero l, mentre $m = 2k$ per qualche intero k. Perciò

$$\begin{aligned} n + m &= (2l + 1) + 2k \\ &= (2l + 2k) + 1 \\ &= 2(l + k) + 1 \end{aligned}$$

che dimostra che $n + m$ è dispari perché ha la forma $2j + 1$ (basta prendere $j = l + k$). □

2. Dimostrazione per assurdo

Una **dimostrazione per assurdo** è una dimostrazione di una proposizione A che assume che A sia falsa e da questa assunzione deriva una **contraddizione**, una proposizione della forma $\text{C} \wedge \neg\text{C}$ (dove C è una proposizione qualsiasi). In particolare, una dimostrazione per assurdo di una proposizione della forma (5) assume che A sia vera e che B sia falsa, e da queste assunzioni deriva una contraddizione. Una dimostrazione con questa struttura viene anche chiamata una **dimostrazione indiretta**.

Vediamo una dimostrazione per assurdo dell'enunciato:

> Per tutti i numeri reali x, y, se $x + y \geq 2$ allora $x \geq 1$ oppure $y \geq 1$.

cioè

$$\forall x\, \forall y \left(\underbrace{\boxed{x + y \geq 2}}_{\text{A}} \to \underbrace{\boxed{x \geq 1}}_{\text{B}} \vee \underbrace{\boxed{y \geq 1}}_{\text{C}} \right)$$

Dimostrazione. Si osservi che assumere che '$x \geq 1$ oppure $y \geq 1$' sia falsa, cioè $\neg(\text{B} \vee \text{C})$ è equivalente ad assumere che $x < 1 \wedge y < 1$, cioè $\neg\text{B} \wedge \neg\text{C}$. Siano x e y numeri reali qualsiasi, e supponiamo che:

$$\begin{aligned} x + y &\geq 2 && \text{A} \\ x &< 1 && \neg\text{B} \\ y &< 1 && \neg\text{C} \end{aligned}$$

Allora $x + y < 1 + 1 = 2$, quindi $x + y < 2$, ma questo contraddice la nostra prima assunzione A, e questo dimostra (per assurdo) che se $x + y \geq 2$ allora $x \geq 1$ oppure $y \geq 1$. □

Dimostriamo ora l'enunciato:

Per ogni numero intero n, se n^2 è pari, allora n è pari

cioè in formule

$$\forall n \left(\underbrace{\boxed{n^2 \text{ è pari}}}_{\text{A}} \to \underbrace{\boxed{n \text{ è pari}}}_{\text{B}} \right).$$

DIMOSTRAZIONE. Dimostriamo che A $\to$ B per un n generico. Assumiamo quindi A, cioè che n^2 sia pari: vorremmo concludere B, cioè che n è pari. Usiamo una dimostrazione per assurdo: assumiamo ¬B, cioè che n sia dispari e facciamo vedere che questa assunzione porta ad una contraddizione. Sia n dispari: allora $n = 2m + 1$ per qualche intero m. Allora possiamo calcolare:

$$\begin{aligned} n^2 &= (2m+1)^2 \\ &= 4m^2 + 4m + 1 \\ &= 2(2m^2 + 2m) + 1 \end{aligned}$$

che dimostra che n^2 è dispari, cioè ¬A che contraddice la prima ipotesi A. Allora abbiamo dimostrato (per assurdo) che n è pari, quindi abbiamo dimostrato (in modo diretto) che se n^2 è pari, allora n è pari, per ogni intero n. □

Graficamente, la struttura di questa dimostrazione potrebbe essere rappresentata in questo modo:

| A: n^2 pari (assunzione della dimostrazione diretta)
| | ¬B: n dispari (assunzione della dimostrazione per assurdo)
| | ⋮
| | ¬A: n^2 dispari
| | A (per ipotesi della dimostrazione diretta)
| B (conclusione della dimostrazione per assurdo)
A $\to$ B (conclusione della dimostrazione diretta)

Il prossimo esempio introduce una tecnica che può essere utilizzata per semplificare la dimostrazione che abbiamo appena visto.

Dimostrazione per contrapposizione. Per dimostrare un enunciato della forma (5), si può anche dimostrare (in modo diretto) l'enunciato equivalente:

$$\neg \text{B} \to \neg \text{A}. \tag{6}$$

Per esempio, si dimostra per contrapposizione l'enunciato:

$$\underbrace{\boxed{n^2 \text{ è pari}}}_{\text{A}} \to \underbrace{\boxed{n \text{ è pari}}}_{\text{B}}$$

dimostrando (in modo diretto) l'enunciato:

$$\underbrace{\boxed{n \text{ è dispari}}}_{\neg\text{B}} \to \underbrace{\boxed{n^2 \text{ è dispari}}}_{\neg\text{A}}$$

Sia n un intero qualsiasi, e si assuma che n sia dispari; bisogna dimostrare allora che anche n^2 è dispari. Se $n = 2k + 1$ per qualche intero k, abbiamo

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= (4k^2 + 4k + 1) \\ &= 2(2k^2 + 2k) + 1 \end{aligned}$$

quindi n^2 è pari, perciò l'enunciato è dimostrato. □

2.A. Dimostrazione per casi. Quando si deve dimostrare un enunciato della forma (5) dove A ha la forma $\mathrm{A}_1 \vee \mathrm{A}_2 \vee \ldots \vee \mathrm{A}_n$, si può cercare equivalentemente di dimostrare tutte le implicazioni

$$(\mathrm{A}_1 \to \mathrm{B}) \wedge \ldots \wedge (\mathrm{A}_n \to \mathrm{B}).$$

Per esempio, si può usare una dimostrazione per casi del seguente enunciato:

Per ogni numero reale x, $x \leq |x|$.

in simboli $\forall x\ (x \leq |x|)$.

Dimostrazione. Consideriamo le proposizioni

$$\underbrace{\boxed{x < 0}}_{\mathrm{A}_1}, \quad \underbrace{\boxed{x \geq 0}}_{\mathrm{A}_2}, \quad \underbrace{\boxed{x \leq |x|}}_{\mathrm{B}}$$

Poiché ogni numero reale è minore di zero o maggiore o uguale a zero, si ha che che per ogni x

$$\mathrm{A}_1 \vee \mathrm{A}_2$$

è sempre vera. È sufficiente quindi dimostrare che

$$\mathrm{A}_1 \vee \mathrm{A}_2 \to \mathrm{B},$$

cioè che

$$(\mathrm{A}_1 \to \mathrm{B}) \wedge (\mathrm{A}_2 \to \mathrm{B}).$$

Distinguiamo due casi:

- $x < 0$, cioè A_1: in questo caso, si ricordi che $|x| = -x$, quindi $|x| > 0 > x$ perciò $|x| \geq x$;
- $x \geq 0$ cioè A_2: $|x| = x \geq 0$ anche in questo caso.

Si può allora concludere che $x \leq |x|$ per ogni reale x. □

Vediamo ora due dimostrazioni (per assurdo) di una nota proprietà:

Teorema 2.1. $\sqrt{2} \notin \mathbb{Q}$

CAPITOLO III

Insiemi e relazioni

1. Insiemi

In matematica è uso comune considerare delle collezioni di oggetti e queste collezioni si dicono **insiemi**. Useremo anche le espressioni **classe** e **famiglia** come sinonimo di insieme, ma non il termine *gruppo* che in matematica ha un significato differente. Un oggetto o **elemento** può appartenere o meno ad un insieme. Per dire che l'oggetto x appartiene all'insieme A scriveremo

$$x \in A$$

Un insieme è completamente determinato dai suoi elementi. Questo discende dal seguente:

PRINCIPIO DI ESTENSIONALITÃ . Due insiemi A e B coincidono se e solo se hanno gli stessi elementi, cioè

$$\forall x \, (x \in A \leftrightarrow x \in B) \, .$$

L'insieme formato dagli elementi $x_1, \ldots, x_n$ lo si indica con

$$\{x_1, \ldots, x_n\} \, .$$

Per esempio l'insieme delle soluzioni dell'equazione $x^3 - 4x^2 + x + 6$ è l'insieme

$$\{-1, 2, 3\} \, , \tag{7}$$

che per il principio di estensionalità è lo stesso insieme che $\{2, -1, 3\}$ oppure $\{3, 2, 3, -1\}$. In altre parole: l'ordine in cui vengno elencati gli elementi di un insieme è irrilevante, e le eventuali ripetizioni non contano. L'insieme di tutti gli x che godono della proprietà P è indicato con

$$\{x \mid P(x)\}$$

o anche con

$$\{x : P(x)\} \, .$$

A volte ci basta considerare tutti gli x appartenenti ad un insieme A e tali che soddisfano la proprietà P, cioè $\{x \mid x \in A \text{ e } P(x)\}$. In questo caso scriveremo

$$\{x \in A \mid P(x)\} \, .$$

Un insieme si dice vuoto se non contiene elementi. Per il principio di estensionalità due insiemi vuoti coincidono, per cui parleremo dell'**insieme vuoto**, che si indica con $\emptyset$.

Un insieme A è **contenuto** in un insieme B ovvero A è un **sottoinsieme** di B, in simboli $A \subseteq B$, se ogni elemento di A è anche un elemento di B, cioè

$$\forall x\,(x \in A \to x \in B)$$

Dal principio di estensionalità si ottiene subito il

Principio di doppia inclusione. Dati due insiemi A e B coincidono se e solo se

$$A \subseteq B \text{ e } B \subseteq A.$$

Poiché $x \in A \to x \in A$ è una tautologia, si ha che

$$A \subseteq A.$$

Quando $A \subseteq B$ ma $A \neq B$ diremo che A è contenuto propriamente in B e scriveremo $A \subset B$.

Per verificare che A non è contenuto in B, in simboli $A \nsubseteq B$, allora non è vero che $\forall x(x \in A \to x \in B)$, cioè $\exists x\,\neg(x \in A \to x \in B)$. Per le Leggi di De Morgan $\neg(x \in A \to x \in B)$ è tautologicamente equivalente a $\neg(x \in A) \wedge (x \in B)$, quindi è sufficiente trovare un elemento di A che non appartiene a B. Poiché $\emptyset$ non ha elementi ne consegue che $\emptyset \subseteq B$, per ogni insieme B.

Osservazione 1.1. Non bisogna confondere la nozione di appartenenza $\in$ con quella di inclusione $\subseteq$: la prima collega elementi ad insiemi, la seconda confronta insiemi.

1.A. Esempi. L'insieme dei **numeri naturali**

$$\mathbb{N} = \{0, 1, 2, \ldots\}$$

è contenuto propriamente nell'insieme dei **numeri interi**

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

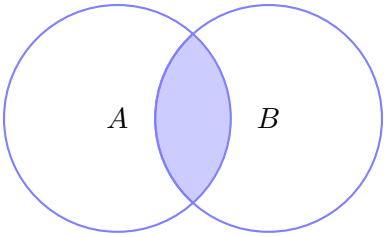
L'insieme $\mathbb{Q}$ dei **numeri razionali** è l'insieme di tutti i numeri della forma n/m con $n, m \in \mathbb{Z}$ e, naturalmente, $m \neq 0$. Ogni intero k può essere scritto come $k/1$ quindi $\mathbb{Z} \subseteq \mathbb{Q}$ e poiché ci sono razionali che non sono interi, l'inclusione è propria, cioè $\mathbb{Z} \subset \mathbb{Q}$. Un razionale ha un'espansione decimale finita (per esempio $\frac{1}{2} = 0{,}5$) oppure un'espansione periodica (per esempio $\frac{1}{3} = 0{,}33333\ldots$). I numeri la cui espansione decimale è arbitraria (cioè finita, periodica o aperiodica) si dicono **numeri reali** e l'insieme dei numeri reali si denota con $\mathbb{R}$. Chiaramente $\mathbb{Q} \subseteq \mathbb{R}$ e poiché ci sono numeri reali che non sono razionali (per esempio $\sqrt{2}$), l'inclusione è propria.

2. Operazioni su insiemi

Dati due insiemi A e B possiamo costruire altri insiemi:

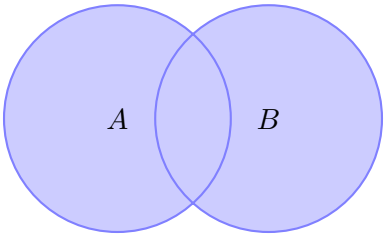
- L'**intersezione** di A e B, in simboli $A \cap B$, è l'insieme di tutti gli enti che stanno tanto in A quanto in B, cioè

$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$



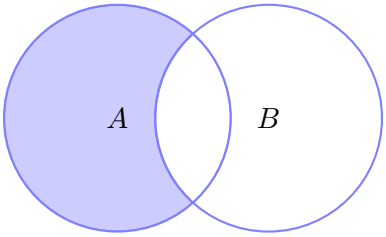
- L'**unione** di A e B, in simboli $A \cup B$, è l'insieme di tutti gli enti che stanno in A o in B (o in entrambi gli insiemi), cioè

$$A \cup B = \{x \mid x \in A \vee x \in B\}$$



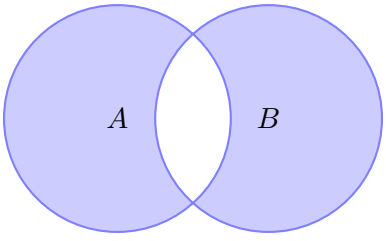
- La **differenza** tra A e B, in simboli $A \setminus B$, è l'insieme di tutti gli enti che stanno in A ma non in B, cioè

$$A \setminus B = \{x \mid x \in A \wedge x \notin B\}$$



- La **differenza simmetrica** tra A e B, in simboli $A \triangle B$, è l'insieme di tutti gli enti che stanno in uno dei due insiemi ma non nell'altro, cioè

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



Esercizio 2.1. Verificare che

$$\forall x \ (x \in A \triangle B \leftrightarrow (x \in A \oplus x \in B))$$

dove $\oplus$ è la disgiunzione esclusiva, *xor*.

L'**insieme delle parti** di un insieme A è l'insieme di tutti i sottoinsiemi di A

$$\mathscr{P}(A) = \{B \mid B \subseteq A\}.$$

Osserviamo che l'insieme delle parti è un insieme i cui elementi sono a loro volta insiemi.

Le operazioni di unione e di intersezione possono essere generalizzate a famiglie arbitrarie di insiemi. Una famiglia arbitraria di insiemi è denotata da $\{A_i \mid i \in I\}$ — ad ogni indice $i \in I$ corrisponde un insieme A_i. L'**unione** degli A_i è l'insieme degli enti che appartengono a *qualche* A_i

$$\bigcup_{i \in I} A_i = \{x \mid \exists i \in I \ (x \in A_i)\}$$

mentre l'**intersezione** degli A_i è l'insieme degli enti che appartengono ad *ogni* A_i

$$\bigcap_{i \in I} A_i = \{x \mid \forall i \in I \ (x \in A_i)\}.$$

Chiaramente ogni $\bigcup_{i \in I} A_i$ contiene ogni A_j mentre $\bigcap_{i \in I} A_i$ è contenuta in ogni A_j. Quando l'insieme degli indici I è $\mathbb{N}$ si utilizzano anche le scritture

$$\bigcup_{n=0}^{\infty} A_n \quad \text{e} \quad \bigcap_{n=0}^{\infty} A_n.$$

Per esempio, se consideriamo la famiglia $\{A_n \mid n \in \mathbb{N}\}$ di intervalli di $\mathbb{R}$ dove $A_n = [-1; 1 - 2^{-n}]$, allora

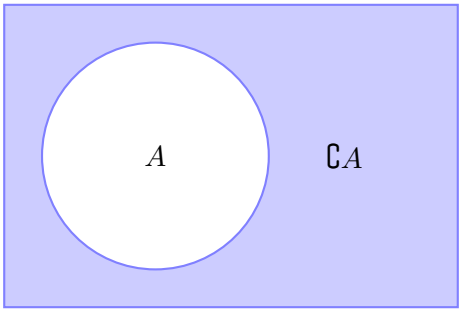
$$\bigcup_{n \in \mathbb{N}} A_n = [-1; 1) \quad \text{e} \quad \bigcap_{n \in \mathbb{N}} A_n = [-1; 0].$$

Se invece $A_n = [-1; 1 + 2^{-n}]$, allora

$$\bigcup_{n \in \mathbb{N}} A_n = [-1; 2] \quad \text{e} \quad \bigcap_{n \in \mathbb{N}} A_n = [-1; 1].$$

Spesso è conveniente assumere che tutti gli insiemi di cui ci stiamo occupando siano contenuti in un insieme universale $\mathcal{U}$, detto appunto **universo**. In altre parole, tutti gli *elementi* appartengono ad $\mathcal{U}$.

Fissiamo ora un universo $\mathcal{U}$. La differenza $\mathcal{U} \setminus A$ si dice **complementare di** A e lo si indica con $\complement A$. Quindi $\complement A = \{x \mid x \notin A\}$



PROPOSIZIONE 2.2. *Per ogni* A, B*:*

$$\complement\complement A = A \tag{8a}$$

$$\complement(A \cup B) = \complement A \cap \complement B \tag{8b}$$

$$\complement(A \cap B) = \complement A \cup \complement B \tag{8c}$$

DIMOSTRAZIONE. Sia $x \in \mathcal{U}$.

$$\begin{aligned} x \in \complement\complement A &\leftrightarrow x \notin \complement A \\ &\leftrightarrow \neg(x \in \complement A) \\ &\leftrightarrow \neg(x \notin A) \\ &\leftrightarrow \neg\neg(x \in A) \\ &\leftrightarrow (x \in A) \end{aligned}$$

Questo dimostra la (8a).

Supponiamo $x \in \complement(A \cup B)$. Allora $\neg(x \in A \vee x \in B)$. Per le leggi di De Morgan, $(x \notin A) \wedge (x \notin B)$, cioè $(x \in \complement A) \wedge (x \in \complement B)$, cioè $x \in (\complement A \cap \complement B)$. Poiché x è arbitrario, questo dimostra che

$$\complement(A \cup B) \subseteq (\complement A \cap \complement B).$$

Viceversa, se $x \in (\complement A \cap \complement B)$ allora $(x \in \complement A) \wedge (x \in \complement B)$, da cui $(x \notin A) \wedge (x \notin B)$. Per le leggi di De Morgan deduciamo $\neg(x \in A \vee x \in B)$ e quindi $x \in \complement(A \cup B)$. Poiché x è arbitrario, questo dimostra che

$$(\complement A \cap \complement B) \subseteq \complement(A \cup B).$$

Per il principio di doppia inclusione $\complement(A \cup B) = (\complement A \cap \complement B)$, cioè (8b) vale.

$$\begin{aligned}
\complement(A \cap B) &= \complement(\complement\complement A \cap \complement\complement B) && \text{per (8a)}\\
&= \complement\left(\complement\left(\complement A \cup \complement B\right)\right) && \text{per (8b)}\\
&= \complement A \cup \complement B && \text{per (8a)}
\end{aligned}$$

Quindi la (8c) è dimostrata. □

La proprietà (8a) si dice **involuzione** e le (8b) e (8c) si dicono **leggi di De Morgan** per gli insiemi.

3. Relazioni e funzioni

Il **prodotto cartesiano** di A e B, in simboli $A \times B$, è l'insieme di tutte le **coppie ordinale** (x, y) dove $x \in A$ e $y \in B$, cioè

$$A \times B = \{(x, y) \mid x \in A \text{ e } y \in B\}.$$

Osserviamo che, a differenza degli insiemi, nelle coppie ordinate l'ordine è fondamentale, cioè (x, y) è un oggetto diverso da (y, x), a meno che x non sia y. Quindi $A \times B$ è distinto da $B \times A$, a meno che $A = B$ nel qual caso scriveremo A^2. Per esempio $\mathbb{R}^2$ è l'insieme delle coppie ordinate di numeri reali e questo insieme viene usualmente identificato con il piano mediante un sistema di assi cartesiani. In generale se $n \geq 2$

$$(x_1, x_2, \ldots, x_n)$$

indica la n-upla ordinata costituita degli elementi $x_1, x_2, \ldots, x_n$ e

$$A^n = \underbrace{A \times \cdots \times A}_{n}$$

è il prodotto cartesiano di n-copie dell'insieme A.

Una **relazione n-aria**, con $n \geq 1$ è un sottoinsieme di $A_1 \times \cdots \times A_n$, per qualche insieme $A_1, \ldots, A_n$ e se questi insiemi sono tutti lo stesso insieme A parleremo di relazione n-aria su A. Se $n = 1$ parleremo di relazione unaria o predicato, se $n = 2$ parleremo di relazione binaria, se $n = 3$ parleremo di relazione ternaria, ecc. Spesso le relazioni binarie si dicono semplicemente relazioni e si scrive $a\ R\ b$ invece di $(a, b) \in R$.

