LOGICA MATEMATICA

Sonia L'Innocente

Corso di Laurea

L31, Informatica e Tecnologie

Capitoli 1-2-3-4

a.a. 2016-2017

Outline

Introduzione

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

$$\text{l'equazione } x^2 = 2 \text{ non ha soluzioni razionali.} \tag{1}$$

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

$$\text{per ogni vettore } v\text{, l'algoritmo } a \text{ produce una permutazione degli elementi di } v \text{ ordinata in ordine crescente.} \tag{2}$$

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.

Commenti

(1) 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 $n^2 = 2m^2$.

(2) 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.

Dimostrazione

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**.

Derivazioni

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.

Linguaggio formale

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**.

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.

Le costanti logiche: i connettivi

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

$$\neg \qquad \vee \qquad \wedge \qquad \rightarrow \qquad \leftrightarrow$$

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.

Le costanti logiche: i connettivi

$\vee$ 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.

Le costanti logiche: i connettivi

$\rightarrow$ 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

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

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.

Osservazione su $\rightarrow$

Un'implicazione non sottintende nessuna relazione di causalità tra la premessa e la conseguenza — l'unico significato di $\mathrm{A} \rightarrow \mathrm{B}$ 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 $\mathrm{A} \rightarrow \mathrm{B}$, mentre "affinché valga A è sufficiente che valga B" significa che A vale quando B vale, cioè $\mathrm{B} \rightarrow \mathrm{A}$.

Le costanti logiche: i connettivi

$\leftrightarrow$ 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".

Le costanti logiche: i quantificatori

$\exists$ è il **quantificatore esistenziale**. L'espressione $\exists x \mathrm{A}$ 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 $\forall x \mathrm{A}$ si legge: "per ogni x vale A", ovvero "A vale, per tutti gli x" e asserisce che *ogni* ente gode della proprietà A.

Le 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

$$\frac{\mathrm{A}_1 \qquad \mathrm{A}_2 \qquad \ldots \qquad \mathrm{A}_n}{\mathrm{B}}$$

dove $\mathrm{A}_1, \ldots, \mathrm{A}_n$ e B sono proposizioni che esprimono il fatto che la conclusione B può essere inferita dalle premesse $\mathrm{A}_1, \ldots, \mathrm{A}_n$.

Tavole di verità

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**

Tavole di verità

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

A	$\neg\mathrm{A}$	$\neg\neg\mathrm{A}$
V	**F**	**V**
F	**V**	**F**

(3)

Quindi da A possiamo ricavare $\neg\neg\mathrm{A}$ e viceversa:

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

Tavole di verità di $\wedge$

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 $\mathrm{A} \wedge \mathrm{B}$ è sufficiente dimostrare A e dimostrare B. Possiamo esprimere graficamente questo così

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

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

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

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

Tavole di verità di $\wedge$

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 $\mathrm{A} \vee \mathrm{B}$ è la stessa di $\mathrm{B} \vee \mathrm{A}$. Quindi asserire $\mathrm{A} \vee \mathrm{B}$ è come asserire $\mathrm{B} \vee \mathrm{A}$. Dimostrato A, possiamo indebolire il nostro risultato asserendo $\mathrm{A} \vee \mathrm{B}$, dove B è un'affermazione qualsiasi. Analogamente, da B si deduce $\mathrm{A} \vee \mathrm{B}$, per qualsiasi A. In simboli

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

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

$$\frac{A \vee B \qquad \neg A}{B} \quad \text{e} \quad \frac{A \vee B \qquad \neg B}{A}. \tag{4}$$

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**.

Tavole di verità di $\rightarrow$

La tavola di verità per l'implicazione è:

A	B	A $\rightarrow$ 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

$$\frac{A \rightarrow B}{\neg A \vee B} \quad \text{e} \quad \frac{\neg A \vee B}{A \rightarrow B}.$$

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

$$\frac{\mathrm{A} \to \mathrm{B} \qquad \mathrm{A}}{\mathrm{B}} \ . \tag{MP}$$

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

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

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

Tavole di verità di $\leftrightarrow$

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

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

e

$$\frac{A \rightarrow B \qquad B \rightarrow A}{A \leftrightarrow B}\ .$$

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

$$\mathrm{A} \oplus \mathrm{B}$$

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

A	B	$\mathrm{A} \oplus \mathrm{B}$
V	**V**	**F**
V	**F**	**V**
F	**V**	**V**
F	**F**	**F**

I valori 0 e 1.