Se R è una relazione n-aria su A e $B \subseteq A$, la **restrizione di R a B** è la relazione n-aria su B:

$$R \restriction B = R \cap B^n.$$

Definizione 3.1. Diremo che una relazione (binaria) R su un insieme A è

riflessiva: se $\forall a \in A\,(a\ R\ a)$,
irriflessiva: se $\forall a \in A\,(\neg(a\ R\ a))$,
simmetrica: se $\forall a, b \in A\,(a\ R\ b \to b\ R\ a)$,
asimmetrica: se $\forall a, b \in A\,(a\ R\ b \to \neg(b\ R\ a))$,
antisimmetrica: se $\forall a, b \in A\,(a\ R\ b \wedge b\ R\ a \to a = b)$,
transitiva: se $\forall a, b, c \in A\,(a\ R\ b \wedge b\ R\ c \to a\ R\ c)$,
totale: se $\forall a, b \in A\,(a\ R\ b \vee a = b \vee b\ R\ a)$.

Talvolta una relazione totale si dice anche connessa. Notare che una relazione non riflessiva non è necessariamente irriflessiva, mentre una relazione asimmetrica è irriflessiva.

La (facile) dimostrazione del seguente risultato è lasciato al lettore.

PROPOSIZIONE 3.2. *Supponiamo R sia una relazione binaria su un insieme A e supponiamo $B \subseteq A$:*

(a) *se R è riflessiva su A, allora $R \restriction B$ è riflessiva su B,*
(b) *se R è irriflessiva su A, allora $R \restriction B$ è irriflessiva su B,*
(c) *se R è simmetrica su A, allora $R \restriction B$ è simmetrica su B,*
(d) *se R è antisimmetrica su A, allora $R \restriction B$ è antisimmetrica su B,*
(e) *se R è asimmetrica su A, allora $R \restriction B$ è asimmetrica su B,*
(f) *se R è transitiva su A, allora $R \restriction B$ è transitiva su B,*
(g) *se R è totale su A, allora $R \restriction B$ è totale su B.*

3.A. Relazioni di equivalenza.

DEFINIZIONE 3.3. Una **relazione di equivalenza su** A è una relazione riflessiva, simmetrica e transitiva su A.

Quindi la restrizione di una relazione di equivalenza è ancora una relazione di equivalenza.

La **diagonale** o **identità** dell'insieme A è

$$I(A) \stackrel{\text{def}}{=} \{(a, a) \mid a \in A\}.$$

$I(A)$ e $A \times A$ sono relazioni di equivalenza su A. Inoltre se E è una relazione di equivalenza su A, allora $I(A) \subseteq E \subseteq A \times A$.

La **classe di equivalenza** di un elemento $a \in A$ relativamente ad una relazione di equivalenza E su A è

$$[a]_E \stackrel{\text{def}}{=} \{x \in A \mid x\ E\ a\}$$

l'insieme di tutti gli elementi E-equivalenti ad a. Spesso si usa il simbolo a/E invece di $[a]_E$. L'**insieme quoziente** è

$$A/E \stackrel{\text{def}}{=} \{[a]_E \mid a \in A\}$$

l'insieme di tutte le classi di equivalenza. Osserviamo che l'insieme quoziente è una famiglia di sottoinsiemi di A, cioè

$$A/E \subseteq \mathscr{P}(A).$$

PROPOSIZIONE 3.4. *Data una relazione di equivalenza E su un insieme A, due classi di equivalenza sono disgiunte o coincidono.*

DIMOSTRAZIONE. Fissiamo due classi di equivalenza $[a]_E$ e $[b]_E$, dove $a, b \in A$.

Caso 1: $a \; E \; b$. Sia $c \in [a]_E$: allora $c \; E \; a$ e per la proprietà transitiva $c \; E \; b$ e quindi $c \in [b]_E$. Quindi $[a]_E \subseteq [b]_E$.

Sia $c \in [b]_E$: allora $c \; E \; b$, per la proprietà simmetrica $b \; E \; a$ e per la proprietà transitiva $c \; E \; a$ e quindi $c \in [a]_E$. Quindi $[b]_E \subseteq [a]_E$.

Per il principio della doppia inclusione abbiamo quindi $[a]_E = [b]_E$.

Caso 2: non vale il Caso 1, cioè $\neg(a \; E \; b)$. Verifichiamo che $[a]_E \cap [b]_E = \emptyset$. Supponiamo, per assurdo, che ci sia un $c \in [a]_E \cap [b]_E$. Allora $c \; E \; b$ e quindi $b \; E \; c$ per simmetria, e dato che $c \; E \; a$ si ha $b \; E \; a$ per transitività. Ma questo contraddice la nostra assunzione.

Quindi il risultato è dimostrato. □

DEFINIZIONE 3.5. Una **partizione** di un insieme $A \neq \emptyset$ è una famiglia $\mathcal{C}$ di sottoinsiemi non vuoti di A, a due a due disgiunti, che ricoprono A, cioè

(1) se $X \in \mathcal{C}$ allora $\emptyset \neq X \subseteq A$,
(2) se $X, Y \in \mathcal{C}$ e $X \neq Y$ allora $X \cap Y = \emptyset$,
(3) ogni elemento di A appartiene a qualche $X \in \mathcal{C}$.

Se E è una relazione di equivalenza su A, allora A/E è una partizione di A. Viceversa, data una partizione $\mathcal{C}$ di A, la relazione $E \subseteq A^2$ definita da

$$a \; E \; b \text{ se e solo se } a \text{ e } b \text{ appartengono al medesimo } X \in \mathcal{C}$$

è una relazione di equivalenza su A.

3.B. Relazioni di ordine.

DEFINIZIONE 3.6. Una **relazione d'ordine su** A — o più semplicemente: un **ordine** o **ordinamento** su A — è una relazione riflessiva, antisimmetrica e transitiva su A.

Quindi la restrizione di una relazione d'ordine è ancora una relazione d'ordine.

L'esempio canonico di ordinamento è la relazione $\leq$ su $\mathbb{N}$, cioè l'insieme

$$\left\{(n,m) \in \mathbb{N}^2 \mid n \leq m\right\}.$$

Analogamente $\leq$ è un ordinamento sugli insiemi $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$. L'ordinamento $\leq$ su questi insiemi è un ordine lineare, dove

DEFINIZIONE 3.7. Un ordine R su un insieme A è **lineare** o **totale** se $a\ R\ b$ o $b\ R\ a$ per ogni scelta di $a, b \in A$.

Se R è un ordine su A, un sottoinsieme $C \subseteq A$ è una **catena** se R ristretto a C è un ordine lineare.

L'inclusione è un ordinamento su $\mathscr{P}(A)$, ma se A ha almeno due elementi, diciamo a e b, questo ordine non è lineare, dato che $\{a\}$ e $\{b\}$ non sono sottoinsiemi l'uno dell'altro.

DEFINIZIONE 3.8. Un **pre-ordine** o **quasi ordine** su A è una relazione binaria $\precsim$ riflessiva e transitiva su A. In questo caso diremo che $(A, \precsim)$ è un insieme pre-ordinato o quasi ordinato.

La nozione di pre-ordine generalizza simultaneamente la nozione di ordine e di relazione di equivalenza.

PROPOSIZIONE 3.9. *Se $\precsim$ è un pre-ordine su A, allora*

$$a \sim b \leftrightarrow a \precsim b \wedge b \precsim a$$

è una relazione di equivalenza su A e la relazione su $A/\!\sim$

$$[a] \leq [b] \leftrightarrow a \precsim b$$

è ben definita ed è un ordine.

DIMOSTRAZIONE. È evidentemente riflessiva, dato che lo è $\precsim$. Se $a \sim b$ allora $a \precsim b \wedge b \precsim a$ e quindi $b \precsim a \wedge a \precsim a$, cioè $b \sim a$; quindi $\sim$ è simmetrica. Se $a \sim b$ e $b \sim c$, allora $a \precsim b \wedge b \precsim a$ e $b \precsim c \wedge c \precsim b$, da cui per transitività di $\precsim$ si ha $a \precsim c \wedge c \precsim a$, cioè $a \sim c$. Abbiamo verificato che $\sim$ è una relazione di equivalenza.

Supponiamo che $a \precsim b$ e $a' \sim a$ e $b' \sim b$: allora $a' \precsim a$ e $b \precsim b'$ quindi $a' \precsim b'$ per la transitività di $\precsim$. Ne segue che la definizione di $\leq$ su $A/\sim$ è ben posta, dato che non dipende dal rappresentante.

È immediato verificare che $\leq$ è riflessiva e transitiva, quindi è sufficiente verificare che è antisimmetrica. Se $[a] \leq [b]$ e $[b] \leq [a]$, allora $a \precsim b \wedge b \precsim a$ da cui $[a] = [b]$. □

DEFINIZIONE 3.10. Sia $\preceq$ un ordinamento su A. Un elemento $a \in A$ si dice

- **massimo** se $b \preceq a$ per ogni $b \in A$
- **minimo** se $a \preceq b$ per ogni $b \in A$.

ESEMPI 3.11.
- L'ordinamento $\leq$ su $\mathbb{N}$ ha minimo (il numero 0), ma non ha massimo.
- L'ordinamento $\leq$ su $\mathbb{Z}$ non ha né minimo, né massimo.
- L'ordinamento $\leq$ sull'intervallo $(0;1] \stackrel{\text{def}}{=} \{x \in \mathbb{R} \mid 0 < x \leq 1\}$ ha massimo (il numero 1) ma non ha minimo.
- L'ordinamento $\subseteq$ su $\mathscr{P}(A)$ ha minimo (l'insieme $\emptyset$) e massimo (l'insieme A).

La relazione $<$ non è un ordine su $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ o $\mathbb{R}$ dato che non vale la proprietà riflessiva. Per questo motivo introduciamo la seguente

DEFINIZIONE 3.12. Un **ordine stretto** su A è una relazione irriflessiva R su A tale che

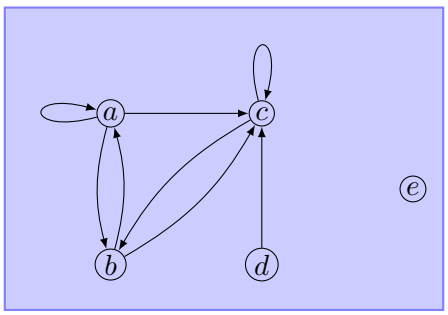
$$R \cup I(A)$$

è un ordine su A.

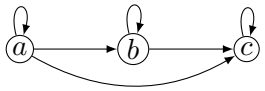
È possibile descrivere una relazione binaria R su un insieme finito M mediante un diagramma. Per esempio la relazione

$$R = \{(a,a),(a,b),(a,c),(b,a),(b,c),(c,c),(d,c)\}$$

sull'insieme $M = \{a,b,c,d,e\}$ è descritta dal diagramma



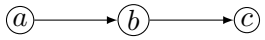
dove la freccia $\textcircled{x} \longrightarrow \textcircled{y}$ significa che $(x, y) \in R$. Quindi un ordine lineare con tre elementi $a \leq b \leq c$ è rappresentato da



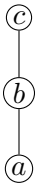
L'informazione contenuta in questo disegno è ridondante — dato che un ordine è una relazione è riflessiva e transitiva, è sufficiente considerare il diagramma della relazione di **successore immediato**

$$R = \{(a, b), (b, c)\}$$

Quindi il diagramma può essere semplificato così:



Inoltre se si stipula che i vertici in basso precedono quelli in alto, possiamo evitare di disegnare le frecce



Rappresentazioni di questo tipo per gli ordini si dicono **diagrammi di Hasse**.

3.C. Funzioni.

DEFINIZIONE 3.13. Una relazione $F \subseteq A \times B$ è una **funzione da A in B** se

(1) per ogni $a \in A$ c'è un $b \in B$ tale che $(a, b) \in F$.
(2) ogni qual volta $(a, b_1) \in F$ e $(a, b_2) \in F$ succede che $b_1 = b_2$.

In questo caso scriveremo $F\colon A \longrightarrow B$ e l'unico $b \in B$ tale che $(a, b) \in F$ lo si indica con $F(a)$.

DEFINIZIONE 3.14. Una funzione $F\colon A \longrightarrow B$ è

iniettiva: se da $a_1 \neq a_2$ segue che $F(a_1) \neq F(a_2)$, o, equivalentemente, se da $F(a_1) = F(a_2)$ segue che $a_1 = a_2$;
suriettiva: se ogni $b \in B$ è della forma $F(a)$ per qualche $a \in A$;
biettiva: se è iniettiva e suriettiva.

DEFINIZIONE 3.15. Una operazione n-aria su A è una funzione $F\colon A^n \longrightarrow A$.

L'insieme delle funzioni da A in B si denota con B^A.

CAPITOLO IV

Il principio di induzione

In matematica (ed in informatica) è spesso necessario dimostrare che una certa proprietà è vera per tutti i numeri naturali. Per esempio:

- Per ogni $n \in \mathbb{N}$,
$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}.$$
- Consideriamo un frammento di codice della forma:
```
while (b)
 S;
```
Se P è una proposizione che esprime una relazione tra i valori delle variabili che compaiono nell'istruzione `S`, allora si può definire un'altra proprietà
$Q(n) \leftrightarrow P$ è vera dopo n iterazioni del ciclo while.
Proprietà di questo tipo sono utilizzate per stabilire che P è una proprietà invariante del ciclo in questione.
- Se $E(n)$ è un'espressione aritmetica che contiene la variabile n, l'equazione
$$f(n) = E(n)$$
stabilisce che la funzione f per l'argomento n ha lo stesso valore dell'espressione $E(n)$. Se immaginiamo che la funzione f sia definita ricorsivamente, si può dimostrare per induzione che $f(n) = E(n)$ per ogni valore naturale di n, stabilendo così la correttezza della definizione ricorsiva della funzione il cui valore per n è dato da $E(n)$.

1. Prima formulazione del principio di induzione

La formulazione più generalmente nota del **principio di induzione** (PI) è la seguente.

Principio di Induzione. Data una proprietà P dei numeri naturali, se $P(0)$ e $\forall n \in \mathbb{N}\ (P(n) \to P(n+1))$, allora $\forall x \in \mathbb{N}\, P(x)$.

Qui una proprietà dei numeri naturali è una proprietà per la quale abbia senso chiedersi se è vera o falsa per un numero naturale. La **base** dell'induzione è la dimostrazione di $P(0)$, mentre il **passo induttivo** è la dimostrazione dell'implicazione $P(n) \to P(n+1)$, che normalmente si articola nel modo seguente: si assume che $P(n)$ sia vera (questa è detta l'**ipotesi induttiva**, e si dimostra che $P(n+1)$. Un'altra formulazione, del tutto equivalente alla prima, del principio di induzione, usa l'**estensione** della proprietà P, cioè l'insieme dei numeri naturali per i quali la proprietà è vera:

Principio di Induzione per insiemi. Se $A \subseteq \mathbb{N}$ è tale che $0 \in A$ e $\forall n \in \mathbb{N}\ (n \in A \to n+1 \in A)$, allora $A = \mathbb{N}$.

Se vogliamo dimostrare per induzione una proposizione del tipo $\forall n \geq k\, P(n)$, è necessario modificare il principio di induzione nel seguente modo.

Principio di Induzione (Per $n \geq k$). Data una proprietà P dei numeri naturali, se $P(k)$ e $\forall n \in \mathbb{N}\ ((n \geq k \wedge P(n)) \to P(n+1))$, allora $\forall x \in \mathbb{N}\,(x \geq k \to P(x))$.

1.A. Aritmetica. Vediamo subito il primo esempio di utilizzo del principio di induzione:

Esempio 1.1. $\forall n \in \mathbb{N}\left[\sum_{i=0}^{n} i = \frac{n(n+1)}{2}\right]$.

Dimostrazione. Qui la proprietà $P(k)$ è

$$\sum_{i=0}^{k} i = \frac{k(k+1)}{2}.$$

La base dell'induzione consiste nel verificare $P(0)$, cioè che $\sum_{i=0}^{0} i = 0 = \frac{0(0+1)}{2}$.

Per dimostrare il passo induttivo, assumiamo che

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$$

e dimostriamo che

$$\sum_{i=0}^{n+1} i = \frac{(n+1)(n+2)}{2}.$$

Ora,

$$\begin{aligned}\sum_{i=0}^{n+1} i &= \left(\sum_{i=0}^{n} i\right) + (n+1) \\ &= \frac{n(n+1)}{2} + (n+1) && \text{per l'ipotesi induttiva} \\ &= \frac{n(n+1)}{2} + \frac{2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2}\end{aligned}$$

e mediante un'applicazione del principio di induzione si ottiene la conclusione. □

ESEMPIO 1.2. $\forall n \in \mathbb{N}\left[\sum_{i=0}^{n}(2i+1) = (n+1)^2\right]$.

DIMOSTRAZIONE. Qui la proprietà $P(k)$ è

$$\sum_{i=0}^{k}(2i+1) = (k+1)^2.$$

La base dell'induzione consiste nel verificare $P(0)$, cioè che $\sum_{i=0}^{0}(2i+1) = 1 = (0+1)^2$.

Per dimostrare il passo induttivo, assumiamo che

$$\sum_{i=0}^{n} 2i+1 = (n+1)^2$$

e dimostriamo che

$$\sum_{i=0}^{n+1} 2i+1 = (n+2)^2.$$

Ora,

$$\begin{aligned}\sum_{i=0}^{n+1} 2i+1 &= \left(\sum_{i=0}^{n} 2i+1\right) + 2(n+1) + 1 \\ &= (n+1)^2 + 2(n+1) + 1 && \text{per l'ipotesi induttiva} \\ &= (n+2)^2\end{aligned}$$

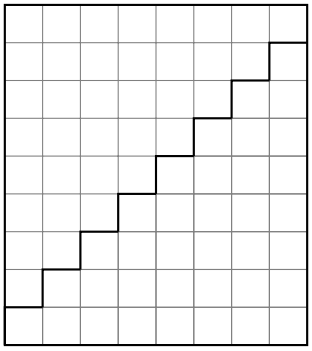
e mediante un'applicazione del principio di induzione si ottiene la conclusione. □

Il metodo dell'induzione fornisce un metodo per *dimostrare* che una certa formula è vera, ma non fornisce, in generale, un metodo per *scoprire* la

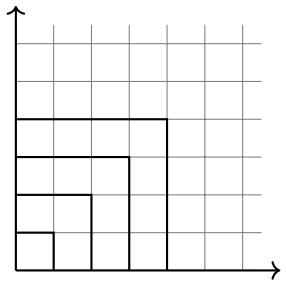
formula che vogliamo dimostrare. Le due formule viste qui sopra

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2} \quad \text{e} \quad \sum_{i=0}^{n} (2i+1) = (n+1)^2$$

si possono dimostrare mediante argomenti geometrici. La figura

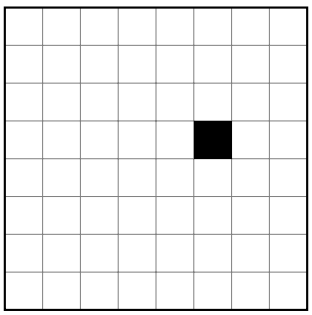


mostra come il rettangolo di area $n \times (n+1)$ si può ripartire in due regioni, ciascuna di area $1 + 2 + \cdots + n$, da cui la formula dell'Esempio 1.1, mentre la figura

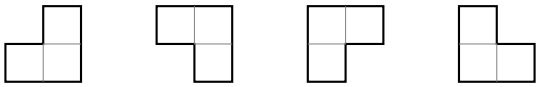


mostra come l'area del quadrato di lato n sia ottenibile sommando l'area delle "cornici" $1 + 3 + 5 + \cdots + (2n-1)$, da cui la formula dell'Esempio 1.2.

ESEMPIO 1.3. Consideriamo la figura geometrica F ottenuta prendendo un quadrato di lato 2^n, composto di $2^n \times 2^n$ quadretti, da cui è stato rimosso un quadretto, per esempio



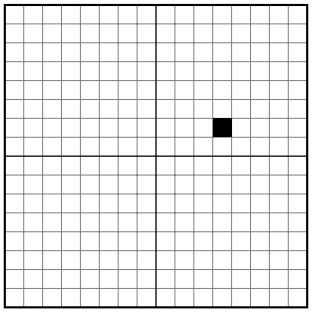
Dimostrare che F è ricopribile con i tasselli



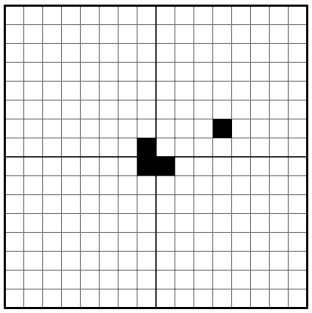
DIMOSTRAZIONE. Vogliamo dimostrare che $\forall n \geq 1\, P(n)$, dove $P(n)$ è la proprietà che ogni figura F ottenuta da un quadrato di lato 2^n è ricopribile nel modo richiesto.

$P(1)$ è immediata, dato che ogni quadrato di lato 2 a cui sia stato rimosso uno dei quattro quadrati è proprio uno dei tasselli.

Supponiamo $P(n)$ valga. Sia F una figura ottenuta da un quadrato di lato 2^{n+1} e suddividiamo questa figura in quattro blocchi costituiti da quadrati di lato 2^n, uno dei quali mancante di una tessera. Per esempio possiamo supporre che il quadrato mancante sia nel blocco in alto a destra



Mettiamo un tassello  nel punto di incontro dei quattro blocchi:



A questo punto abbiamo quattro figure a cui possiamo applicare l'ipotesi induttiva □

1.B. Correttezza di programmi. Consideriamo il problema di calcolare il quoziente q ed il resto r della divisione di due numeri interi $X \geq 0$ e $D > 0$. L'algoritmo usuale consiste nel sottrarre ripetutamente D a X,

aumentando ogni volta di 1 il valore di q che inizialmente ha valore 0. Schematicamente, l'algoritmo è il seguente:

(1) fino a quando $X \geq D$ esegui le seguenti azioni: sottrai D a X; aumenta q di 1
(2) quando $X < D$, poni $r = X$.

Un programma Java che realizza questo algoritmo è il seguente:

```
class divisione {
public static void main (String[] args) {
  int X, D, q, r;
  X = 14;
  D = 3;
  q = 0;
  r = X;
  while (r >= D) {
   r = r - D;
   q = q + 1;
  }
  System.out.println ("Il quoziente è: " + q);
  System.out.println ("Il resto è: " + r);
  }
}
```

Come si può dimostrare che il programma precedente è corretto? Prima di tutto, serve una specifica precisa del problema da risolvere: La condizione di ingresso del programma, cioè la proprietà che i dati in ingresso X e D devono soddisfare, è che $X \geq 0$ e $D > 0$ (la seconda proprietà serve ad evitare casi di divisione per 0). La condizione di uscita del programma, cioè la proprietà che i dati in uscita q ed r devono soddisfare, è che $X = q * D + r$, con $r < D$. Questa proprietà dice proprio che q ed r sono, rispettivamente, il quoziente ed il resto della divisione intera di X per D. La correttezza del programma (qualche volta si parla di questa condizione come di **correttezza parziale** asserisce che:

> per ogni dato in ingresso che soddisfa la condizione di ingresso, se il programma termina, allora i dati in uscita soddisfano la condizione di uscita.

Una condizione più esigente di correttezza è quella che si chiama **correttezza totale**:

> per ogni dato in ingresso che soddisfa la condizione di ingresso, *il programma termina* e i dati in uscita soddisfano la condizione di uscita.

Per stabilire che un programma soddisfa la specifica vi sono vari modi, ma la tecnica più conveniente consiste nel trovare quello che si chiama un **invariante** (di ciclo):

> invariante (di un ciclo) è una proprietà che lega (tutte o alcune del)le variabili coinvolte nel ciclo, e che è vera dopo un numero arbitrario di iterazioni del ciclo. In particolare, è vera all'ingresso nel ciclo (cioè dopo 0 iterazioni).

Ci sono molte proprietà invarianti del ciclo

```
while (r >= D) {
  r = r - D;
  q = q + 1;
}
```

nel programma precedente, per esempio la proprietà $q \geq 0$. Tra tutte le possibili proprietà ce ne sono alcune che sono più interessanti di altre. Consideriamo ora la proprietà:

$$X = q * D + r \tag{9}$$

che è molto simile alla condizione di uscita del programma. Che si tratti veramente di un invariante è qualcosa che deve ancora essere dimostrato, ma per il momento assumiamo che lo sia. Quando il ciclo termina (e prima o poi deve terminare, perché ad ogni iterazione a r viene sottratto il valore D che, per la condizione di ingresso, è un numero > 0, quindi prima o poi deve accadere che $r < D$) abbiamo che $X = q * D + r$ perché abbiamo assunto che questa proprietà sia invariante, ed inoltre si esce dal ciclo perché $r < D$. Ma allora è vera la proprietà $X = q * D + r$, con $r < D$, che è proprio la condizione di uscita del programma. L'uso dell'invariante ci permette quindi di dimostrare che il programma è (parzialmente) corretto. In questo caso abbiamo già implicitamente dimostrato che il programma è anche totalmente corretto, perché abbiamo già visto che il ciclo deve terminare. Resta da dimostrare che la proprietà (9) è proprio invariante. Questo si può fare per induzione sul numero di iterazioni del ciclo. Supponiamo che questo numero sia 0 (base dell'induzione) (ovviamente, la dimostrazione che (9) è invariante vale in generale, non solo per gli specifici valori di X e D che abbiamo scelto). Allora $q = 0$ (perché q non viene incrementato) e $r = X$. Allora $X = q*D+r$ perché questo si riduce a dire che $X = 0 * D + X$, che è ovviamente vero. Supponiamo che il ciclo sia stato eseguito n volte, e che la proprietà (9) sia

vera (ipotesi induttiva); vogliamo dimostrare ora che resta vera anche dopo la $(n+1)$-esima iterazione. Durante questa iterazione vengono modificati i valori di q e di r, ottenendo valori

$$q' = q + 1$$
$$r' = r - D$$

dove q' ed r' sono i valori delle variabili q ed r dopo l'esecuzione delle istruzioni

```
r = r - D;
q = q + 1;
```

Allora calcoliamo:

$$\begin{aligned} q' * D + r' &= (q+1) * D + (r - D) \\ &= q * D + D + r - D \\ &= q * D + r = X \end{aligned}$$

dove l'ultimo passaggio sfrutta l'ipotesi induttiva. Per induzione si conclude allora che la proprietà (9) è vera per qualsiasi numero di iterazioni del ciclo, quindi (9) è invariante.

Esempio 1.4. (Quadrato di un numero naturale) Vediamo un altro esempio della tecnica appena usata per dimostrare la correttezza del programma per la divisione intera, utilizzandola questa volta per sintetizzare un programma per calcolare il quadrato di un numero naturale N. La condizione di ingresso sarà dunque $N \geq 0$, mentre la condizione di uscita sarà $Y = X * X$ e $X = N$ dove Y è il dato in uscita ed X una variabile ausiliaria utilizzata come contatore. L'invariante appropriato in questo caso è la formula

$$Y = X * X. \tag{10}$$

Inizialmente avremo dunque $X = 0$ e $Y = 0$: l'invariante è ovviamente vero in questo caso, e questo stabilisce la base della dimostrazione induttiva che la proprietà (10) è invariante.

```
class quadrato {
  public static void main (String[] args) {
   int N, X, Y;
   N = ? ; // inizializzazione
   X = 0;
   Y = 0;
   while (X < N) {
     Y = Y + 2 * X + 1;
     X = X + 1;
   }
```

```
   System.out.println ("Quadrato = " + Y);
  }
}
```

Per quanto riguarda il passo induttivo, l'ipotesi induttiva è

$$Y = X * X \text{ dopo l'}n\text{-esima iterazione;}$$

bisogna dimostrare che (10) resta vera dopo la $(n+1)$-esima iterazione. Se Y' è il valore di Y dopo l'esecuzione dell'istruzione $Y = Y + 2 * X + 1$, mentre X' è il valore di X dopo l'esecuzione dell'istruzione $X = X + 1$, possiamo calcolare

$$\begin{aligned} Y' &= Y + 2 * X + 1 \\ &= (X * X) + 2 * X + 1 && \text{(per ipotesi induttiva)} \\ &= (X + 1) * (X + 1) \\ &= X' * X' \end{aligned}$$

da cui si conclude che (10) è proprio invariante. Poiché il valore di $N - X$ decresce strettamente ad ogni iterazione, il ciclo deve terminare (perché non ci può essere una sequenza infinita di numeri naturali $k_0 > k_1 > k_2 > \ldots$) all'uscita dal ciclo avremo $X = N$ (perché la condizione del while è diventata falsa e sappiamo, per come è fatto il programma, che $X \leq N$) quindi, per l'invariante, $Y = N * N$. Questo mostra che la condizione di uscita è soddisfatta dal dato in uscita Y, perciò il programma è corretto.

1.C. Definizioni ricorsive di funzioni. Immaginiamo di volere definire una funzione $f\colon \mathbb{N} \longrightarrow A$, dove $\mathbb{N}$ è l'insieme dei numeri naturali ed A un insieme qualsiasi. Si può allora utilizzare il seguente schema di ricorsione:

$$\begin{aligned} f(0) &= a \\ f(n+1) &= E(f(n)) \end{aligned}$$

dove a è un elemento di A e con la notazione $E(f(n))$ si indica che l'espressione E può utilizzare al suo interno il valore $f(n)$. Una giustificazione intuitiva di questo schema si può ottenere considerando la struttura dei numeri naturali: la funzione f è definita per 0 perché la prima clausola dello schema ne fornisce il valore a; supponiamo invece che k sia un numero positivo, e che quindi $k = n + 1$ per qualche numero naturale n. Si può immaginare di avere già calcolato il valore di $f(n)$ (la funzione f viene calcolata "dal basso", partendo dall'argomento 0), e si può quindi calcolare $E(f(n))$ che dà il valore di $f(n+1)$. (Una giustificazione rigorosa di questo metodo di definizione di funzioni verrà data più tardi, nel Teorema **??**.)

Vediamo solo una applicazione di questo schema, riprendendo un esempio già trattato quando abbiamo discusso gli invarianti:

ESEMPIO 1.5. (La funzione quadrato) Si può definire ricorsivamente il quadrato di un numero naturale mediante le clausole:

$$\begin{aligned} q(0) &= 0 \\ q(n+1) &= q(n) + 2 * n + 1 \end{aligned}$$

Vediamo che le clausole precedenti definiscono effettivamente la funzione desiderata, dimostrando per induzione che la proprietà $q(n) = n * n$ è vera per ogni valore di n:

(Base dell'induzione)

$$\begin{aligned} q(0) &= 0 && \text{(per definizione)} \\ &= 0 * 0 \end{aligned}$$

(Passo indutttivo)

$$\begin{aligned} q(n+1) &= q(n) + 2 * n + 1 && \text{(per definizione)} \\ &= n * n + 2 * n + 1 && \text{(per ipotesi induttiva)} \\ &= (n+1) * (n+1) && \text{(per proprietà algebriche)} \end{aligned}$$

Si osservi che le clausole della definizione ricorsiva della funzione $q(n)$ consentono anche di calcolare il valore di questa funzione per un valore arbitrario dell'argomento. Per esempio:

$$\begin{aligned} q(5) &= q(4+1) \\ &= q(4) + 2 * 4 + 1 \\ &= q(3+1) + 2 * 4 + 1 \\ &= q(3) + 2 * 3 + 1 + 2 * 4 + 1 \\ &= q(2+1) + 2 * 3 + 1 + 2 * 4 + 1 \\ &= q(2) + 2 * 2 + 1 + 2 * 3 + 1 + 2 * 4 + 1 \\ &= q(1+1) + 2 * 2 + 1 + 2 * 3 + 1 + 2 * 4 + 1 \\ &= q(1) + 2 * 1 + 1 + 2 * 2 + 1 + 2 * 3 + 1 + 2 * 4 + 1 \\ &= q(0+1) + 2 * 1 + 1 + 2 * 2 + 1 + 2 * 3 + 1 + 2 * 4 + 1 \\ &= q(0) + 2 * 0 + 1 + 2 * 1 + 1 + 2 * 2 + 1 + 2 * 3 + 1 + 2 * 4 + 1 \\ &= 0 + 2 * 0 + 1 + 2 * 1 + 1 + 2 * 2 + 1 + 2 * 3 + 1 + 2 * 4 + 1 \\ &= 1 + 2 + 1 + 4 + 1 + 6 + 1 + 8 + 1 \\ &= 25 \end{aligned}$$

2. Generalizzazioni del principio di induzione

C'è un altro principio fondamentale per ragionare sui numeri naturali, il **Principio del Minimo** (PM)

PRINCIPIO DEL MINIMO. Se la proprietà P è vera per qualche numero naturale, allora c'è un minimo numero naturale n tale che $P(n)$.

Dire che n è il minimo per il quale la proprietà P vale implica, in particolare, che $\forall k < n \neg P(k)$. Una conseguenza fondamentale del principio del minimo è la seguente proprietà, che si esprime dicendo che la relazione d'ordine stretta $<$ sui numeri naturali è **ben fondata**:

PROPOSIZIONE 2.1. *Non esiste alcuna successione discendente infinita di numeri naturali*

$$n_0 > n_1 > n_2 > \dots \tag{11}$$

DIMOSTRAZIONE. Per assurdo, se esistesse una successione come in (11), l'insieme $\{n_0, n_1, n_2, \dots\}$ non avrebbe un minimo elemento. □

L'importanza di questa proprietà dei numeri naturali, che verrà generalizzata nella sezione **??**, risiede tra l'altro nell'utilizzo che se ne può fare per dimostrare la terminazione di programmi. Si ricordi che implicitamente questa proprietà era già stata utilizzata, per esempio, nella dimostrazione della correttezza totale del programma per la divisione intera. La terminazione del ciclo sul quale quel programma si basa viene dimostrata assegnando a ciascuna configurazione di valori $c = (X, D, q, r)$ assunti dalle corrispondenti variabili del programma un numero naturale $T(c)$ (nel caso specifico `r`). Si utilizza poi l'osservazione che, se il programma permette di passare da una configurazione $c = (X, D, q, r)$ ad una configurazione $c' = (X', D', q', r')$, allora $T(c) > T(c')$. Questo è sufficiente a stabilire la terminazione: se il programma non terminasse dovrebbe esistere una successione di configurazioni $c_0, c_1, c_2, \dots$ tale che il programma passa dalla configurazione c_i alla configurazione c_{i+1} , per ogni $i = 0, 1, 2, \dots$. Ma allora dovrebbe anche esistere una successione discendente di numeri naturali $T(c_0) > T(c_1) > T(c_2) > \dots$, contro la buona fondazione di $<$ su $\mathbb{N}$.

Vediamo un'applicazione del principio del minimo:

PROPOSIZIONE 2.2. *Ogni numero naturale ≥ 2 ha una scomposizione in fattori primi.*

DIMOSTRAZIONE. Per assurdo, sia $n \geq 2$ tale da non avere una scomposizione in fattori primi. Supponiamo anche che n sia il minimo numero con questa proprietà. Ci sono due casi:

(1) n è primo: allora n ha una scomposizione in fattori primi, assurdo.
(2) n è composto: sia $n = pq$, dove $p, q \geq 2$. I numeri p e q devono avere una scomposizione in fattori primi, perché n è il minimo che non ce l'ha, quindi anche n deve averla, componendo in modo opportuno le scomposizioni di p e q, assurdo.

In entrambi i casi abbiamo contraddetto l'ipotesi che ci sia un numero naturale che non ha scomposizione in fattori primi, quindi abbiamo dimostrato la proposizione. □

2..1. *Il principio di induzione forte.* Il **Principio di dimostrazione per induzione forte** (PIF) è una forma del principio che risulterà essere equivalente al principio di induzione (PI). Diciamo che una proprietà P dei numeri naturali è **progressiva** se

$$\forall x \left((\forall y < x \, P(y)) \to P(x) \right),$$

e scriviamo $\mathrm{Prog}(P)$ per indicare che P è una proprietà progressiva.

PRINCIPIO DI INDUZIONE FORTE. Se $\mathrm{Prog}(P)$, allora $\forall n \in \mathbb{N} \, P(n)$.

In altre parole: per dimostrare $\forall n \in \mathbb{N} \, P(n)$ è sufficiente dimostrare che, preso un generico k, se $\forall x < k \, P(x)$ allora $P(k)$.

ESEMPIO 2.3. Come esempio di applicazione del principio di induzione forte, si consideri il seguente enunciato:

> Supponiamo che ci siano due pile di carte ciascuna delle quali contiene $n > 0$ carte. Due giocatori, a turno, scelgono una pila e rimuovono da questa un numero di carte arbitrario, ma positivo. Il giocatore che rimuove l'ultima carta vince. Dimostrare che il secondo giocatore ha una strategia vincente.

La dimostrazione è per induzione forte. Abbreviamo con $P(n)$ la proposizione che il secondo giocatore può sempre vincere quando le due pile contengono n carte. Bisogna dimostrare che P è una proprietà progressiva. Per questo, per un n generico, supponiamo che $P(k)$ per ogni $k < n$ positivo; bisogna concludere che $P(n)$. Supponiamo che il primo giocatore rimuova i carte da una pila, allora il secondo giocatore può vincere rimuovendo i carte dall'altra pila. Infatti:

(1) se $i = n$: allora il secondo giocatore rimuove tutta la pila rimanente, e quindi l'ultima carta, vincendo.
(2) se $i < n$: per ipotesi $P(n-i)$, e il secondo giocatore vince seguendo la strategia per la situazione in cui entrambe le pile hanno $n - i$ carte, essendo il secondo giocatore anche in questa situazione.

Poiché abbiamo dimostrato che P è progressiva, (PIF) ci permette di concludere $\forall n > 1\, P(n)$, cioè che il secondo giocatore può sempre vincere in questo gioco.

TEOREMA 2.4. *Le seguenti affermazioni sono equivalenti:*

- *Il Principio di Induzione (PI),*
- *Il Principio di Induzione Forte (PIF),*
- *Il Principio del Minimo (PM).*

DIMOSTRAZIONE. (PI)→(PIF): Assumiamo che Prog(P). L'idea naturale sarebbe quella di dimostrare per induzione che $P(n)$ per ogni $n \in \mathbb{N}$. In effetti si dimostra che $P(0)$ perché $\forall y < 0\, P(y)$ e non c'è alcun elemento di $\mathbb{N}$ minore di 0, quindi per l'assunzione che Prog(P) abbiamo $P(0)$. Per dimostrare il passo induttivo tuttavia, dovremmo riuscire a dimostrare che $P(n+1)$ assumendo che $P(n)$, ma questo non basta per applicare l'ipotesi Prog(P). Allora seguiamo un'altra strategia: dimostriamo per induzione che

$$\forall n \in \mathbb{N}\, P^\sharp(n),$$

dove la nuova proprietà $P^\sharp$ è definita nel modo seguente, per $x \in \mathbb{N}$:

$$P^\sharp(x) \text{ se e solo se } \forall y < x\, P(y).$$

Possiamo concludere per lo stesso ragionamento di prima che $P^\sharp(0)$. Supponiamo ora (ipotesi induttiva) che $P^\sharp(n)$ per un generico $n \in \mathbb{N}$, e vediamo di dimostrare che è anche vero che $P^\sharp(n+1)$. Se $P^\sharp(n)$, allora per la definizione di $P^\sharp$ abbiamo $\forall y < n\, P(y)$. Poiché Prog(P), $P(n)$ è vera e quindi $\forall y < n+1\, P(y)$, ma questo equivale alla verità di $P^\sharp(n+1)$. Per induzione concludiamo allora che $\forall n \in \mathbb{N}\, P^\sharp(n)$. Sia ora k un generico numero naturale: allora $P^\sharp(k+1)$, quindi $\forall y < k+1\, P(y)$ e perciò $P(k)$, quindi possiamo asserire che $\forall n \in \mathbb{N}\, P(n)$, che è la conclusione desiderata.

(PIF)→(PI): Assumiamo (PIF) e assumiamo anche che $P(0)$ e che $P(n) \to P(n+1)$ per un generico $n \in \mathbb{N}$. Vogliamo dimostrare che P è progressiva: assumiamo quindi che P non lo sia cercando di ottenere una contraddizione. Se $\neg$Prog(P), per qualche $k \in \mathbb{N}$ abbiamo che $\forall y < k\, P(y)$ ma non $P(k)$. Ci sono due casi:

- $k = 0$: questo contraddice l'assunzione che $P(0)$;

- $k \neq 0$: allora $k = k' + 1$ per qualche k'. Poiché $k' < k$, abbiamo $P(k')$ e per assunzione $P(k' + 1)$, cioè $P(k)$, contraddizione.

In entrambi i casi abbiamo così una contraddizione, che implica che l'assunzione che $\neg\mathrm{Prog}(P)$ porta ad una contraddizione, quindi $\mathrm{Prog}(P)$. Allora $\forall x\, P(x)$, che è la conclusione di (PI), per (PIF).

(PM) $\to$ (PIF): Supponiamo che $\mathrm{Prog}(P)$, e che (per assurdo) $\neg\forall x\, P(x)$, cioè che esista un $n \in \mathbb{N}$ tale che non $P(n)$. Allora c'è un minimo $m \in \mathbb{N}$ tale che non $P(m)$. Quindi $\forall y < m\, P(y)$ e dalla progressività di P segue che $P(m)$, contraddizione.