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

Tautologie e conseguenze logiche

Ora che abbiamo visto le tavole logiche dei connettivi analizziamo 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 $\mathrm{A}, \mathrm{B}, \mathrm{C}, \ldots$ 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 $(\mathrm{B} \to \mathrm{A}) \wedge ((\mathrm{B} \vee \mathrm{C}) \leftrightarrow \mathrm{A})$ è ottenuta a partire dalle tavole di verità di $\mathrm{B} \to \mathrm{A}$, di $\mathrm{B} \vee \mathrm{C}$, e di $(\mathrm{B} \vee \mathrm{C}) \leftrightarrow \mathrm{A}$:

A	B	C	$\mathrm{B} \to \mathrm{A}$	$\mathrm{B} \vee \mathrm{C}$	$(\mathrm{B} \vee \mathrm{C}) \leftrightarrow \mathrm{A}$	$(\mathrm{B} \to \mathrm{A}) \wedge ((\mathrm{B} \vee \mathrm{C}) \leftrightarrow \mathrm{A})$
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

Example

La tavola di verità di $(\mathrm{A} \wedge \neg \mathrm{A}) \rightarrow \mathrm{B}$ è

A	B	$\neg$A	A $\wedge \neg$A	$(\mathrm{A} \wedge \neg \mathrm{A}) \rightarrow \mathrm{B}$
0	0	1	0	1
0	1	1	0	1
1	0	0	0	1
1	1	0	0	1

Example

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

Example

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.

Example

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?

Example

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

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

sono proposizioni vere. Dalla prima vediamo che A e C sono false. Supponiamo D sia vera: allora $\mathrm{D} \vee \mathrm{E}$ sarebbe vera e $\mathrm{C} \leftrightarrow \mathrm{D}$ falsa e quindi $(\mathrm{D} \vee \mathrm{E}) \to (\mathrm{C} \leftrightarrow \mathrm{D})$ è falsa. D'altra parte $\mathrm{D} \to \mathrm{A}$ è falsa, quindi $(\mathrm{D} \to \mathrm{A}) \vee ((\mathrm{D} \vee \mathrm{E}) \to (\mathrm{C} \leftrightarrow \mathrm{D}))$ 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.

Definition

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.

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 $\neg\mathrm{A}$ è una contraddizione proposizionale.

Definition

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

Examples

$\neg\mathrm{A} \vee \mathrm{A}$ è una tautologia, $\neg\mathrm{A} \wedge \mathrm{A}$ è una contraddizione, mentre $\mathrm{A} \to \mathrm{B}$ è soddisfacibile.

Definition

Una proposizione B è **conseguenza tautologica** o, più semplicemente, **conseguenza logica** di proposizioni $\mathrm{A}_1, \ldots, \mathrm{A}_n$ se la proposizione

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

è una tautologia.

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

$$\frac{\mathrm{A}_1 \qquad \mathrm{A}_2 \qquad \dots \qquad \mathrm{A}_n}{\mathrm{B}}$$

è **logicamente corretta** se e solo se B è una conseguenza logica di $\mathrm{A}_1, \dots, \mathrm{A}_n$. Per quanto detto prima, questo equivale a dire che la proposizione

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

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

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

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

Leggi logiche

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 $\mathrm{A} \to \mathrm{A}$

legge della doppia negazione $\mathrm{A} \leftrightarrow \neg\neg\mathrm{A}$

commutatività di $\wedge$ $\mathrm{A} \wedge \mathrm{B} \leftrightarrow \mathrm{B} \wedge \mathrm{A}$

associatività di $\wedge$ $(\mathrm{A} \wedge \mathrm{B}) \wedge \mathrm{C} \leftrightarrow \mathrm{A} \wedge (\mathrm{B} \wedge \mathrm{C})$

commutatività di $\vee$ $\mathrm{A} \vee \mathrm{B} \leftrightarrow \mathrm{B} \vee \mathrm{A}$

associatività di $\vee$ $(\mathrm{A} \vee \mathrm{B}) \vee \mathrm{C} \leftrightarrow \mathrm{A} \vee (\mathrm{B} \vee \mathrm{C})$

idempotenza di $\wedge$ $\mathrm{A} \wedge \mathrm{A} \leftrightarrow \mathrm{A}$