(PIF)$\to$(PM): Consideriamo la proprietà $Q(x)$ che vale se e solo se $\neg P(x)$. Applichiamo (PIF) a Q, ottenendo

$$\begin{aligned}
\mathrm{Prog}(Q) &\to \forall x Q(x) \\
\forall x Q(x) &\to \neg\mathrm{Prog}(Q) && \text{(per contrapposizione)} \\
\neg\forall x\, \neg P(x) &\to \exists x\, ((\forall y < x\, \neg P(y)) \wedge P(x)) && \text{(dualità dei quantificatori)} \\
\exists x\, P(x) &\to \exists x\, (P(x) \wedge \forall y < x\, \neg P(y))
\end{aligned}$$

dove l'ultima formula è proprio (PM). □

È conveniente visualizzare la struttura della dimostrazione (PIF)$\to$(PI):

(PIF)
| $P(0) \wedge \forall x\, (P(x) \to P(x+1))$ (assunzione della dimostrazione diretta)
| | $\neg\forall x\, P(x)$ (assunzione della sottodimostrazione per assurdo)
| | $\vdots$ (sottodimostrazione per casi)
| | contraddizione (conclusione della sottodimostrazione per casi)
| $\forall x\, P(x)$ ((conclusione della sottodimostrazione per assurdo, per (PIF))
(PI)(conclusione della dimostrazione diretta)

Il principio di induzione forte ammette una generalizzazione interessante a insiemi per i cui elementi è definita una nozione di altezza.

Corollario 2.5 (Principio di induzione strutturale). *Sia A un insieme con una funzione $h\colon A \longrightarrow \mathbb{N}$. Data una proprietà P, assumiamo che per ogni $n \in \mathbb{N}$:*

($\star$)**:** *se $P(a)$ per ogni a con $h(a) < n$, allora $P(a)$ per ogni a con $h(a) = n$.*

Allora $P(a)$, per ogni $a \in A$.

DIMOSTRAZIONE. Definiamo, per un generico $n \in \mathbb{N}$:

$$\overline{P}(n) \text{ se e solo se } \forall a \in A\,(h(a) = n \to P(a)).$$

Abbiamo $\mathrm{Prog}(\overline{P})$, perché $\overline{P}(k)$ per ogni $k < n$ implica che $\overline{P}(n)$, per l'ipotesi $(\star)$ su P. Quindi, per induzione forte, $\overline{P}(n)$ per ogni $n \in \mathbb{N}$. Sia $a \in A$ qualsiasi: abbiamo allora $\overline{P}(h(a))$, perciò $P(a)$, da cui la conclusione del principio di induzione strutturale. □

Naturalmente, questa formulazione del principio di induzione strutturale è significativa soltanto nel caso in cui la funzione h non sia a sua volta definita induttivamente sulla costruzione di A. Purtroppo, questo è quello che accade nella maggior parte delle applicazioni: è così necessario in generale trovare un'altra giustificazione di questo principio, che tuttavia richiede l'approfondimento di tecniche che escono dall'ambito di questo corso.

CAPITOLO V

Sintassi

Dato un insieme non vuoto A indicheremo con A^* l'insieme di tutte le **stringhe** finite di elementi di A. Se, per esempio, $A = \{a, b, c\}$ alcuni tra gli elementi di A^* sono

$$a \quad b \quad c \quad aacba \quad bab \quad bb \quad ccbabbc \quad \dots$$

Talvolta per delimitare una stringa useremo le parentesi angolari e scriveremo $\langle aacba\rangle$ invece di $aacba$, ma se non c'è pericolo di confusione tralasceremo le parentesi angolari.

Infine considereremo anche la **stringa vuota** $\langle\rangle$ che non contiene nessun simbolo. Spesso in informatica la stringa vuota la si indica con la lettera greca ε.

Date due stringhe $s, t \in A^*$, la **concatenazione** di s con t è la stringa st ottenuta scrivendo la stringa s seguita dalla stringa t. Per esempio se $A = \{a, b, c\}$ e s e t sono rispettivamente $ccbabbc$ e $aacba$, allora

$$st = \langle ccbabbc\rangle\langle aacba\rangle = ccbabbcaacba.$$

Notiamo che $s\langle\rangle = \langle\rangle s = s$, per ogni $s \in A^*$.

La funzione **lunghezza** $\mathrm{lh}\colon A^* \to \mathbb{N}$ associa ad ogni stringa $s \in A^*$ il numero di caratteri che compaiono in s, dove naturalmente poniamo $\mathrm{lh}\langle\rangle = 0$. Quindi se dobbiamo dimostrare un risultato sulle stringhe potremo usare l'induzione strutturale.

Se A è costituito da un unico elemento, diciamo $A = \{a\}$, allora

$$A^* = \{\langle\rangle, a, aa, aaa, aaaa, aaaaa, \dots\}$$

Osserviamo che in questo caso $\mathrm{lh}\colon A^* \to \mathbb{N}$ è biettiva.

1. Il calcolo proposizionale

Fissiamo un insieme L non vuoto i cui elementi si dicono **lettere proposizionali**. Le lettere proposizionali sono indicate dalle prime lettere dell'alfabeto $\mathrm{A}, \mathrm{B}, \mathrm{C}, \ldots$. L'insieme $\mathrm{Prop}(L)$ delle **proposizioni** su L è un sottoinsieme di

$$(L \cup \{(,), \neg, \vee, \wedge, \to, \leftrightarrow, \oplus\})^*$$

di tutte le stringhe finite di simboli che sono elementi di L oppure connettivi o parentesi. $\mathrm{Prop}(L)$ è definito dalle clausole

- Se $\mathrm{A} \in L$ allora $(\mathrm{A}) \in \mathrm{Prop}(L)$,
- Se $\mathrm{P} \in \mathrm{Prop}(L)$ allora $(\neg \mathrm{P}) \in \mathrm{Prop}(L)$,
- Se $\square$ è un connettivo binario, e se $\mathrm{P}, \mathrm{Q} \in \mathrm{Prop}(L)$ allora $(\mathrm{P} \square \mathrm{Q}) \in \mathrm{Prop}(L)$.

Le clausole della definizione sono anche regole di costruzione. S'intende che ogni proposizione si ottiene applicando un numero finito di volte le clausole della definizione. Le lettere $\mathrm{P}, \mathrm{Q}, \mathrm{R}, \ldots$ variano su elementi di $\mathrm{Prop}(L)$. Le proposizioni della forma (A) si dicono **proposizioni atomiche**.

Definizione 1.1. Per $n \in \mathbb{N}$ definiamo $\mathrm{Prop}_n(L)$ un sottoinsieme di $(L \cup \{(,), \neg, \vee, \wedge, \to, \leftrightarrow, \oplus\})^*$ mediante le clausole

$$\begin{aligned} \mathrm{Prop}_0(L) &= \{(\mathrm{A}) \mid \mathrm{A} \in L\} \\ \mathrm{Prop}_{n+1}(L) &= \{(\mathrm{P} \square \mathrm{Q}) \mid \mathrm{P}, \mathrm{Q} \in \mathrm{Prop}_n(L), \square \in \{\neg, \vee, \wedge, \to, \leftrightarrow, \oplus\}\} \\ &\quad \cup \{(\neg \mathrm{P}) \mid \mathrm{P} \in \mathrm{Prop}_n(L)\} \cup \mathrm{Prop}_n(L). \end{aligned}$$

Quindi $\mathrm{Prop}_0(L) \subseteq \mathrm{Prop}_1(L) \subseteq \ldots$ e

$$\mathrm{Prop}(L) = \bigcup_{n \in \mathbb{N}} \mathrm{Prop}_n(L)$$

La **lunghezza** di una proposizione P è la lunghezza di P vista come stringa,

$$\mathrm{lh}\colon \mathrm{Prop}(L) \longrightarrow \mathbb{N}$$

mentre l'**altezza** di una proposizione $\mathrm{ht}(\mathrm{P})$ è definita da

$$\mathrm{ht}\colon \mathrm{Prop}(L) \longrightarrow \mathbb{N} \qquad \mathrm{ht}(\mathrm{P}) = \min\{n \mid \mathrm{P} \in \mathrm{Prop}_n(L)\},$$

Per esempio se $\mathrm{P} = (\mathrm{A})$, allora $\mathrm{lh}(\mathrm{P}) = 3$ e $\mathrm{ht}(\mathrm{P}) = 0$.

La lunghezza e l'altezza di una proposizione si dicono **misure di complessità** e ci permettono di dimostrare fatti sulle proposizioni per induzione strutturale.

Proposizione 1.2. *Per ogni* $\mathrm{P} \in \mathrm{Prop}(L)$

- P *inizia con una parentesi* (, *termina con una parentesi*),
- *il numero di parentesi sinistre è uguale al numero di parentesi destre,*
- lh(P) *è divisibile per* 3.

DIMOSTRAZIONE. Dimostriamo il risultato per induzione strutturale.

Se $\mathrm{P} \in \mathrm{Prop}_0(L)$, allora $\mathrm{P} = (\mathrm{A})$ per qualche $\mathrm{A} \in L$ e il risultato segue immediatamente.

Supponiamo il risultato valga quando $\mathrm{P} \in \mathrm{Prop}_n(L)$ e dimostriamolo per $\mathrm{P} \in \mathrm{Prop}_{n+1}(L)$. Fissiamo dunque una $\mathrm{P} \in \mathrm{Prop}_{n+1}(L)$:

- Se $\mathrm{P} \in \mathrm{Prop}_n(L)$ il risultato segue immediatamente dall'ipotesi induttiva.
- Se $\mathrm{P} = (\mathrm{Q} \square \mathrm{R})$ con $\mathrm{Q}, \mathrm{R} \in \mathrm{Prop}_n(L)$, allora chiaramente P inizia con una parentesi (e termina con una parentesi); per ipotesi induttiva il numero di parentesi sinistre è uguale al numero di parentesi destre tanto per Q quanto per R, quindi il medesimo risultato vale per P; inoltre se $\mathrm{lh}(\mathrm{Q}) = 3n$ e $\mathrm{lh}(R) = 3m$, allora $\mathrm{lh}(\mathrm{P}) = 1 + 3n + 1 + 3m + 1 = 3(n + m + 1)$.
- Se $\mathrm{P} = (\neg \mathrm{Q})$ con $\mathrm{Q} \in \mathrm{Prop}_n(L)$, allora chiaramente P inizia con una parentesi (e termina con una parentesi); per ipotesi induttiva il numero di parentesi sinistre è uguale al numero di parentesi destre in Q, quindi il medesimo risultato vale per P; inoltre se $\mathrm{lh}(\mathrm{Q}) = 3n$, allora $\mathrm{lh}(\mathrm{P}) = 1 + 1 + 3n + 1 = 3(n + 1)$. □

ESEMPI 1.3. Siano $\mathrm{A}, \mathrm{B} \in L$.

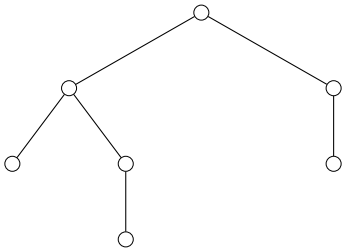
(1) $\mathrm{A} \wedge \mathrm{B}$ non è una proposizione, perché ogni proposizione contiene almeno una parentesi.
(2))A(non è una proposizione, come non lo sono A o)A), perché ogni proposizione inizia con una parentesi (e termina con una parentesi).
(3) $((\mathrm{A}) \to (\mathrm{B}))$ è una proposizione perché ottenuta dalle (A) e (B) con una applicazione della clausola induttiva relativa a $\to$.
(4) $(\neg((\mathrm{A}) \to (\mathrm{B})))$ è una proposizione perché ottenuta da (A) e (B) con una prima applicazione della clausola induttiva relativa a $\to$ e una seconda applicazione della clausola relativa a $\neg$.
(5) ((A) non è una proposizione perché in ogni proposizione il numero di parentesi sinistre è uguale al numero di parentesi destre.
(6) (AB) non è una proposizione perché non è atomica e non contiene nessun connettivo.

Se una proposizione è della forma $(\neg P)$ o della forma $(P \square Q)$, $\neg$ e $\square$ sono rispettivamente il suo connettivo principale, e P e Q le sottoproposizioni immediate.

1.A. Analisi sintattica. Una proposizione è una lista di simboli, ma è anche passibile di una rappresentazione con una diversa struttura. A ogni proposizione è associato un **albero di costruzione**, o di **analisi sintattica**,[1] che è un albero etichettato finito binario.

Un albero binario è un insieme X parzialmente ordinato, cioè con una relazione $\preceq$ con le seguenti proprietà: $\preceq$ è una relazione riflessiva, transitiva e antisimmetrica. Gli elementi dell'albero si chiamano **nodi**. Se $x \preceq y$, si dice che y è un **successore**, o un **discendente** di x. Esiste un nodo minimo r tale che $r \preceq x$ per ogni nodo di X, e si chiama **radice**. I nodi a tali che non esiste $b \neq a$ per cui $a \preceq b$ si chiamano foglie.[2] Ogni nodo che non sia una foglia ha uno o al massimo due successori immediati,[3] dove si dice che b è un successore immediato di a se $a \preceq b$, $a \neq b$ e non esiste un c tale che $a \preceq c \preceq b$, con $c \neq a$ e $c \neq b$.

La rappresentazione usuale di un albero binario è di questo tipo:



dove la radice è in alto e l'albero cresce verso il basso.

Un **ramo** è un insieme totalmente ordinato[4] di nodi che va dalla radice a una foglia. La sua lunghezza è il numero di nodi che vi appartengono. L'**altezza** dell'albero è la massima lunghezza dei suoi nodi.

Un albero si dice etichettato se ad ogni nodo è associato un elemento di qualche insieme prefissato, che si chiama etichetta (*label*). Le etichette si possono sovrapporre ed identificare con i nodi.

---

[1] In inglese *parsing*.

[2] Esistono sempre se l'albero, ovvero l'insieme dei nodi X, è finito.

[3] Un'altra terminologia è "figli". Se ci sonodue figli, s'intende che sono esplicitamente distinti il primo e il secondo — sulla pagina, a sinistra e a destra.

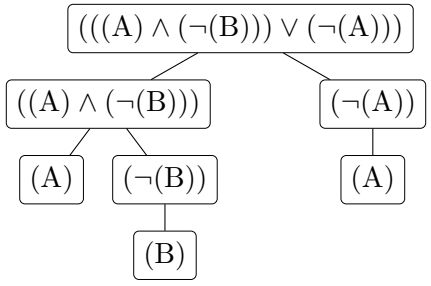
[4] Per ora basti intendere che due nodi qualunque del ramo sono confrontabili, quindi ogni nodo del ramo salvo l'ultimo ha esattamente un successore immediato, e con ogni nodo nel ramo ci sono tutti i suoi precedenti.

L'albero sintattico di una proposizione è definito in questo modo:

- la radice è (etichettata con) la proposizione data
- ogni nodo ha nessuno, uno o due successori immediati a seconda che la proposizione etichetta del nodo sia atomica, o della forma $(\neg P)$, o della forma $(P \square Q)$. Nel secondo caso il successore è etichettato con P, nel terzo caso i due successori sono etichettati rispettivamente con P e con Q.

Si chiama **altezza** della proposizione l'altezza del suo albero di costruzione.

ESEMPIO 1.4. L'albero per $(((A) \wedge (\neg(B))) \vee (\neg(B)))$ è il seguente:



La sua altezza è quattro.

Le etichette dei nodi dell'albero di costruzione di una proposizione sono le sue **sottoproposizioni**. Le lettere che compaiono nelle (proposizioni atomiche nelle) foglie sono le lettere che occorrono nella proposizione; si dice che un simbolo occorre in una proposizione se è un elemento della lista (che è la proposizione); le occorrenze di un simbolo in una proposizione sono i vari posti della lista in cui il simbolo si presenta. Se $A_1, \ldots, A_n$ sono le lettere che occorrono nella proposizione P, si scrive anche $P[A_1, \ldots, A_n]$. Qualche volta si usa questa notazione anche se $A_1, \ldots, A_n$ sono solo alcune delle lettere che occorrono in P, o viceversa se le lettere che occorrono in P sono incluse tra le $A_1, \ldots, A_n$; invece di introdurre notazioni distinte apposite, la differenza sarà chiarita dal contesto o da esplicite precisazioni.

Le parentesi sono essenziali per individuare il connettivo principale di una proposizione, e quindi per costruire il suo albero sintattico.

Alcune parentesi sono sovrabbondanti, ma solo quelle della coppia più esterna e quelle nelle proposizioni atomiche, dove sono usate sia per uniformità sia per sottolineare la differenza tra una lettera come elemento dell'alfabeto e la lettera come proposizione. Ma ora per comodità di scrittura e lettura è meglio ridurre il numero di parentesi con le seguenti convenzioni: non si scrivono le parentesi intorno alle lettere nelle proposizioni atomiche,

non si scrivono le parentesi più esterne, e si eliminano alcune coppie di parentesi intorno ad alcune sottoproposizioni, con un criterio sufficiente a farle ripristinare in modo corretto e univoco che è formulato nel seguente modo.

Si ordinano per priorità i connettivi secondo le seguente graduatoria:

$$\neg \quad \wedge \quad \vee \quad \oplus \quad \to \quad \leftrightarrow .$$

Data quindi una parola le cui parentesi non rispettano le condizioni per essere una proposizione (sì però la parità, il fatto che il numero di parentesi sinistre sia uguale a quello delle parentesi destre, il fatto che in ogni punto che non sia l'ultimo il numero di sinistre è maggiore o uguale di quello delle destre, e tutte le proprietà che si mantengono quando si eliminano alcune *coppie* di parentesi corrispondenti) le parentesi si rimettono secondo questo procedimento: prima si rimettono le parentesi a sinistra e a destra delle lettere; quindi si prende in esame la negazione, se occorre nella parola; si esamina un'occorrenza della negazione che non abbia immediatamente alla sua destra un'altra negazione. Alla sua destra c'è una parentesi sinistra — altrimenti si può dire che quella parola non proviene dalla eliminazione di coppie di parentesi da una genuina proposizione (brevemente, che non è una proposizione). Sia σ la parola alla sua destra che termina con la parentesi destra che chiude la parentesi sinistra. Per trovare la parentesi destra che "chiude" la parentesi sinistra si usa di nuovo il contatore in modo ovvio. Allora si rimette una parentesi sinistra alla sinistra della negazione, se non c'è già, e una parentesi destra a destra di σ, se non c'è già, ottenendo $(\neg\sigma)$; si ripete per ogni occorrenza di $\neg$, quindi si passa ai connettivi binari. Per ciascuno di essi, indicato con $\square$, nell'ordine di priorità, si considerano le più corte sottoparole σ e τ a sinistra e a destra di $\square$ che sono chiuse tra due parentesi sinistre e destre, e si introduce una parentesi (a sinistra di σ e) a destra di τ, se non ci sono già, ottenendo $(\sigma\square\tau)$, e così via.

Per occorrenze multiple dello stesso connettivo si prende in esame l'ultima, quella più a destra; questo significa che per formule composte con uno stesso connettivo ripetuto si conviene l'associazione a destra, cioè ad esempio con $\mathrm{A} \to \mathrm{B} \to \mathrm{C}$ si intende $\mathrm{A} \to (\mathrm{B} \to \mathrm{C})$, e con $\mathrm{A} \wedge \mathrm{B} \wedge \mathrm{C}$ si intende $\mathrm{A} \wedge (\mathrm{B} \wedge \mathrm{C})$.

Esempi 1.5. Data $\mathrm{A} \wedge \neg \mathrm{B} \vee \neg \mathrm{A}$, la reintroduzione delle parentesi avviene attraverso questa successione di passi:

(1) $(\mathrm{A}) \wedge \neg(\mathrm{B}) \vee \neg(\mathrm{A})$
(2) $(\mathrm{A}) \wedge \neg(\mathrm{B}) \vee (\neg(\mathrm{A}))$
(3) $(\mathrm{A}) \wedge (\neg(\mathrm{B})) \vee (\neg(\mathrm{A}))$
(4) $((\mathrm{A}) \wedge (\neg(\mathrm{B}))) \vee (\neg(\mathrm{A}))$
(5) $(((\mathrm{A}) \wedge (\neg(\mathrm{B}))) \vee (\neg(\mathrm{A})))$.

I passi 2 e 3 si possono naturalmente fare in parallelo.

Data $A \to \neg(B \wedge \neg\neg C)$

(1) $(A) \to \neg((B) \wedge \neg\neg(C))$
(2) $(A) \to \neg((B) \wedge \neg(\neg(C)))$
(3) $(A) \to \neg((B) \wedge (\neg(\neg(C))))$
(4) $(A) \to (\neg((B) \wedge (\neg(\neg(C)))))$
(5) $((A) \to (\neg((B) \wedge (\neg(\neg(C))))))$

oppure, per rendere più chiara la lettura

(1) $A \to \neg(B \wedge \neg(\neg C))$
(2) $A \to \neg(B \wedge (\neg(\neg C)))$
(3) $A \to (\neg(B \wedge (\neg(\neg C))))$
(4) $(A \to (\neg(B \wedge (\neg(\neg C)))))$

rimettendo infine le parentesi intorno alle lettere.

Si noti che se fosse stata data $A \to \neg B \wedge \neg\neg C$ la reintroduzione delle parentesi avrebbe portato a una diversa proposizione:

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

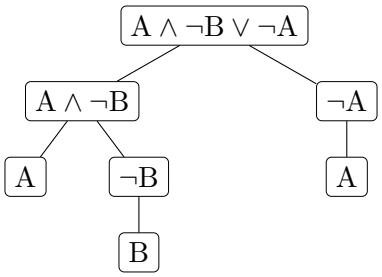
(esercizio, e si confrontino i due alberi sintattici), per cui le due parentesi lasciate in $A \to \neg(B \wedge \neg\neg C)$ sono essenziali, se si vuole parlare della proposizione $((A) \to (\neg((B) \wedge (\neg(\neg(C))))))$.

Non è comunque necessario né obbligatorio togliere tutte le parentesi; per agevolare la lettura, o all'inizio quando non si è ancora fatta esperienza, può essere conveniente lasciarne alcune, che pure grazie alle convenzioni si potrebbero eliminare. Così ad esempio si potrà scrivere $P \to (Q \wedge R)$ invece di $P \to Q \wedge R$ oppure $(P \vee Q) \to R$ invece di $P \vee Q \to R$.

Le parentesi si rimettono solo se si ha necessità di capire quale è il connettivo principale, per svolgere l'analisi sintattica. Le parentesi esterne possono tranquillamente essere tralasciate, finché la proposizione non deve essere combinata con altre mediante qualche connettivo — allora si devono rimettere.

L'albero sintattico si può costruire direttamente anche per le espressioni prive di tutte le parentesi, se si tiene presente la priorità dei connettivi. Il connettivo principale è sempre quello di priorità più bassa.

Esempio 1.6. L'albero sintattico per $A \wedge \neg B \vee \neg A$ è il seguente, essendo $\vee$ il connettivo principale:



Le etichette sono diverse, ma l'albero è lo stesso della proposizione analizzata in precedenza.

1.B. Esercizi.

(1) Discutere se le seguenti parole sono proposizioni:
   (A ∧ (B)
   (A)) ∧ B)
   ((A) ∧ B)
   ((A) ∧ (¬(B)))
   ((A) → ∧)
   A
   ((A)).

(2) Verificare quali delle seguenti parole sono proposizioni — secondo la definizione originaria — e quali no, costruendo l'albero sintattico e spiegando dove eventualmente la costruzione fallisce e per quale ragione:
   (¬(¬A))
   ((A) → ((B) ∨ (¬(C))))
   (¬¬((A) → (B)))
   ((((A) → (B)) ∧ (A)) → (B))
   ((¬(A)) ∧ (B)) ∨ (C))
   (((¬(A)) ∧ (B)) ∨ (C))
   ((A) ∧ (B) ∧ (C)).

(3) Dare ragioni per le seguenti proprietà:
   - Ogni proposizione ha lunghezza maggiore o uguale a 3.
   - In ogni proposizione non atomica occorre un connettivo.
   - In nessuna proposizione occorrono due connettivi consecutivi.
   - In nessuna proposizione occorre la sottosequenza (), né)A.
   - In ogni proposizione la sua lunghezza (come lista) è maggiore della sua altezza.

- In ogni proposizione, ogni suo segmento iniziale proprio contiene più parentesi sinistre che destre.
  [Suggerimento: la dimostrazione di queste proprietà per induzione sulla altezza delle proposizioni: si dimostrano prima per le proposizioni (A), quindi supponendo che valgano per proposizioni P, Q si dimostra che valgono anche per $(\neg P)$ e $(P \square Q)$.]

(4) Una misura di complessità delle proposizioni è una funzione

$$\mathrm{Prop}(L) \longrightarrow \mathbb{N}$$

che soddisfa la condizione che la misura di una proposizione è maggiore delle misure delle proposizioni componenti, e le atomiche hanno tutte la stessa misura minima. Il numero (di occorrenze) dei connettivi è una misura di complessità, come lo sono la lunghezza (della stringa) e l'altezza (dell'albero sintattico).

Trovare la relazione tra il numero di occorrenze di connettivi e l'altezza.

Dimostrare con un controesempio che il numero di connettivi diversi non è una misura di complessità.

(5) Eliminare le parentesi, applicando le convenzioni sulla priorità dei connettivi, dalle seguenti proposizioni:
$((A) \wedge ((\neg(B)) \to (\neg(C))))$
$((\neg(\neg(\neg(A)))) \vee ((A) \wedge (B)))$
$(((\neg(A)) \vee (\neg(B))) \wedge ((\neg(A)) \vee (B)))$
$(((A) \oplus (\neg(B))) \to ((A) \vee (\neg(B))))$.

(6) Reintrodurre le parentesi nelle seguenti parole in modo da ottenere, se possibile, proposizioni, o se no spiegare il perché:
$\neg\neg A$
$\neg A \wedge B \vee C$
$A \to B \vee \neg C$
$(A \to B) \wedge A \to B$
$A \to B \wedge A \to B$
$A \vee B \wedge C \to \neg A$
$A \wedge B \wedge C \vee \neg C$
$A \wedge (\to C \vee A)$
$A \oplus \neg B \to \neg A \oplus B$
$A \oplus B \vee C$.

(7) Definire le proposizioni nel seguente modo:
- Ogni lettera A è una proposizione;
- se P è una proposizione, anche $\neg(P)$ è una proposizione;
- se $\square$ è un connettivo binario e P e Q sono proposizioni, anche $(P)\square(Q)$ è una proposizione.

Definire il nuovo procedimento per decidere se una parola è una proposizione e costruire l'albero sintattico.

Discutere eventuali vantaggi e svantaggi della definizione alternativa.

1.C. Semantica. La semantica ha a che fare con le interpretazioni, grazie alle quali le proposizioni, con la sostituzione di frasi alle lettere, vengono ad assumere un senso (che a noi non interessa, lo bypassiamo) e diventano vere o false. Tale attribuzione *finale* di valori di verità è per noi l'operazione di interpretazione, che viene studiata in astratto per vedere se abbia proprietà generali, indipendenti dalle interpretazioni concrete.

I valori di verità saranno rappresentati dall'insieme $\{0,1\}$. Ci si colloca con tale scelta nell'ottica della logica classica a due valori.

Nell'insieme $\{0,1\}$ è necessario introdurre un minimo di struttura: la più semplice consiste in convenire che $0<1$ e usare la sottrazione come se 0 e 1 fossero numeri interi, con $|x|$ a indicare il valore assoluto.

Un'interpretazione è una funzione $i\colon L \longrightarrow \{0,1\}$; una valutazione è una funzione $v : \mathrm{Prop}(L) \to \{0,1\}$ che soddisfa le seguenti condizioni:[5]

$$\begin{aligned} v((\neg \mathrm{P})) &= 1 - v(\mathrm{P}) \\ v((\mathrm{P} \wedge \mathrm{Q})) &= \min\{v(\mathrm{P}), v(\mathrm{Q})\} \\ v((\mathrm{P} \vee \mathrm{Q})) &= \max\{v(\mathrm{P}), v(\mathrm{Q})\} \\ v((\mathrm{P} \oplus \mathrm{Q})) &= |v(\mathrm{P}) - v(\mathrm{Q})| \\ v((\mathrm{P} \to \mathrm{Q})) &= \max\{1 - v(\mathrm{P}), v(\mathrm{Q})\} \\ v((\mathrm{P} \leftrightarrow \mathrm{Q})) &= 1 - |v(\mathrm{P}) - v(\mathrm{Q})|\,. \end{aligned}$$

In alternativa, si considerano 0 e 1 come interi modulo[6] 2, $\{0,1\} = \mathbb{Z}_2$, e si scrivono le condizioni:

$$\begin{aligned} v((\neg \mathrm{P})) &= 1 + v(\mathrm{P}) \\ v((\mathrm{P} \wedge \mathrm{Q})) &= v(\mathrm{P}) \cdot v(\mathrm{Q}) \\ v((\mathrm{P} \vee \mathrm{Q})) &= v(\mathrm{P}) + v(\mathrm{Q}) + v(\mathrm{P}) \cdot v(\mathrm{Q}) \\ v((\mathrm{P} \oplus \mathrm{Q})) &= v(\mathrm{P}) + v(\mathrm{Q}) \\ v((\mathrm{P} \to \mathrm{Q})) &= 1 + v(\mathrm{P}) \cdot (1 + v(\mathrm{Q})) \\ v((\mathrm{P} \leftrightarrow \mathrm{Q})) &= 1 + (v(\mathrm{P}) + v(\mathrm{Q})). \end{aligned}$$

[5]Si noti che in $v\,((\neg \mathrm{A}))$ e in altre espressioni analoghe ci sono due tipi di parentesi, che andrebbero tipograficamente distinte; quelle interne sono le parentesi della proposizione, quelle esterne servono per la notazione funzionale $v(x)$.

[6]Per chi non sa cosa significa, l'importante è che $1+1=0$. In pratica i numeri sono divisi in due classi, quella dei pari, rappresentata da 0 e quella dei dispari, rappresentata da 1. La somma di due pari è pari, la somma di due dispari è pari ....

Ogni interpretazione i si estende a una valutazione i^* ponendo

$$i^*((\mathrm{A})) = i(\mathrm{A})$$

e definendo i^* sulle proposizioni composte in modo da soddisfare le condizioni della definizione di valutazione.

1.C.1. *Validità e conseguenza.* Se $i^*(\mathrm{A}) = 1$, si dice che A è **vera** nell'interpretazione i, o che i *soddisfa* A, o che i è un **modello** di A, e si scrive anche

$$i \models \mathrm{A}.$$

Se esiste almeno una i tale che $i \models \mathrm{A}$, si dice che A è *soddisfacibile*, o (semanticamente) **consistente**. Se non esiste alcun modello di A, si dice che A è **insoddisfacibile**, o (semanticamente) **inconsistente**, o **contraddittoria**, o una **contraddizione**. Se per ogni i si ha $i \models \mathrm{A}$, si dice che A è *logicamente valida*, o *logicamente vera*, o una *tautologia*, e si scrive

$$\models \mathrm{A}.$$

Si dice che B è **conseguenza logica** di A, o che A **implica** B, e si scrive

$$\mathrm{A} \models \mathrm{B}$$

se per ogni i, se $i \models \mathrm{A}$ allora $i \models \mathrm{B}$. Si noti che

Osservazione 1.7. Per ogni A e B,

$$\mathrm{A} \models \mathrm{B} \text{ se e solo se } \models \mathrm{A} \to \mathrm{B}.$$

Siccome $i \models \mathrm{A}_1 \wedge \ldots \wedge \mathrm{A}_n$ se e solo se $i \models \mathrm{A}_j$ per ogni $1 \leq j \leq n$, la definizione di modello si può generalizzare dicendo che i soddisfa un insieme di proposizioni T se e solo se $i \models \mathrm{A}$ per ogni $\mathrm{A} \in T$.

Quindi se A è $\mathrm{A}_1 \wedge \ldots \wedge \mathrm{A}_n$, invece di $\mathrm{A}_1 \wedge \ldots \wedge \mathrm{A}_n \models B$ si scrive $\{\mathrm{A}_1, \ldots, \mathrm{A}_n\} \models \mathrm{B}$, o anche $\mathrm{A}_1, \ldots, \mathrm{A}_n \models \mathrm{B}$.

Se $\mathrm{A} \models \mathrm{B}$ e $\mathrm{B} \models \mathrm{A}$, si dice che A e B sono **logicamente equivalenti**, o anche solo equivalenti, e si scrive $\mathrm{A} \equiv \mathrm{B}$.

Osservazione 1.8. Per ogni A e B,

$$\mathrm{A} \equiv \mathrm{B} \text{ se e solo se } \models \mathrm{A} \leftrightarrow \mathrm{B}.$$

Si noti che $\models$ e $\equiv$ sono segni metalinguistici, non connettivi.

Dalle definizioni semantiche segue immediatamente che

$$\mathrm{A}_1, \ldots, \mathrm{A}_n \models \mathrm{B} \text{ se e solo se } \{\mathrm{A}_1, \ldots, \mathrm{A}_n, \neg\mathrm{B}\} \text{ è insoddisfacibile.}$$

Questo significa che si può assumere come concetto semantico fondamentale sia quello di conseguenza logica sia quello di soddisfacibilità e a seconda

di quale sia privilegiato orientare diversamente la ricerca dei metodi più efficienti per rispondere alle domande semantiche.

La relazione di conseguenza logica è evidentemente transitiva: se $A \models C$ e $C \models B$ allora $A \models B$ (esercizio).

Lo stesso vale per la relazione di equivalenza logica.

Per mezzo di esse, dalle leggi elencate sopra se ne derivano altre; ad esempio dal *modus ponens* e dall'esportazione, con la prima, si ricava

sillogismo disgiuntivo: $A \wedge (\neg A \vee B) \to B$

Ma queste leggi soprattutto permettono di vedere che i connettivi $\oplus, \to, \leftrightarrow$ sono definibili in termini di $\neg, \wedge$ e $\vee$.

2. Linguaggi del prim'ordine

2.A. Simboli, termini e formule.

Simboli. Un linguaggio L del prim'ordine consiste dei seguenti oggetti:

- la parentesi aperta (e la parentesi chiusa),
- i simboli $\neg$, $\wedge$, $\vee$, $\to$, $\Leftrightarrow$, $\exists$, $\forall$ e $=$,
- una lista infinita di simboli detti **variabili**

$$v_0, v_1, v_2, \ldots$$

  Le lettere $x, y, z, \ldots$, eventualmente decorate con apici o pedici, indicano una generica variabile v_n,
- dei simboli di costante $c, d, e, \ldots$,
- dei simboli di funzione $f, g, h, \ldots$,
- dei simboli di predicato $P, Q, R, \ldots$

Ad ogni simbolo di funzione e di predicato è associato un numero intero positivo detto **arietà** del simbolo — i simboli di arietà 1, 2 e 3 si dicono, rispettivamente, simboli unari, binari e ternari. La arietà di f o di P è indicata con $\mathrm{ar}(f)$ e $\mathrm{ar}(g)$.

Termini. L'insieme dei **termini** di un linguaggio L è definito induttivamente dalle clausole:

- una variabile è un termine,

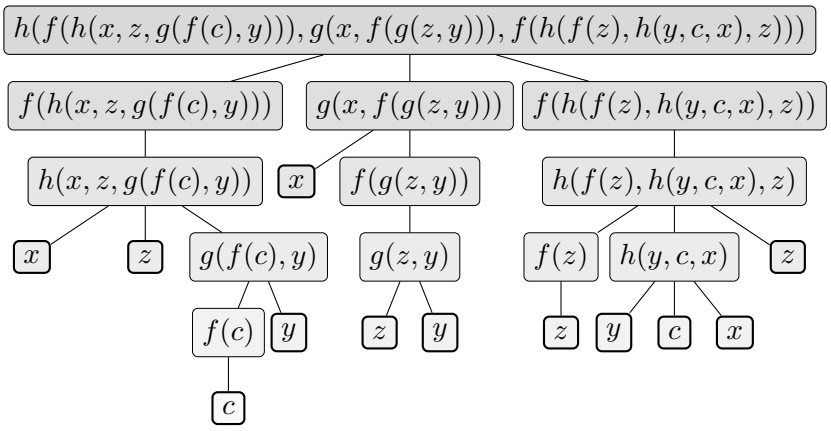


FIGURA 1. L'albero sintattico del termine descritto nella (12).

- un simbolo di costante è un termine,
- un'espressione del tipo $f(t_1, \ldots, t_n)$ è un termine, dove f è un simbolo di funzione n-ario e $t_1, \ldots, t_n$ sono termini.

Formalmente, se Vbl è l'insieme delle variabili, Const è l'insieme dei simboli di costante e Func è l'insieme dei simboli di funzione del linguaggio L , consideriamo l'insieme

$$\mathcal{S} = \Big(\{(,)\} \cup \mathrm{Vbl} \cup \mathrm{Const} \cup \mathrm{Func}\Big)^*$$

di tutte le stringhe di parentesi, variabili, simboli di costante e di variabile, e definiamo una funzione

$$\mathbb{N} \longrightarrow \mathscr{P}(\mathcal{S}), \qquad n \mapsto \mathrm{Term}_n$$

nel seguente modo:

$$\mathrm{Term}_0 = \mathrm{Vbl} \cup \mathrm{Const},$$
$$\mathrm{Term}_{n+1} = \{f(t_1, \ldots, t_n) \mid f \in \mathsf{F} \text{ e } t_1, \ldots, t_n \in \mathrm{Term}_n \text{ e } n = \mathrm{ar}(f)\}.$$

L'insieme dei termini è

$$\mathrm{Term} = \bigcup_{n \in \mathbb{N}} \mathrm{Term}_n .$$

Un termine t è una stringa di simboli (ottenuta secondo un protocollo ben definito), ma può essere visualizzato meglio mediante il suo **albero sintattico** in cui la radice è etichettata da t e gli altri nodi sono etichettati da termini che compongono t. Per esempio l' albero sintattico del termine

$$h(f(h(x, z, g(f(c), y))), g(x, f(g(z, y))), f(h(f(z), h(y, c, x), z))), \tag{12}$$

dove c è un simbolo di costante e f, g e h sono simboli di funzione di arietà 1, 2 e 3, è l'oggetto descritto nella Figura 1. I nodi terminali, cioè quelli che

non hanno nessun nodo al di sotto di essi, sono etichettati con le variabili e coi simboli di costante e sono evidenziati da una cornice più spessa. Potremmo anche semplificare la notazione etichettando ogni nodo non terminale il simbolo di funzione usata per costruire quel termine. In questo caso l'albero sintattico può essere disegnato come nella Figura 2.

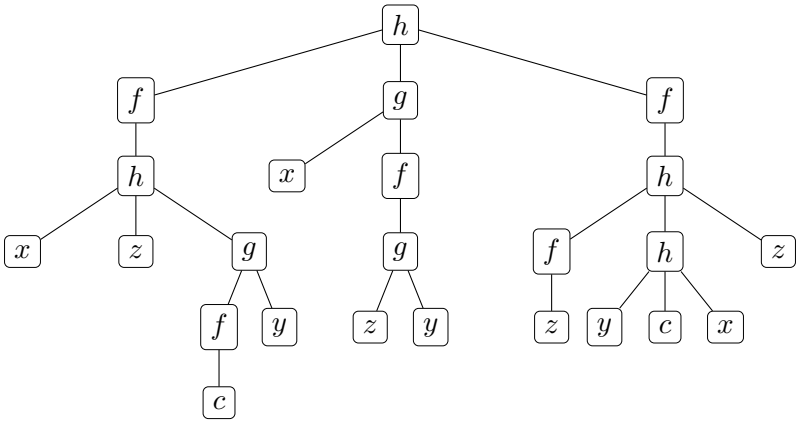


FIGURA 2. Una descrizione semplificata dell'albero sintattico della Figura 1.

Le parentesi (e le virgole) non sono strettamente necessarie per descrivere un termine, servono solo per agevolare la nostra lettura. Per esempio se sappiamo che $\mathrm{ar}(f) = 1$, $\mathrm{ar}(g) = 2$, $\mathrm{ar}(h) = 3$ e che c è una costante, il termine descritto in (12) può essere scritto come

$$hfhxzgfcygxfgzyfhfzhycxz.$$

Per rimettere al proprio posto le parentesi, si comincia ad individuare nella stringa qui sopra i termini di altezza 1, cioè le funzioni applicate a termini di altezza 0...

$$hfhxzg\,f(u)\,ygxf\,g(z,y)\,fh\,f(z)\;\;h(y,u,x)\,z$$

... passiamo poi a quell di altezza 2...

$$hfhxz\,g(f(u),y)\,gx\,f(g(z,y))\,f\,h(f(z),h(y,u,x),z)$$

... poi a quelle di altezza 3...

$$hf\,h(x,z,g(f(u),y)\;\;g(x,f(g(z,y))\;\;f(h(f(z),h(y,u,x),z)$$

... poi a quelli di altezza 4...

$$h\,f(h(x,z,g(f(u),y))\,g(x,f(g(z,y)))f(h(f(z),h(y,u,x),z)$$

... e a questo punto riotteniamo la scrittura (12).

NOTAZIONE. Se f è un simbolo di funzione binaria, si usa solitamente la notazione infissa $t_1\ f\ t_2$ invece di quella prefissa $f(t_1, t_2)$. In particolare scriveremo $t_1 + t_2$ e $t_1 \cdot t_2$ al posto di $+(t_1, t_2)$ e $\cdot(t_1, t_2)$.