idempotenza di $\vee$ $\mathrm{A} \vee \mathrm{A} \leftrightarrow \mathrm{A}$

eliminazione di $\wedge$ $\mathrm{A} \wedge \mathrm{B} \to \mathrm{A}$

introduzione di $\vee$ $\mathrm{A} \to \mathrm{A} \vee \mathrm{B}$

Leggi logiche

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

legge del terzo escluso $\neg A \vee A$

legge di non contraddizione $\neg(A \wedge \neg A)$

legge di contrapposizione $A \rightarrow B \leftrightarrow \neg B \rightarrow \neg A$

legge di Lewis, o *ex falso quodlibet* $A \wedge \neg A \rightarrow B$

affermazione del conseguente $A \rightarrow (B \rightarrow A)$

negazione dell'antecedente $\neg A \rightarrow (A \rightarrow B)$

Leggi logiche

legge di riduzione all'assurdo $(\mathrm{A} \to \mathrm{B} \wedge \neg \mathrm{B}) \to \neg \mathrm{A}$

riduzione all'assurdo debole $(\mathrm{A} \to \neg \mathrm{A}) \to \neg \mathrm{A}$

consequentia mirabilis $(\neg \mathrm{A} \to \mathrm{A}) \to \mathrm{A}$

legge di Peirce $((\mathrm{A} \to \mathrm{B}) \to \mathrm{A}) \to \mathrm{A}$

legge di Dummett $(A \to B) \vee (B \to A)$

modus ponens $\mathrm{A} \to ((\mathrm{A} \to \mathrm{B}) \to \mathrm{B})$

scambio antecedenti $\mathrm{A} \to (\mathrm{B} \to \mathrm{C}) \leftrightarrow \mathrm{B} \to (\mathrm{A} \to \mathrm{C})$

distinzione di casi $(\mathrm{A} \to \mathrm{C}) \wedge (\mathrm{B} \to \mathrm{C}) \leftrightarrow \mathrm{A} \vee \mathrm{B} \to \mathrm{C}$

distinzione di casi $(\mathrm{A} \to \mathrm{B}) \wedge (\neg \mathrm{A} \to \mathrm{B}) \to \mathrm{B}$

distributività di $\to$ $(\mathrm{A} \to (\mathrm{B} \to \mathrm{C})) \to ((\mathrm{A} \to \mathrm{B}) \to (\mathrm{A} \to \mathrm{C}))$

transitività di $\to$ $(\mathrm{A} \to \mathrm{B}) \wedge (\mathrm{B} \to \mathrm{C}) \to (\mathrm{A} \to \mathrm{C})$

importazione delle premesse $\mathrm{A} \to (\mathrm{B} \to \mathrm{C}) \leftrightarrow (\mathrm{A} \wedge \mathrm{B}) \to \mathrm{C}$

Osservazioni

1. 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.

2. 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).

3. 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.

Osservazioni

4. Anche le seguenti sono leggi logiche:

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

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.

Esercizi

1. Costruire la tavola di verità delle proposizioni:

   $(A \to A) \to A$

   $A \to (A \to A)$

   $A \vee B \to A \wedge B$

   $A \vee B \wedge C \to A \wedge C \vee D$

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

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

Esercizi

2. 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.

3. 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?

4. $(\mathrm{A} \to \mathrm{B}) \to (\mathrm{B} \to \mathrm{A})$ 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.

I 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 .