Se f è un simbolo di funzione binaria, l'espressione $t_1 f \dots f t_n$ è ambigua, dato che dipende da dove inseriamo le parentesi. Per esempio, le possibili definizioni di $t_1\ f\ t_2\ f\ t_3$ sono due: $t_1\ f\ (t_2\ f\ t_3)$ e $(t_1\ f\ t_2)\ f\ t_3$. In generale, il numero di modi possibili di mettere le parentesi tra $n+1$ oggetti è dato da $\binom{2n}{n} - \binom{2n}{n-1}$. Per questo motivo introduciamo la seguente:

CONVENZIONE 1. Nell'espressione $t_1\ f\ \dots\ f\ t_n$ si intende sempre che si associa a destra, cioè $t_1\, f\, (t_2\, f\, (\dots (t_{n-1}\, f\, t_n) \dots))$. In particolare $t_1 + \dots + t_n$ sta per $t_1 + (\dots + (t_{n-1} + t_n) \cdots)$ e $t_1 \cdot \dots \cdot t_n$ sta per $t_1 \cdot (\dots \cdot (t_{n-1} \cdot t_n) \cdots)$. Utilizzeremo le abbreviazioni

$$nt \text{ al posto di } \underbrace{t + \dots + t}_{n} \quad \text{e} \quad t^n \text{ al posto di } \underbrace{t_1 \cdot \dots \cdot t_n}_{n}.$$

Infine, se f è un simbolo di funzione unaria e t è un termine, la scrittura

$$f^{(n)}(t)$$

denota il termine

$$\underbrace{f(\dots f}_{n \text{ volte}}(t) \dots).$$

Una misura di complessità per i termini è una funzione dall'insieme dei termini a valore nei numeri naturali tale per cui la complessità di un termine t sia sempre maggiore della complessità dei termini che concorrono a costruire t. Abbiamo due misure naturali di complessità per un termine t:

- $\mathrm{lh}(t)$, la **lunghezza** (incluse le parentesi) della stringa t e
- $\mathrm{ht}(t)$, l'**altezza** di t, cioè la massima lunghezza di un cammino nell'albero sintattico di t che parta dalla radice ed arrivi ad un nodo terminale.

Quindi se t è il termine descritto in (12) a pagina 59, allora $\mathrm{lh}(t) = 48$ e $\mathrm{ht}(t) = 5$.

OSSERVAZIONE 2.1. Le misure di complessità come lh e ht, sono utili per fare dimostrazioni per induzione sull'insieme dei termini. Per esempio, per verificare che ogni termine gode di una proprietà $\mathcal{P}$ si verifica che la proprietà $\mathcal{P}$ vale per i termini di complessità minima (caso base) e che se $\mathcal{P}$ vale per tutti i termini di complessità inferiore alla complessità di t, allora anche t gode della proprietà $\mathcal{P}$.

Formule. Una **formula atomica** è un'espressione della forma

$$P(t_1, \dots, t_n)$$

oppure della forma

$$t_1 = t_2$$

dove $t_1, t_2, \dots, t_n$ sono termini e P è un simbolo di predicato n-ario. L'insieme delle **formule** è definito induttivamente dalle clausole:

- una formula atomica è una formula,
- se φ è una formula, allora anche $(\neg\varphi)$ è una formula,
- se φ e ψ sono formule, allora anche $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \to \psi)$ e $(\varphi \Leftrightarrow \psi)$ sono formule,
- se φ è una formula e x è una variabile, allora anche $\exists x\varphi$ e $\forall x\varphi$ sono formule.

Useremo le lettere greche φ, ψ, e χ, variamente decorate, per le formule.Una formula della forma $\neg(\varphi)$ è detta negazione; analogamente, una formula della forma $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \to \psi)$, $(\varphi \Leftrightarrow \psi)$, $\exists x\varphi$ e $\forall x\varphi$ è detta, rispettivamente, congiunzione, disgiunzione, implicazione, bi-implicazione, **formula esistenziale** e **formula universale**. Una formula del linguaggio L si dice L-formula.

Convenzioni 1.(i) Per evitare l'eccessivo proliferare di parentesi, le sopprimeremo quando ciò non comporti ambiguità. Per esempio scriveremo $\varphi \wedge \psi$, $\varphi \vee \psi$, $\varphi \to \psi$ e $\varphi \Leftrightarrow \psi$ invece di $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, ...; ma se vogliamo prendere la negazione di una di queste formule reintrodurremo le parentesi. Seguiremo la convenzione che $\wedge$ e $\vee$ legano più fortemente di $\to$ e $\Leftrightarrow$, e che $\neg$ lega più fortemente di tutti gli altri connettivi. Quindi

$$\varphi \wedge \psi \to \chi, \quad \neg\varphi \vee \psi$$

sono abbreviazioni per

$$((\varphi \wedge \psi) \to \chi), \quad ((\neg\varphi) \vee \psi).$$

In analogia con quanto detto per i termini, se $\square$ è un connettivo binario (cioè diverso da $\neg$) scriveremo $\varphi_1 \square \dots \square \varphi_n$ al posto di $\varphi_1 \square (\varphi_2 \square (\dots \square \varphi_n) \dots)$.

(ii) Se P è un simbolo di relazione binario spesso useremo la notazione infissa $t_1\ P\ t_2$ al posto della notazione prefissa $P(t_1, t_2)$. In particolare, scriveremo $s < t$ invece di $<(s, t)$.

(iii) $t_1 \neq t_2$ è un'abbreviazione di $\neg(t_1 = t_2)$.

Una **sottoformula** di una formula φ è una formula usata per costruire φ. In altre parole:

- se φ è atomica, allora non ha sottoformule,
- se φ è $\neg\psi$, allora le sue sottoformule sono ψ e le sottoformule di ψ,

- se φ è $\psi \square \chi$ dove $\square$ è un connettivo binario, allora le sue sottoformule sono: ψ, χ, le sottoformule di ψ e le sottoformule di χ,
- se φ è $\exists x \psi$ o $\forall x \psi$, allora le sottoformule di φ sono ψ e tutte le sottoformule di ψ.

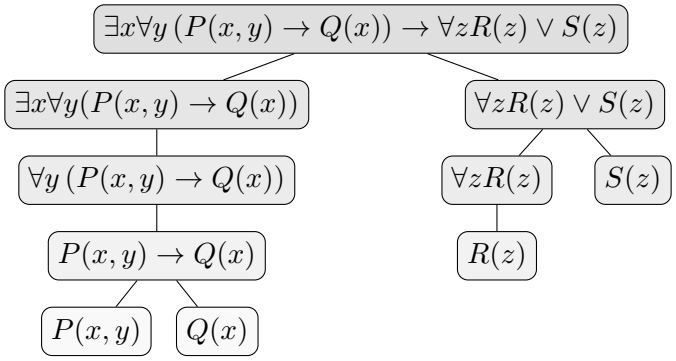
Per esempio, le sottoformule della formula

$$\exists x \forall y \, (P(x,y) \to Q(x)) \to \forall z R(z) \vee S(z) \tag{13}$$

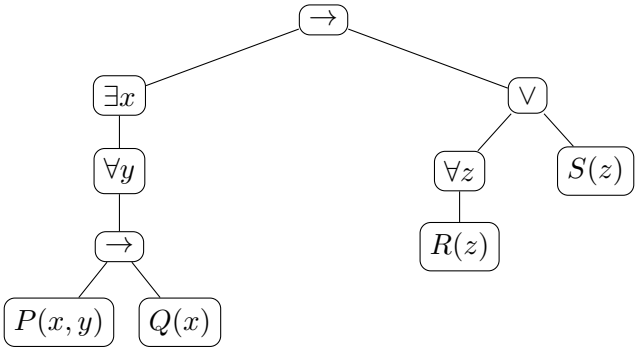
sono $\exists x \forall y \, (P(x,y) \to Q(x))$, $\forall z R(z) \vee S(z)$ e tutte le sottoformule di queste due. Quindi la lista completa delle sottoformule di (13) è:

$$\begin{array}{rr}
\exists x \forall y (P(x,y) \to Q(x)) & \forall z R(z) \vee S(z) \\
\forall y (P(x,y) \to Q(x)) & \forall z R(z) \\
P(x,y) \to Q(x) & R(z) \\
P(x,y) & S(z) \\
Q(x) &
\end{array}$$

Come per i termini, anche le formule possono essere descritte mediante alberi: l'albero sintattico della formula (13) è



o più semplicemente



Anche in questo caso abbiamo due nozioni di complessità: la lunghezza e l'altezza, definite in modo del tutto simile a quanto detto per i termini a pagina 61.

2.A.1. *Variabili libere e vincolate.* Ogni formula contiene una quantità finita di variabili e ogni volta che una variabile compare in una formula parleremo di **occorrenza della variabile nella formula**. Per esempio la variabile z occorre tre volte nella formula (13) a pagina 63: nelle prime due occorrenze la z è muta dato che dire $\forall z R(z)$ ha lo stesso significato di $\forall u R(u)$, cioè ogni oggetto gode della proprietà R, mentre la terza occorrenza serve per asserire che z gode della proprietà S. Le occorrenze del primo tipo si dicono **vincolate**,quelle del secondo tipo si dicono **libere**.

Definizione 2.2. Sia φ una formula e x una variabile.

- Se φ è atomica allora ogni occorrenza di x in φ è libera.
- Se φ è della forma $\neg\psi$ allora le occorrenze libere di x in φ sono esattamente quelle di x in ψ.
- Se φ è della forma $\psi\Box\chi$, dove $\Box$ è un connettivo binario, allora le occorrenze libere di x in φ sono quelle di x in ψ e quelle di x in χ.
- Supponiamo φ sia della forma $\exists y\psi$ oppure $\forall y\psi$. Se y è la variabile x, allora tutte le occorrenze di x in φ sono vincolate. Se invece y è una variabile diversa da x, allora le occorrenze libere di x in φ sono esattamente le sue occorrenze libere di x in ψ.

Diremo che la variabile x occorre libera in φ (equivalentemente: x è una variabile libera di φ) se c'è almeno un'occorrenza libera di x in φ. La notazione

$$\varphi(x_1, \ldots, x_n)$$

serve per porre in evidenziare il fatto che le variabili che occorrono libere in φ sono alcune tra le $x_1, \ldots, x_n$. (Non richiediamo che *ogni* $x_1, \ldots, x_n$ compaia libera o compaia del tutto in φ ed è perfettamente possibile che la formula non contenga alcuna variabile libera, o addirittura nessuna variabile.) L'insieme delle variabili libere di φ è indicato con

$$FV(\varphi).$$

Un **enunciato** o **formula chiusa** è una formula che non contiene variabili libere, cioè $FV(\varphi) = \emptyset$. La **chiusura universale di una formula** φ è la formula $\varphi^\forall$ ottenuta quantificando universalmente tutte le variabili libere di φ; se invece quantificando esistenzialmente tutte le variabili libere si ottiene **chiusura esistenziale** $\varphi^\exists$. Nell'uso comune le formule prive di quantificatori sono considerate equivalenti alla loro chiusura universale.

CAPITOLO VI

Formalizzazione

1. Dal linguaggio naturale alla logica

1.A. Predicati e relazioni nei linguaggi naturali. Noi saremo interessati a linguaggi simbolici in cui formiamo proposizioni a partire da nomi o da altre proposizioni mediante operazioni che corrispondono a modi di costruzione delle proposizioni che si trovano nei linguaggi naturali (in particolare, l'italiano). Nella logica matematica, tuttavia, resta ben poco della struttura altamente complessa di un linguaggio naturale. La semplificazione è guidata dalla volontà di restringersi ad espressioni matematiche. Per esempio, vengono dimenticati gli avverbi, i tempi, le persone ed i modi dei verbi, i verbi e gli aggettivi vengono in molti casi identificati. C'è una motivazione storica per questo impoverimento di struttura: nel ragionamento matematico, che è stata la motivazione principale per lo sviluppo della logica matematica, risulta superfluo considerare modo, tempo e persona dei verbi, e parti del discorso come avverbi. Si devono evitare ambiguità e ridondanze, con l'obiettivo di capire e far emergere la struttura logica.

Esempio 1.1. La frase

La vecchia porta la sbarra

è ambigua, dato che può essere intesa come

la vecchia signora trasporta un oggetto che risulta essere una sbarra

oppure come

l'antica porta, la sbarra

dove *la* si riferisce, presumibilmente, ad una strada.

Esempio 1.2. La frase

> Giovanni vede Mario che è malato e piange

è ambigua per ragioni di scansione, occorrono delimitatori come le virgole. Infatti questa frase potrebbe essere intesa come

> Giovanni vede Mario, il quale è malato e piange

oppure come

> Giovanni vede Mario che è malato, e a causa di ciò Giovanni piange.

Esempio 1.3. Come nell'Esempio precedente, la frase

> Se l'uomo sapesse realmente il valore che ha una donna andrebbe a quattro zampe alla sua ricerca[1]

cambia completamente significato a seconda di dove si inserisce la virgola: dopo *donna* oppure dopo *ha*.

Le frasi elementari nel linguaggio naturale sono di diverso tipo, ma in tutte si può individuare un soggetto, un verbo e un complemento (eventualmente più soggetti e più complementi, o nessuno). I verbi possono essere intransitivi o transitivi, ed esprimere stati o azioni.

Nella terminologia logica si introducono *proprietà* e *relazioni*; le primi corrispondono ai verbi intransitivi e alla copula "essere", le seconde ai verbi transitivi e corrispondono ai predicati introdotti nella Sezione 2.A del Capitolo V. Si dice che una proprietà è goduta da un soggetto, o che un soggetto ha una determinata proprietà o che soddisfa un predicato. Si dice anche che una proprietà è predicata di un soggetto, espressione dalla quale si vede il collegamento tra i due termini. Gli enti matematici che descrivono Con "la rosa è profumata" o "la rosa profuma" si esprime il fatto che la rosa ha una proprietà, quella di essere profumata. Lo stesso se si dice "la rosa ha profumo". Il verbo "avere" in generale indica possesso, ma non in questo caso. In "Giovanni ama Maria" invece[2] il verbo "amare" ha un soggetto e un complemento oggetto; in logica si dice che sussiste una relazione tra Giovanni e Maria, o che Giovanni e Maria stanno nell'ordine in una relazione, che è la relazione (non simmetrica) di amore.

[1] Questo esempio è dovuto alla scrittore e poeta argentino Julio Cortázar (1914–1984), il quale scrisse che "la virgola è la porta girevole del pensiero".

[2] O "Maria è amata da Giovanni", la distinzione tra forma attiva e passiva è inessenziale, salvo che dal punto di vista psicologico.

Tutti i verbi si potrebbero standardizzare nella forma della attribuzione di uno stato a uno o più termini, e questo corrisponderebbe ad avere un solo verbo, la copula "essere", nelle due versioni "essere qualcosa" per i verbi intransitivi e "essere nella relazione ... con" per i verbi transitivi. Questo è il motivo per cui nella trattazione formale si userà la dizione unica "predicati" per proprietà e relazioni, distinguendo quelli a un argomento (proprietà) da quelli a più argomenti (relazioni). Il "numero di argomenti" è il numero di entità a cui si applica il predicato. Ma informalmente si preferisce distinguere tra predicati in senso stretto (a un solo argomento, o predicati monadici), e relazioni (a più argomenti).

La frase "Giovanni dorme" può diventare "Giovanni ha la proprietà di stare dormendo" (o "Giovanni è addormentato", "Giovanni *sta* dormendo", "Giovanni è nello *stato* di sonno").

Le frasi matematiche elementari, uguaglianze e disuguaglianze, "è uguale a", "è minore di", rientrano in questa tipologia. Così quelle insiemistiche con "appartiene a", cioè "è un elemento di".

Alcune frasi possono essere rese sia mediante relazioni che mediante predicati; dipende da come si definiscono le relazioni e i predicati. In "Giovanni è amico di Mario" si può considerare la proprietà "essere amico di Mario" e attribuirla a Giovanni, oppure la relazione "essere amico di" e affermare che sussiste tra Giovanni e Mario.

Non si può dire che una sia giusta e l'altra no; dipende dal contesto; se dopo la prima osservazione si vuole aggiungere che Giovanni piange perché Mario è malato, e bisogna quindi citare di nuovo Mario, si deve usare il nome "Mario" e allora è meglio la versione relazionale, perché in quella con il predicato in nome "Mario" scompare, nella versione formalizzata, assorbito dal simbolo per il predicato: "essere amico di Mario" *in quanto* predicato, nell'analisi logica, è una unità linguistica non scomponibile, anche se espressa in italiano da una successione di parole tra le quali compare "Mario".

Le relazioni a due argomenti, come quelle viste negli esempi, si chiamano binarie. Le relazioni non sono solo binarie: "il punto C giace tra A e B" è un esempio di una relazione ternaria, o tra tre termini.

1.B. Termini nei linguaggi naturali. Vediamo come la nozione di termine, che è stata introdotta nella Sezione 2.A del Capitolo Vper i linguaggi del prim'ordine, è essere usata nei linguaggi naturali.

I soggetti o gli oggetti, più in generale i termini tra cui sussiste una

relazione, sono indicati da vari costrutti linguistici. Il più semplice è il nome proprio, come "Giovanni" e "Maria" — questi corrispondono alle costanti. Gli altri sono le descrizioni e i nomi comuni.

In "Maria ama il padre di Giovanni", "padre di Giovanni" è una descrizione, ben precisa, di una persona. Analogamente "il quadrato di 2" è una descrizione di un numero; entrambe le descrizioni sono ottenute applicando una funzione, nel primo caso "padre di" nel secondo "il quadrato di", a descrizioni più semplici, che in questi esempi sono nomi. Si possono dare descrizioni più complesse, come "la madre del padre di Giovanni" o "meno il quadrato di 2".

Nella grammatica, un ruolo fondamentale è svolto dai pronomi, che si presentano in grande varietà, come "uno", "chiunque", "ogni", "qualche" e simili.

I pronomi servono a formare nuove frasi collegandone alcune che hanno un riferimento in comune; nella frase "se uno ha un amico, è fortunato" si individuano due proposizioni componenti "uno ha un amico" e "è fortunato". La seconda frase non presenta il soggetto, ma s'intende che è lo stesso della prima; si può ripetere ("uno è fortunato") oppure più spesso, in altri casi, si deve precisare, con un indicatore che faccia capire esplicitamente che il soggetto è lo stesso (ad esempio "egli", "costui" e simili).

Nella seconda di due frasi collegate, il soggetto della prima può essere presente come oggetto, ad esempio in "se uno è generoso, tutti ne dicono bene", dove "ne" significa "di lui". Il simbolismo deve essere arricchito. L'uso dei pronomi è standardizzato per mezzo di simboli che si chiamano variabili: $x, y, \ldots$. Il simbolo x sta per "una cosa", "uno", "una persona" se il discorso si riferisce a esseri umani, "un numero" se il discorso si riferisce ai numeri e così via.

La variabile è creduta un elemento alieno del linguaggio, che compare solo nei simbolismi matematici, ma non è così. "Se uno ha un amico, è fortunato" equivale nella semiformalizzazione a: "se x ha un amico, x è fortunato".

La struttura di una frase del tipo "Giovanni dorme" è rappresentata da "dorme(Giovanni)", o

$$P(a).$$

"Giovanni ama Maria" da "ama(Giovanni, Maria)", o

$$R(a, b).$$

Più in generale, i termini a cui si applica la relazione non sono necessariamente costanti, o nomi, ma anche descrizioni, come "Il padre di Giovanni

ama Maria", che diventa

$$R(f(a), b),$$

o descrizioni incomplete, cioè contenenti variabili, come

$$\text{"Uno dorme":} \qquad P(x).$$

Tuttavia la rappresentazione grafica scelta per i simboli non è essenziale, per comodità di traduzione si possono anche usare altre lettere, come le iniziali delle parole italiane (A per "essere amici"), o addirittura complessi di lettere o parole intere, magari in caratteri particolari, come $\textsc{amici}(x, y)$.

Anche la particolare forma $R(a, b)$ non è rigida, talvolta può essere sostituita da $a\ R\ b$. Questo succede in particolare con i simboli per tradizionali relazioni matematiche che hanno adottato tale notazione: $x < y$, $x = y$.

1.C. Quantificatori nei linguaggi naturali. L'uso delle variabili o della loro versione con pronomi presenta aspetti delicati per trattare i quali il formalismo finora introdotto non è abbastanza discriminante.

Nella frase "se uno ha un amico, è fortunato" ci sono due tipi di "uno", il primo "uno" è il soggetto, presente tacitamente anche come soggetto di "è fortunato", e il secondo è l'"un" di "ha un amico".[3] Il primo "uno" significa "chi", nel senso di "chiunque", il secondo significa "qualche". La stessa parola "uno", e le corrispondenti variabili x e y possono cioè avere sia un senso universale che uno particolare.

La frase "uno che ha un amico è fortunato" diventa, schematizzata,

$$\forall x(\exists y(A(x, y)) \to F(x)),$$

dove A è un simbolo di predicato binario che designa la relazione di amicizia e F è il predicato unario che designa la proprietà di "essere fortunato".

Le variabili svolgono il ruolo di "uno", "una cosa", "un numero" e simili; di quale esattamente dipende dall'universo di discorso. Questo va precisato, in vari modi. Spesso la scelta dei predicati e delle relazioni suggerisce implicitamente di cosa si parla: se si usa una relazione A per "essere amico di ..." è implicito che si parla di persone o animali. Allora $\forall x(\exists y A(x, y) \to F(x))$ si legge "ogni persona o animale che abbia ...".

Tuttavia è difficile che il discorso entro il quale si inserisce $\forall x(\exists y A(x, y) \to F(x))$ si limiti a persone o animali; nel prosieguo possono essere menzionate anche cose o idee. Al di fuori della matematica, dove è di solito ben

[3]Non c'è differenza tra "uno" e "un"; si potrebbe dire in entrambi i casi "una persona", ristabilendo l'uniformità.

precisato,[4] l'universo di discorso è ricco e variegato. La formula $\forall x \ldots$ si legge dunque "per ogni x ..." dove x a priori può stare per gli elementi più disparati.

In molte frasi tuttavia i quantificatori chiaramente non si riferiscono a tutti gli elementi dell'universo di discorso ma a parti più ristrette; le frasi aritmetiche per esempio raramente iniziano con "tutti i numeri", piuttosto con "tutti i numeri positivi", o "tutti i numeri primi"; e raramente si parla di tutti gli esseri viventi, ma piuttosto di tutti gli uomini, o di tutte le donne, o di tutti gli italiani e così via restringendo.

Nel formalismo logico la restrizione dei quantificatori avviene nel seguente modo. La frase "tutti i tedeschi sono biondi" si rappresenta con due predicati, "tedesco" e "biondo", e la forma

$$\forall x(T(x) \to B(x)),$$

dove il quantificatore $\forall x$ è letto "per tutte le persone", cioè con la x che varia su tutto l'universo del discorso (la specie umana): "per ogni x, se x è tedesco allora x è biondo".

Questa forma è corretta grazie alle proprietà del condizionale, che vedremo meglio in seguito. Se $T(x) \to B(x)$ è vero per tutte le persone, allora ogni tedesco rende vero il condizionale, l'antecedente e quindi vero il conseguente, ed è vero che tutti i tedeschi sono biondi; se viceversa è vero che tutti i tedeschi sono biondi, anche l'enunciato di sopra che si riferisce con $\forall x$ non ai tedeschi ma a tutte le persone è vero: se uno è tedesco, allora è biondo e il condizionale è vero; se Giovanni è biondo ma non è tedesco, lo si vorrà considerare un controesempio che falsifica l'affermazione? Non sembra ragionevole; si assume che $T(\text{Giovanni}) \to B(\text{Giovanni})$ sia vero, e così $T(x) \to B(x)$ è vera per tutte le persone.

In pratica, gli aggettivi sono resi da predicati con l'ausilio del condizionale: in "tutte le persone tedesche sono bionde" l'aggettivo "tedesco" diventa il predicato "essere tedesco" e la frase "tutte le persone, se sono tedesche, sono bionde".

"Tutti i P sono ..." e "qualche P è ...", dove P delimita il campo di variabilità del riferimento, si realizzano dunque introducendo un predicato unario P e scrivendo rispettivamente $\forall x(P(x) \to \ldots)$ e $\exists x(P(x) \wedge \ldots)$. Si noti ovviamente la differenza nel caso del quantificatore esistenziale, dove la restrizione è realizzata con la congiunzione, che viene dalla traduzione di "esiste uno che è P e che ...".

[4]Non sempre: se si discute una equazione e non si precisa quale è il dominio numerico, le risposte possono essere bene diverse.

In particolare è da sottolineare che si usa un solo tipo di variabili; nella pratica matematica talvolta se ne usa più di uno, ad esempio in geometria lettere maiuscole $A, B, \ldots$ per punti e minuscole $r, s, \ldots$ per rette. Ma ci si riconduce a un solo tipo di variabili usando gli opportuni predicati, ad esempio "essere un punto" e "essere una retta".

1.D. Esempi tratti dal linguaggio naturale.

ESEMPIO 1.4. "Maria ama il padre di Giovanni" è formalizzata da

$$A(m, f(g)),$$

dove m e g sono costanti, m per "Maria" e g per "Giovanni", ed f un simbolo funzionale per "il padre di ...".

ESEMPIO 1.5. Per formalizzare "Maria ama il figlio di Giovanni" non si può usare un simbolo f per "il figlio di", perché "figlio di" non è una funzione univoca: a una persona possono corrispondere diversi figli, o nessuno. Allora "Maria ama il figlio di Giovanni" si formalizza come sotto "Maria ama un figlio di Giovanni" e a parte si afferma che Giovanni ha un solo figlio (vedremo come).

ESEMPIO 1.6. "Maria ama un figlio di Giovanni" è formalizzata da

$$\exists x(A(m, x) \wedge F(x, g)),$$

letta

esiste un x tale che Maria ama x e x è figlio di Giovanni,

dove F è un simbolo *relazionale* a due posti, e $F(x, y)$ sta per "x è figlio di y".

ESEMPIO 1.7. "Maria ama i figli di Giovanni", che significa che Maria ama tutti i figli di Giovanni, si formalizza con

$$\forall x(F(x, g) \to A(m, x))$$

e non con $\forall x(A(m, x) \wedge F(x, g))$; questa significa che tutti sono figli di Giovanni, e che Maria li ama tutti.

Per la formalizzazione corretta, può essere utile vedere nella frase un caso di quantificatore ristretto, ai figli di Giovanni, leggendola "Tutti i figli di Giovanni, Maria li ama" o al passivo: "Tutti i figli di Giovanni sono amati da Maria".

ESEMPIO 1.8. "Sono eligibili tutti e soli gli studenti in corso".

Non interessa a cosa siano eligibili; serve un predicato per "essere eligibile", uno per "essere studente" e uno per "essere in corso".

$$\forall x(E(x) \leftrightarrow S(x) \wedge C(x)).$$

La dizione "tutti e soli" è strettamente legata a "se e solo se". "Tutti gli studenti in corso sono eligibili" è formalizzata da

$$\forall x(S(x) \wedge C(x) \rightarrow E(x)),$$

mentre "solo gli studenti in corso sono eligibili" da

$$\forall x(E(x) \rightarrow S(x) \wedge C(x)).$$

La congiunzione di queste due ultime frasi è equivalente, come vedremo, alla prima.

1.E. Esempi tratti dalla matematica.

Esempio 1.9. La frase "dati due numeri, uno minore dell'altro, esiste un terzo numero compreso tra i due", vera nel campo dei razionali e in quello dei reali, falsa negli interi, può essere resa da

$$\forall x \forall y(x < y \rightarrow \exists z(x < z \wedge z < y)).$$

La congiunzione $x < z \wedge z < y$ si può abbreviare, secondo l'uso matematico, con $x < z < y$.

Non esiste un quantificatore che quantifichi sulle coppie; ci si comporta come se la frase fosse "dato un primo numero e dato un secondo numero ...". Ma "un primo" e "un secondo" servono solo a facilitare l'espressione, si sarebbe potuto dire anche "dato un numero e dato un numero ...", con qualche difficoltà nel seguito per i riferimenti appropriati.

Si faccia attenzione che neanche la presenza di "due" vuol dire che i numeri devono essere considerati diversi; tale forma comune di espressione distingue il modo, il momento in cui i numeri sono presentati, o pensati, ma non è escluso in generale che si presenti lo stesso numero due volte.

"Dati due numeri" significa "fatta due volte la scelta di un numero", e le scelte possono cadere sullo stesso numero. In termini probabilistici, si tratta di scelte con reimmissione; oppure si deve considerare che la scelta di un numero non lo toglie certo dall'insieme. "Dati due numeri, esiste la loro somma" si può scrivere

$$\forall xy \exists z(z = x + y)$$

ma esiste anche la somma di ogni numero con se stesso; x e y possono prendere tutti i valori in tutte le combinazioni possibili, quindi anche valori uguali.

Quando tuttavia si mette come sopra la condizione "uno minore dell'altro" — come nella frase proposta — allora si esclude che possano essere uguali perché la relazione "minore di" non è riflessiva. Tuttavia lo si esclude solo attraverso una deduzione, non con la semplice scrittura: se x e y denotano lo stesso numero, e bisogna considerare anche questo caso per verificare se la frase è vera, in $x < y \to \exists z(x < z \wedge z < y)$ l'antecedente $x < y$ risulta falso (come nell'esempio dei tedeschi).

Con "un terzo" di nuovo si vuol dire semplicemente "un numero", e che sia diverso dai primi due segue automaticamente se "compreso" significa "strettamente compreso"; altrimenti, se la relazione d'ordine fosse intesa come $\leq$ allora potrebbe anche essere uguale a uno dei due; non è questo il senso della frase, che vuole esprimere la densità dell'ordine dei numeri reali — e anche dei razionali.

Se nella stessa formula il segno di relazione è interpretato su di una relazione riflessiva, come

$$\forall x \forall y(x \leq y \to \exists z(x \leq z \wedge z \leq y)),$$

o più in generale "se R è riflessiva allora ...", ovvero

$$\forall x R(x, x) \to \forall x \forall y(R(x, y) \to \exists z(R(x, z) \wedge R(z, y))),$$

allora la formula è banalmente vera per ogni relazione.[5]

Esempio 1.10. "La relazione R è riflessiva", che significa che ogni elemento sta nella relazione R con se stesso, si scrive

$$\forall x R(x, x),$$

come abbiamo fatto sopra.

Esempio 1.11. "La relazione R è simmetrica", che significa che se la relazione R sussiste tra uno primo e un secondo elemento allora sussiste anche tra il secondo e il primo, si scrive

$$\forall x \forall y(R(x, y) \to R(y, x)).$$

Esempio 1.12. "La relazione R è transitiva", che significa che se R sussiste tra un primo elemento e un secondo, e tra questo e un terzo, allora sussiste anche tra il primo e il terzo, si scrive,

$$\forall x \forall y \forall z(R(x, y) \wedge R(y, z) \to R(x, z)).$$

Esempio 1.13. Come non esiste un quantificatore sulle coppie, così non esiste un quantificatore che esprima "esiste esattamente un ...", o "esiste un solo ...". Tale locuzione si realizza mediante l'uguaglianza come nel seguente esempio.

[5]Con "banalmente" s'intende che dati x e y come z si può prendere o x o y, e la formula non ci dà veramente informazioni.

La frase "dati due numeri, esiste un solo numero che è la loro somma" si formalizza come

$$\forall x \forall y \exists z (z = x + y \wedge \forall u (u = x + y \to u = z)).$$

In generale "Esiste un solo x tale che $P(x)$" si formalizza come

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

ESEMPIO 1.14. In modo analogo si può esprimere la locuzione "esistono esattamente due elementi tali che ..." (esercizio).

[Suggerimento. Si scriva prima "esistono almeno due elementi tali che ...", ricordando quanto detto nell'esempio 1.9 a proposito delle coppie di quantificatori.]

ESEMPIO 1.15. La frase "dati due numeri diversi tra loro, esiste un numero che è propriamente compreso tra i due numeri dati" si rappresenta con

$$\forall x \forall y (x \neq y \to \exists z (x < z < y \vee y < z < x)).$$

dove $x \neq y$ è un'abbreviazione per $\neg(x = y)$.

ESEMPIO 1.16. La frase "ogni numero positivo ha una radice quadrata", vera nei reali, falsa nei razionali, si rappresenta come

$$\forall x (0 < x \to \exists y (x = y^2)),$$

dove con y^2 si indica la funzione potenza di esponente 2.

ESEMPIO 1.17. "Un numero è divisibile per un altro numero se e solo se esiste un terzo numero che moltiplicato per il secondo dà il primo".

Scriviamo $x \mid y$ per "y è divisibile per x" o "x divide y" e usiamo il solito segno di moltiplicazione:

$$\forall x \forall y (x \mid y \leftrightarrow \exists z (y = x \cdot z)),$$

ma di nuovo si noti che x, y, z non devono necessariamente indicare numeri tutti diversi tra loro.

ESEMPIO 1.18. "Esistono due numeri primi consecutivi".

Per questa frase complicata procediamo in due passi; usiamo un'abbreviazione $\mathrm{pr}(x)$ per "x è primo " e scriviamo

$$\exists x \exists y (x = y + 1 \wedge \mathrm{pr}(x) \wedge \mathrm{pr}(y))$$

riservandoci di sostituire $\mathrm{pr}(x)$ con la sua scrittura corretta data nel prossimo esercizio.

Che i numeri siano due non risulta dallo scrivere $\exists x \exists y$ ma da $x = y + 1$ che implica $x \neq y$ (lo si deduce facilmente dagli assiomi dei numeri naturali); si potrebbe anche scrivere:

$$\exists x(\mathrm{pr}(x) \wedge \mathrm{pr}(x+1)),$$

dando per scontato, come sopra, che $x \neq x + 1$.

Esempio 1.19. "Un numero è primo se e solo se è maggiore di 1 ed è divisibile solo per 1 e per se stesso".

Per esprimere questa che è la definizione di un nuovo predicato usiamo un nuovo simbolo $\mathrm{pr}(x)$ e scriviamo

$$\forall x(\mathrm{pr}(x) \to x > 1 \wedge \forall z(z \mid x \to z = 1 \vee z = x))$$

Esempio 1.20. "2 è l'unico numero primo pari".

"Numero pari" significa "divisibile per 2". La frase si può trasformare in "2 è primo e pari e se un numero è primo e pari allora è uguale a 2". Quindi

$$\mathrm{pr}(2) \wedge 2 \mid 2 \wedge \forall x(\mathrm{pr}(x) \wedge 2 \mid x \to x = 2).$$

Esempio 1.21. "3 è dispari"

Il predicato "dispari" si può definire come "non pari" e quindi

$$\neg(2 \mid 3),$$

oppure dicendo che un numero dispari è della forma $2 \cdot y + 1$, e in aritmetica si dimostra che le due definizioni sono equivalenti, quindi

$$\exists y(3 = 2 \cdot y + 1).$$

Esempio 1.22. "Ogni primo maggiore di 2 è dispari" è un caso di quantificatore ristretto, ma lo si può restringere in due modi: ai numeri primi oppure ai numeri primi maggiori di 2. Il predicato "essere primo maggiore di 2" si può definire con $(\mathrm{pr}(x) \wedge x > 2)$ e si ha allora, se si scrive $\mathrm{disp}(x)$ per "x è dispari ",

$$\forall x((\mathrm{pr}(x) \wedge x > 2) \to \mathrm{disp}(x)).$$

Oppure se si restringe solo ai primi si deve scrivere

$$\forall x(\mathrm{pr}(x) \to (x > 2 \to \mathrm{disp}(x))).$$

In questo caso le parentesi interne servono a evidenziare la composizione corretta della frase mediante le due occorrenze del condizionale.

Esempio 1.23. "Esistono numeri pari arbitrariamente grandi".

La locuzione "arbitrariamente grandi" o "grandi quanto si vuole" significa che comunque si dia un numero, ne esiste uno più grande con la proprietà in

oggetto — non che un numero è grande quanto si vuole, un numero è quello che è. Quindi

$$\forall x \exists y (x < y \wedge 2 \mid y).$$

ESEMPIO 1.24. "Ci sono almeno due quadrati minori di 10".

Consideriamo 10 una costante (in realtà è un termine complesso). "x è un quadrato" significa che x è il quadrato di qualche numero, e si formalizza come $\exists u(x = u^2)$. Quindi

$$\exists x \exists y (x \neq y \wedge x < 10 \wedge y < 10 \wedge \exists u(x = u^2) \wedge \exists u(y = u^2)).$$

Si noti che da $\exists u(x = u^2) \wedge \exists u(y = u^2))$ non segue che la u sia la stessa, e quindi x e y uguali; le due frasi sono indipendenti; è come se si dicesse: "esiste *un numero* il cui quadrato è x ed esiste *un numero* il cui quadrato è y"; non vuol dire che sia lo stesso numero. Ma si sarebbe potuto anche scrivere $\exists u(x = u^2) \wedge \exists v(y = v^2))$.

ESEMPIO 1.25. "Per due punti passa una e una sola retta".

Primo modo. Usiamo variabili diverse per punti e rette e una relazione binaria Q per "un punto giace su una retta".

$$\forall A \forall B \exists r (Q(A, r) \wedge Q(B, r) \wedge \forall s (Q(A, s) \wedge Q(B, s) \to r = s))$$

Secondo modo. Usiamo un solo tipo di variabili e due predicati P per "essere un punto" e R per "essere una retta".

$$\forall x \forall y (P(x) \wedge P(y) \to \exists z (R(z) \wedge Q(x, z) \wedge Q(y, z) \wedge \forall u (R(u) \wedge Q(x, u) \wedge Q(y, u) \to z = u)).$$

Le due soluzioni sono equivalenti; nella prima si usa un linguaggio a due sorta di variabili, che ha le stesse proprietà logiche di quello con una sola sorta.

ESEMPIO 1.26. "La funzione $y = x^3$ è iniettiva e suriettiva" si formalizza

$$\forall x_1 \forall x_2 (x_1 \neq x_2 \to x_1^3 \neq x_2^3) \wedge \forall y \exists x (y = x^3),$$

in un linguaggio che abbia un simbolo funzionale indicato con x^3.

ESEMPIO 1.27. L'affermazione che la relazione "$y = 2 \cdot x$" è una relazione funzionale e iniettiva è formalizzata da:

$$\forall x \exists y (y = 2 \cdot x \wedge \forall z (z = 2 \cdot x \to z = y)) \wedge \forall x_1 \forall x_2 (x_1 \neq x_2 \to 2 \cdot x_1 \neq 2 \cdot x_2).$$

Dagli esempi si traggono diverse regole euristiche: riformulare la frase in un italiano semplice, con soggetto, verbo e complementi; trasformare i pronomi quantitativi come "ognuno", "alcuni", "nessuno", "uno" ... usando sempre solo "per tutti ..." ed "esiste un ...", anche se la frase diventa

barocca; guardare i verbi, se sono intransitivi o transitivi, e sostituire le frasi elementari con le dizioni "ha la proprietà ..." e "sussiste la relazione ..."; non prendere relazioni troppo inglobanti che nascondano la sintassi informale, immaginando possibili proseguimenti della frase che richiedono di riprendere certi elementi; invece lasciare cadere particolari empirici; nelle frasi matematiche, risalire sempre alle definizioni dei termini coinvolti.

1.E.1. *Ancora esempi.* Si assuma come universo di discorso l'insieme degli interi positivi, $\mathbb{Z}_+ = \{1, 2, 3, \ldots\}$, e si utilizzi il seguente vocabolario:

$$\begin{aligned} x \text{ divide } y &\rightsquigarrow x \mid y \\ \text{la somma di } x \text{ e } y &\rightsquigarrow x + y \\ x \text{ è minore di } y &\rightsquigarrow x < y \\ x \text{ è un numero primo} &\rightsquigarrow \mathrm{Pr}(x) \end{aligned}$$

Si usino liberamente i numerali $1, 2, 3, \ldots$ come costanti.

(1) "Se un numero è minore di un altro, allora quest'ultimo non è minore del primo"
$$\forall x, y\, (x < y \to \neg(y < x)).$$

(2) "Nessun numero è minore di ogni numero"
$$\neg\exists x\, \forall y\, (x < y)$$
o, equivalentemente:
$$\forall x\, \exists y\, \neg(x < y)$$

(3) "Ogni numero è minore di qualche numero"
$$\forall x\, \exists y\, (x < y)$$

(4) "Ogni numero pari è la somma di due numeri dispari"
$$\forall x\, (2 \mid x \to \exists n, m\, (\neg(2 \mid n) \wedge \neg(2 \mid m) \wedge x = n + m))$$

(5) "Solo 1 è minore di ogni numero pari"
$$\forall x\, (x = 1 \leftrightarrow \forall y\, (2 \mid y \to x < y))$$

(6) "Tutti i numeri tranne 1 sono maggiori di qualche numero"
$$\forall x\, (\exists y\, (y < x) \to x \neq 1)$$

(7) "Il numero minore di 2 è dispari"
$$\exists x\, (x < 2 \wedge \neg(2 \mid x) \wedge \forall y\, (y < 2 \to y = x)).$$

(8) (Teorema di Euclide) "Esistono numeri primi arbitrariamente grandi"
$$\forall x\, \exists y\, (\mathrm{Pr}(y) \wedge x < y)$$

Naturalmente, nella formalizzazione del teorema di Euclide, si può rimpiazzare il predicato $\mathrm{Pr}(y)$ con la sua definizione:

$$1 < y \wedge (\forall z\,(z \mid y \to z = 1 \vee z = y))$$

e la formula finale diventa

$$\forall x\,\exists y\,(x < y \wedge (1 < y \wedge (\forall z\,(z \mid y \to z = 1 \vee z = y))))$$

(9) (Congettura di Goldbach) "Ogni numero pari maggiore di 2 è somma di due primi".

$$\forall x\,((2 < x \wedge 2 \mid x) \to \exists n \exists m\,(\mathrm{Pr}(n) \wedge \mathrm{Pr}(m) \wedge x = n + m))$$

Come esercizio riassuntivo, si formalizzi la proposizione usando solo l'ordinamento $<$, la costante 2, la somma $+$ e la relazione di divisibilità $\mid$.