I quantificatori

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

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

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

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

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

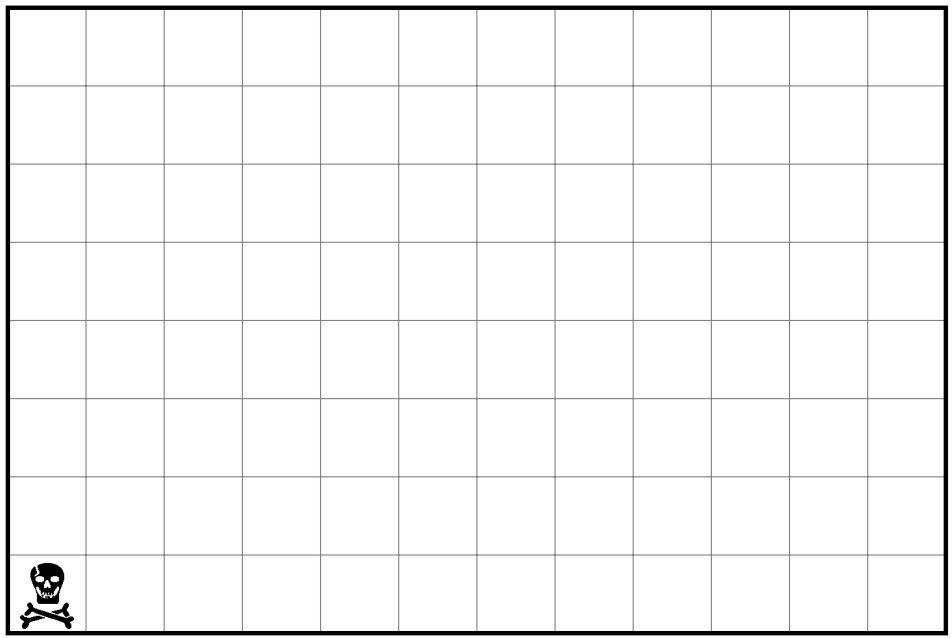
$$\frac{(\forall x \mathrm{A}) \vee (\forall x \mathrm{B})}{\forall x\,(\mathrm{A} \vee \mathrm{B})}\,.$$

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 $P(0) \wedge P(1) \wedge P(2) \wedge \ldots$

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.

ESEMPIO.

Consideriamo il seguente gioco. Fissiamo una tavoletta di cioccolata rettangolare