(10) Formalizzare le seguenti frasi usando il simbolo f:

- f è iniettiva
$$\forall x, y\,(f(x) = f(y) \to x = y)$$
- f è suriettiva
$$\forall x\,\exists y\,(x = f(y))$$
- f è biettiva
$$\forall x, y\,(f(x) = f(y) \to x = y) \wedge \forall x\,\exists y\,(x = f(y))$$
- f è una involuzione, cioè la composizione di f con se stessa è l'identità.
$$\forall x\ (f(f(x)) = x)$$

CAPITOLO VII

Cardinalità

1. Insiemi equipotenti

Due insiemi X e Y sono **equipotenti**, in simboli

$$X \approx Y,$$

se c'è una funzione $f\colon X \to Y$ biettiva. La relazione $\approx$ è una relazione di equivalenza; spesso diremo che due insiemi equipotenti X e Y hanno la medesima **cardinalità** e scriveremo

$$|X| = |Y|.$$

Per definizione, un insieme è **finito** se e solo se è in biezione con $\{0, \dots, n-1\}$, per qualche $n \in \mathbb{N}$, dove poniamo $\{0, \dots, n-1\} = \emptyset$ quando $n = 0$. Se X è finito scriveremo

$$|X| = n.$$

Un insieme X **si inietta in** Y, in simboli

$$X \precsim Y$$

se c'è una funzione iniettiva $f\colon X \to Y$; in questo caso scriveremo che

$$|X| \leq |Y|.$$

Proposizione 1.1. *Se $X \precsim Y$ e $X \neq \emptyset$, allora c'è una suriezione $\pi\colon Y \to X$.*

Dimostrazione. Sia $f\colon X \to Y$ iniettiva e sia $x_0 \in X$. Definiamo

$$\pi(y) = \begin{cases} f^{-1}(y) & \text{se } y \in \operatorname{ran} f \\ x_0 & \text{altrimenti.} \end{cases}$$

□

Il simbolo $\leq$ suggerisce che si tratti di una relazione di ordine sulle cardinalità: la proprietà riflessiva e transitiva sono immediate, mentre la proprietà antisimmetrica è garantita dal seguente risultato.

Teorema 1.2 (Cantor-Schröder-Bernstein). *Se $X \precsim Y$ e $Y \precsim X$ allora $X \approx Y$.*

DIMOSTRAZIONE. Fissiamo due funzioni iniettive $f\colon X \to Y$ e $g\colon Y \to X$. Sia $\Phi\colon \mathscr{P}(X) \to \mathscr{P}(X)$ la funzione

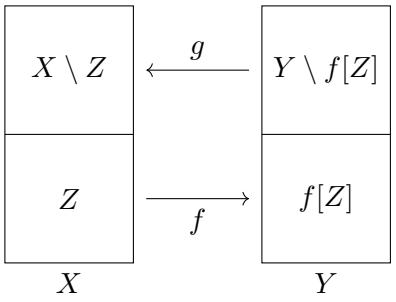
$$\Phi(Z) = X \setminus g[Y \setminus f[Z]].$$

Se $Z_1 \subseteq Z_2$ allora $f[Z_1] \subseteq F[Z_2]$, quindi $Y \setminus f[Z_1] \supseteq Y \setminus f[Z_2]$, quindi $g[Y \setminus f[Z_1]] \supseteq g[Y \setminus f[Z_2]]$, da cui $X \setminus g[Y \setminus f[Z_1]] \subseteq X \setminus g[Y \setminus f[Z_2]]$. Abbiamo quindi dimostrato che

$$Z_1 \subseteq Z_2 \to \Phi(Z_1) \subseteq \Phi(Z_2).$$

Poiché il reticolo $\mathscr{P}(X)$ è completo le ipotesi del Teorema del punto fisso di Tarski-Knaster **??** sono soddisfatte, quindi esiste un $Z \subseteq X$ tale che $\Phi(Z) = Z$, ovvero $X \setminus Z = g[Y \setminus f[Z]]$. Poiché g è iniettiva, g^{-1} è una biezione tra $X \setminus Z$ e $Y \setminus f[Z]$, quindi la funzione $h\colon X \to Y$

$$h(x) = \begin{cases} f(x) & \text{se } x \in Z \\ g^{-1}(x) & \text{se } x \in X \setminus Z \end{cases}$$



è una biezione. □

2. Insiemi numerabili

Un insieme si dice **numerabile** se è in biezione con $\mathbb{N}$.

PROPOSIZIONE 2.1. *Se $X \subseteq \mathbb{N}$ non è finito, allora è numerabile.*

DIMOSTRAZIONE. Sia $f\colon \mathbb{N} \to X$ la funzione definita per ricorsione da

$$\begin{aligned} f(0) &= \min X \\ f(n+1) &= \min\left(X \setminus \{f(0), \dots, f(n)\}\right). \end{aligned}$$

Osserviamo che f è ben definita: l'insieme $X \setminus \{f(0), \dots, f(n)\}$ è non vuoto, visto che X non è finito. Per costruzione $f(n) < f(n+1)$, quindi f è strettamente crescente, quindi iniettiva. Verifichiamo che f è suriettiva. Se per assurdo $X \setminus \operatorname{ran} f \neq \emptyset$, per il principio del minimo sia $x = \min(X \setminus \operatorname{ran} f)$. Abbiamo bisogno del seguente risultato.

ESERCIZIO 2.2. Dimostrare per induzione che se $g\colon \mathbb{N} \to \mathbb{N}$ è strettamente crescente allora $\forall k \in \mathbb{N}\,(k \leq g(k))$.

Poiché f è strettamente crescente, allora $f(x) \geq x$. Quindi $\{k \in \mathbb{N} \mid f(k) \geq x\} \neq \emptyset$. Per il principio del minimo sia $n = \min\{k \mid f(k) \geq x\}$. Dato che $x \notin \operatorname{ran} f$, allora $f(n) > x$. Poiché $f(0) = \min X \leq x$, allora $0 < n$, cioè $n = m + 1$ per qualche m. Per minimalità di n, allora $f(m) < x \in X$ e $f(m) \in X$, quindi $f(m+1) \leq x$: contraddizione. □

PROPOSIZIONE 2.3. *Se $f\colon \mathbb{N} \to Y$ è suriettiva, allora Y è finito oppure numerabile.*

DIMOSTRAZIONE. Supponiamo Y non sia finito. La funzione $g\colon Y \to \mathbb{N}$

$$g(y) = \min\{n \in \mathbb{N} \mid f(n) = y\}$$

è iniettiva, dato che f è una funzione, e $X \stackrel{\text{def}}{=} \operatorname{ran} g$ è un sottoinsieme infinito di $\mathbb{N}$. Ne segue che c'è una biezione $h\colon \mathbb{N} \to X$, quindi $g^{-1} \circ h\colon \mathbb{N} \to Y$ è una biezione. □

TEOREMA 2.4. $\mathbb{N} \times \mathbb{N} \approx \mathbb{N}$.

PROPOSIZIONE 2.5. *Se X e Y sono numerabili, allora anche $X \cup Y$ è numerabile.*

DIMOSTRAZIONE. Se $f\colon \mathbb{N} \to X$, e $g\colon \mathbb{N} \to Y$ sono biezioni, allora $h\colon \mathbb{N} \to X \cup Y$, $h(2n) = f(n)$ e $h(2n+1) = g(n)$, è una suriezione. Poiché $X \cup Y$ è infinito, allora $X \cup Y \approx \mathbb{N}$. □

ESEMPIO 2.6. $\mathbb{Z}$ è numerabile, dato che $\mathbb{N}$ e $\{k \in \mathbb{Z} \mid k < 0\}$ sono numerabili.

DIMOSTRAZIONE. Dobbiamo definire una biezione $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$. Per esempio la funzione

$$f(n) = \begin{cases} (0,0) & \text{se } n = 0, \\ (k,m) & \text{se } n = 2^k \cdot (2m+1). \end{cases}$$

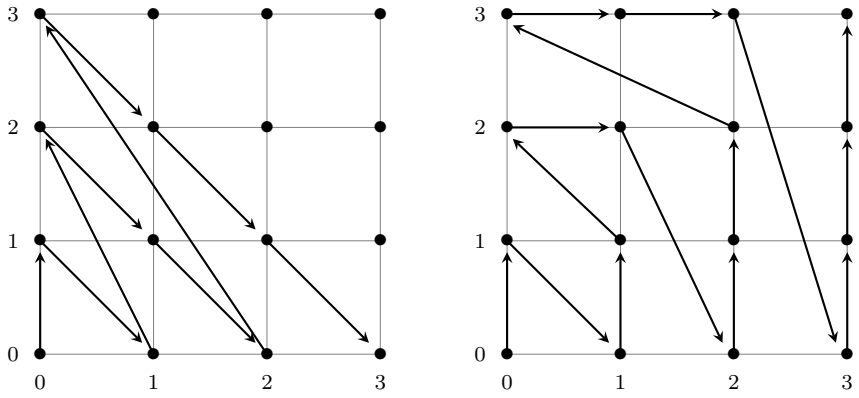
In effetti ci sono moltissime biezioni tra $\mathbb{N}$ e $\mathbb{N} \times \mathbb{N}$. Nella Figura 1 sono descritte due metodi importanti per enumerare $\mathbb{N} \times \mathbb{N}$:

- l'**enumerazione diagonale** o **triangolare**, ottenuta enumerando $\mathbb{N}^2$ secondo l'ordinamento

$$(x,y) \lhd_T (x',y') \Leftrightarrow x + y < x' + y' \vee [x + y = x' + y' \wedge x < x'],$$

- l'**enumerazione quadrata**, ottenuta enumerando $\mathbb{N}^2$ secondo l'ordinamento

$$\begin{aligned}(x,y) \lhd_Q (x',y') \Leftrightarrow \big(&\max(x,y) < \max(x',y') \\ &\vee [\max(x,y) = \max(x',y') \wedge (x < x' \vee [x = x' \wedge y < y'])]\big),\end{aligned}$$



Enumerazione triangolare Enumerazione quadrata

FIGURA 1. Enumerazioni di $\mathbb{N} \times \mathbb{N}$

□

Entrambe le biezioni $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$ sono utili, ma quella diagonale ha il vantaggio di avere un'espressione analitica particolarmente semplice: la funzione $\boldsymbol{J} \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ la cui inversa enumera diagonalmente $\mathbb{N} \times \mathbb{N}$ è data da

$$\boldsymbol{J}(x, y) = \frac{1}{2}(x + y)(x + y + 1) + x. \tag{14}$$

Ogni biezione $f \colon X \to Y$ induce una biezione

$$\mathscr{P}(X) \to \mathscr{P}(Y), \quad A \mapsto f[A] = \{f(x) \mid x \in A\}$$

In particolare $\mathscr{P}(\mathbb{N} \times \mathbb{N}) \approx \mathscr{P}(\mathbb{N})$.

TEOREMA 2.7. $\mathbb{Q}$ *è numerabile.*

DIMOSTRAZIONE. Le funzioni

$$\mathbb{N} \times \mathbb{N} \to \mathbb{Q}_{\geq 0} \stackrel{\text{def}}{=} \{q \in \mathbb{Q} \mid q \geq 0\}, \qquad (n, m) \mapsto \frac{n}{m+1}$$

$$\mathbb{N} \times \mathbb{N} \to \mathbb{Q}_{<0} \stackrel{\text{def}}{=} \{q \in \mathbb{Q} \mid q < 0\}, \qquad (n, m) \mapsto -\frac{n+1}{m+1}$$

sono suriettive, quindi componendo con una biezione $\mathbb{N} \approx \mathbb{N} \times \mathbb{N}$ si ha che $\mathbb{N}$ si surietta su $\mathbb{Q}_{\geq 0}$ e su $\mathbb{Q}_{<0}$. Poiché $\mathbb{Q}_{\geq 0}$ e $\mathbb{Q}_{<0}$ sono infiniti, allora sono numerabili (Proposizione 2.3), quindi $\mathbb{Q} = \mathbb{Q}_{\geq 0} \cup \mathbb{Q}_{<0}$ è numerabile (Proposizione 2.5). □

2.A. Insiemi e sequenze finite. Se X è non vuoto, indichiamo con

$$X^{<\mathbb{N}} = \{(x_0, \dots, x_{k-1}) \mid k \in \mathbb{N} \wedge \forall i < k\, (x_i \in X)\},$$

l'insieme delle stringhe finite di elementi di X, con la convenzione che se $k = 0$ si prende la sequenza vuota $\emptyset$. Se indichiamo con X^k l'insieme delle stringhe di X di lunghezza k si ha che

$$X^{<\mathbb{N}} = \bigcup_{k\in\mathbb{N}} X^n$$

C'è un'unica stringa di lunghezza 0, la stringa vuota, quindi $X^0 = \{\emptyset\}$. Le stringhe di lunghezza 1 sono in biezione con gli elementi di X, mediante la funzione $(x) \mapsto x$, quindi spesso X^1 viene identificato con X stesso. Le stringhe di lunghezza 2 sono le coppie ordinate di X, le stringhe di lunghezza 3 sono le triple ordinate di X, e così via.

Componendo una qualsiasi biezione $F\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, per esempio $\boldsymbol{J}$, con sé stessa possiamo definire delle biezioni

$$\begin{aligned}
&F^1\colon \mathbb{N} \to \mathbb{N}, \quad n \mapsto n,\\
&F^2\colon \mathbb{N}^2 \to \mathbb{N}, \quad (n,m) \mapsto F(n,m),\\
&F^3\colon \mathbb{N}^3 \to \mathbb{N}, \quad (n,m,k) \mapsto F(n,F(m,k)),\\
&F^4\colon \mathbb{N}^4 \to \mathbb{N}, \quad (n,m,k,j) \mapsto F(n,F^3(m,k,j)),\\
&\quad\vdots
\end{aligned}$$

Per ottenere una biezione tra $\mathbb{N}^{<\mathbb{N}}$ ed $\mathbb{N}$ è sufficiente dimostrare che $\mathbb{N}^{<\mathbb{N}} \precsim \mathbb{N}$ e $\mathbb{N} \precsim \mathbb{N}^{<\mathbb{N}}$ e utilizzare il Teorema 1.2. La mappa $\mathbb{N} \to \mathbb{N}^{<\mathbb{N}}$, $n \mapsto (n)$, è chiaramente iniettiva. Per ottenere una funzione iniettiva $G\colon \mathbb{N}^{<\mathbb{N}} \to \mathbb{N}$ procediamo così: se $s \in \mathbb{N}^{<\mathbb{N}}$ è di lunghezza n allora

$$G(s) = \begin{cases} F(0,0) & \text{se } n = 0,\\ F(n, F^n(s)) & \text{se } n > 0. \end{cases}$$

La funzione G è iniettiva: se $s \neq t$ allora si hanno due casi:

Caso 1: $n = \mathrm{lh}(s) \neq \mathrm{lh}(t) = m$. Allora $G(s) \neq G(t)$ dato che questi due numeri sono della forma $F(n,*)$ e $F(m,*)$.

Caso 2: $n = \mathrm{lh}(s) = \mathrm{lh}(t)$. Allora $F^(s) \neq F^n(t)$ da cui $G(s) \neq G(t)$.

Abbiamo quindi dimostrato

Teorema 2.8. $\mathbb{N}^{<\mathbb{N}}$ *è numerabile.*

Corollario 2.9. $\{0,1\}^{<\mathbb{N}}$ *è numerabile.*

DIMOSTRAZIONE. Poiché $\{0,1\}^{<\mathbb{N}} \subseteq \mathbb{N}^{<\mathbb{N}}$, allora $\{0,1\}^{<\mathbb{N}} \preceq \mathbb{N}$. D'altra parte la funzione $n \mapsto (\underbrace{0,\dots,0}_{n})$ testimonia che $\mathbb{N} \precsim \{0,1\}^{<\mathbb{N}}$, quindi il risultato segue dal Teorema 1.2. □

Un altro modo per enumerare $\mathbb{N}^{<\mathbb{N}}$ è il seguente.

Sia $(\boldsymbol{p}_n)_n$ l'enumerazione di tutti i numeri primi, cioè $\boldsymbol{p}_0 = 2$, $\boldsymbol{p}_1 = 3$, $\boldsymbol{p}_2 = 5$, ...

Data una stringa $s = (m_0, m_1, \dots, m_k) \in \mathbb{N}^{<\mathbb{N}}$ costruiamo il numero

$$f(s) = \begin{cases} \boldsymbol{p}_0^{m_0+1} \cdot \boldsymbol{p}_1^{m_1+1} \cdots \boldsymbol{p}_k^{m_k+1} & \text{se } s \neq \emptyset \\ 0 & \text{altrimenti.} \end{cases}$$

Il numero così ottenuto ha la seguente proprietà: se un primo p lo divide, anche tutti i primi più piccoli lo dividono. Quindi da $f(s)$ ricavo la lunghezza di s: basta guardare il massimo k tale che $\boldsymbol{p}_k$ divide $f(s)$.

Per la fattorizzazione unica, la funzione $f\colon \mathbb{N}^{<\mathbb{N}} \to \mathbb{N}$ è iniettiva.

2.B. Insieme potenza.

TEOREMA 2.10 (Cantor). *Non esiste alcuna suriezione da X su $\mathscr{P}(X)$ e quindi $\mathscr{P}(X) \not\preceq X$.*

DIMOSTRAZIONE. Sia $\pi\colon X \twoheadrightarrow \mathscr{P}(X)$ una suriezione e sia

$$Y = \{x \in X \mid x \notin \pi(x)\}.$$

Fissiamo un $\bar{x} \in X$ tale che $\pi(\bar{x}) = Y$. Allora $\bar{x} \in Y \leftrightarrow \bar{x} \notin \pi(\bar{x}) = Y$: contraddizione. □

In particolare $\mathscr{P}(\mathbb{N})$ non è in biezione con $\mathbb{N}$.

DEFINIZIONE 2.11. Se X e Y sono insiemi indicheremo con Y^X l'insieme $\{f \mid f\colon X \to Y\}$ di tutte le funzioni da X in Y.

L'insieme $\mathscr{P}(X)$ è in biezione con $\{0,1\}^X$, l'insieme delle funzioni da X in $\{0,1\}$: ad ogni $Z \subseteq X$ associamo la sua funzione caratteristica $\boldsymbol{\chi}_Z^X = \boldsymbol{\chi}_Z\colon X \to \{0,1\}$, definita da

$$\boldsymbol{\chi}_Z(x) = \begin{cases} 1 & \text{se } x \in Z \\ 0 & \text{altrimenti.} \end{cases}$$

ESERCIZIO 2.12. Dimostrare che:

(i) $X \precsim Y \to \mathscr{P}(X) \precsim \mathscr{P}(Y)$;
(ii) $X \precsim Y \wedge Z \precsim W \to X^Z \precsim Y^W$;
(iii) se $Y \cap Z = \emptyset$, allora $X^{(Y \cup Z)} \approx X^Y \times X^Z$;
(iv) $(X \times Y)^Z \approx X^Z \times Y^Z$;
(v) $(X^Y)^Z \approx X^{Y \times Z}$.

Se identifichiamo una funzione $f \in \mathbb{N}^{\mathbb{N}}$ con il suo grafo $\mathrm{Gr}(f) \in \mathscr{P}(\mathbb{N} \times \mathbb{N})$ allora $\{0,1\}^{\mathbb{N}} \subseteq \mathbb{N}^{\mathbb{N}} \precsim \mathscr{P}(\mathbb{N} \times \mathbb{N})$, e per il Teorema 2.4 $\mathscr{P}(\mathbb{N} \times \mathbb{N}) \approx \mathscr{P}(\mathbb{N}) \approx \{0,1\}^{\mathbb{N}}$, da cui

$$\{0,1\}^{\mathbb{N}} \approx \mathbb{N}^{\mathbb{N}}.$$

TEOREMA 2.13. $\mathbb{R}$ *è in biezione con* $\mathscr{P}(\mathbb{N})$, *quindi non è numerabile.*

APPENDICE A

Lettere Greche

Le lettere greche sono usate costantemente in matematica. Per chi non le conosce le elenchiamo qui sotto, minuscole e maiuscole, con il loro nome in italiano.

minuscola	maiuscola	nome in italiano
α	A	alfa
β	B	beta
γ	Γ	gamma
δ	Δ	delta
ϵ	E	epsilon
ζ	Z	zeta
η	H	eta
θ	Θ	theta
ι	I	iota
κ	K	kappa
λ	Λ	lambda
μ	M	mi
ν	N	ni
ξ	Ξ	xi
o	O	omicron
π	Π	pi
ρ	P	rho
σ	Σ	sigma
τ	T	tau
υ	Υ	upsilon
ϕ	Φ	phi
χ	X	chi
ψ	Ψ	psi
ω	Ω	omega

Alcune lettere minuscole ammettono una forma leggermente differente.

forma solita	variante
ϵ	ε
θ	ϑ
π	ϖ
κ	$\varkappa$
ρ	ϱ
σ	ς
ϕ	φ