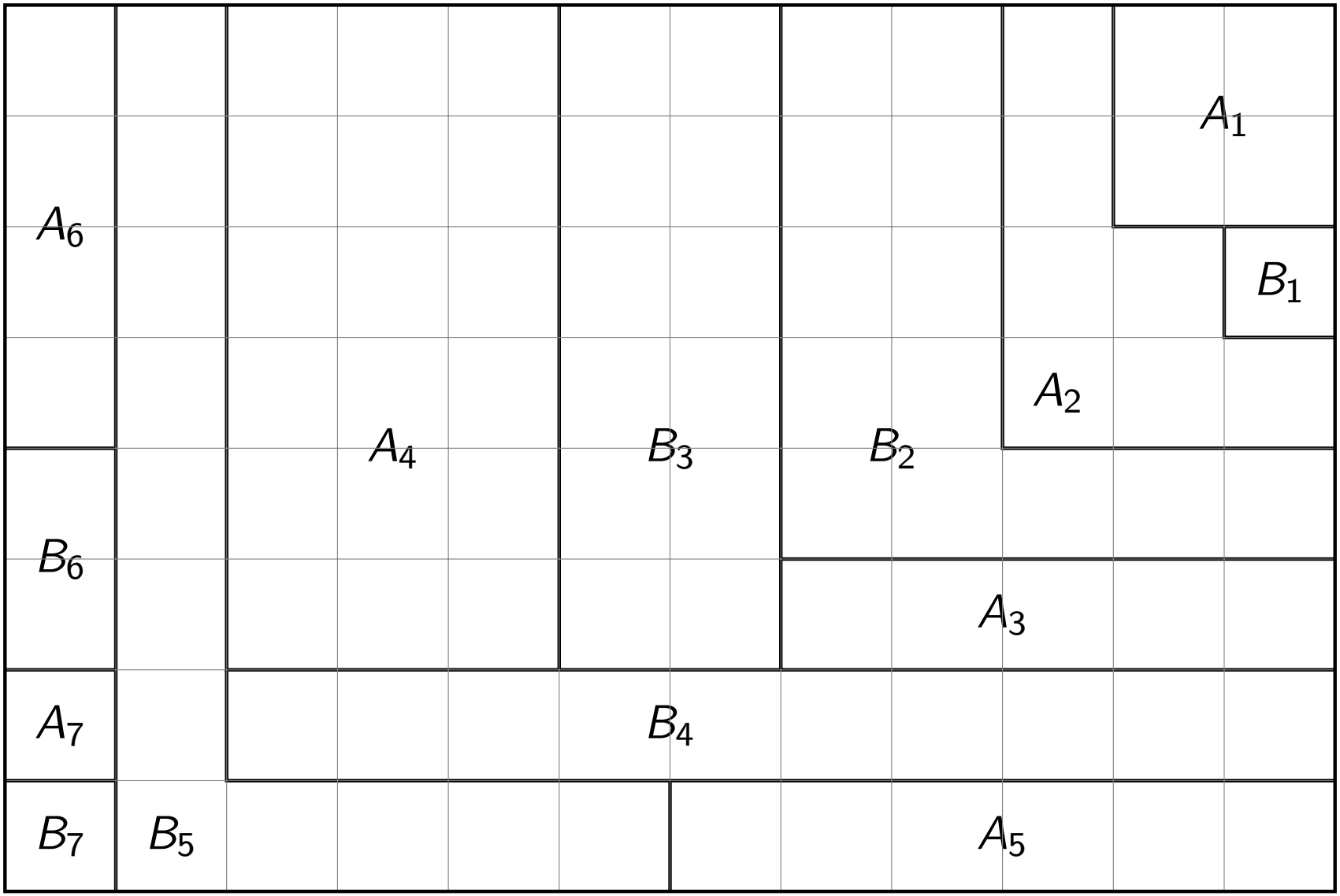


Due giocatori, che convenzionalmente chiameremo Alice e Bob, a turno prendono dei pezzi della tavoletta seguendo la seguente regola

> *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.



Tecniche di dimostrazione.

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

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:

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

Dimostrazione diretta.

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.

Dimostrazione diretta.

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.

Osservazione. 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.

Dimostrazione diretta: esempio.

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

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

Per la dimostrazione: siano n ed m interi qualsiasi, ed assumiamo $\mathrm{A} \wedge \mathrm{B}$, 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 $2j + 1$ ($j = l + k$).

Dimostrazione diretta: esercizi.

1. Si dia una dimostrazione diretta del fatto che, se n è pari, allora n^2 è divisibile per 4.

2. Siano a e b due numeri reali. Si definisce il *minimo* $\min(a, b)$ tra a e b nel modo seguente:

$$\min(a, b) = \begin{cases} a & \text{if } a \leq b; \\ b & \text{if } a > b. \end{cases}$$

Si dia una dimostrazione diretta dell'enunciato:

Se $x \leq \min(a, b)$, *allora* $x \leq a$ *e* $x \leq b$.

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 $\mathrm{C} \wedge \neg \mathrm{C}$ (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**.

Dimostrazione per assurdo: esempio.

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

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

Dimostrazione.

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

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

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 $y \geq 1$. □

Dimostrazione per assurdo: esempio.

Dimostriamo ora l'enunciato:

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

cioè in formule

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

Dimostrazione.

Dimostriamo che $\mathrm{A} \to \mathrm{B}$ 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 $\neg\mathrm{B}$, 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 $\neg\mathrm{A}$ 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:

$\left|\begin{array}{l} \mathrm{A}\text{: } n^2 \text{ pari (assunzione della dimostrazione diretta)} \\ \left|\begin{array}{l} \neg\mathrm{B}\text{: } n \text{ dispari (assunzione della dimostrazione per assurdo)} \\ \vdots \\ \neg\mathrm{A}\text{: } n^2 \text{ dispari} \\ \mathrm{A} \text{ (per ipotesi della dimostrazione diretta)} \end{array}\right. \\ \mathrm{B} \text{ (conclusione della dimostrazione per assurdo)} \end{array}\right.$

$\mathrm{A} \to \mathrm{B}$ (conclusione della dimostrazione diretta)

Dimostrazione per contrapposizione.

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

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

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

Per esempio, si dimostra per contrapposizione l'enunciato:

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

dimostrando (in modo diretto) l'enunciato:

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

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

$$n^2 = (2k + 1)^2$$

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

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

Dimostrazione per casi: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

$$(\mathrm{A_1} \to \mathrm{B}) \wedge (\mathrm{A_2} \to \mathrm{B}).$$

Dimostrazione.

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:

Theorem

$\sqrt{2} \notin \mathbb{Q}$

Dimostrazione.

Per assurdo (dimostrazione indiretta). Supponiamo che esistano $n, m \in \mathbb{N} \setminus \{0\}$ tali che

$$\left(\frac{m}{n}\right)^2 = 2$$

e cerchiamo di ottenere una contraddizione. Se n e m hanno d come massimo comuni divisore, cioè $n = n_1 d$ e $m = m_1 d$, allora $\frac{m}{n} = \frac{m_1}{n_1}$, quindi

possiamo supporre che n e m siano relativamente primi.

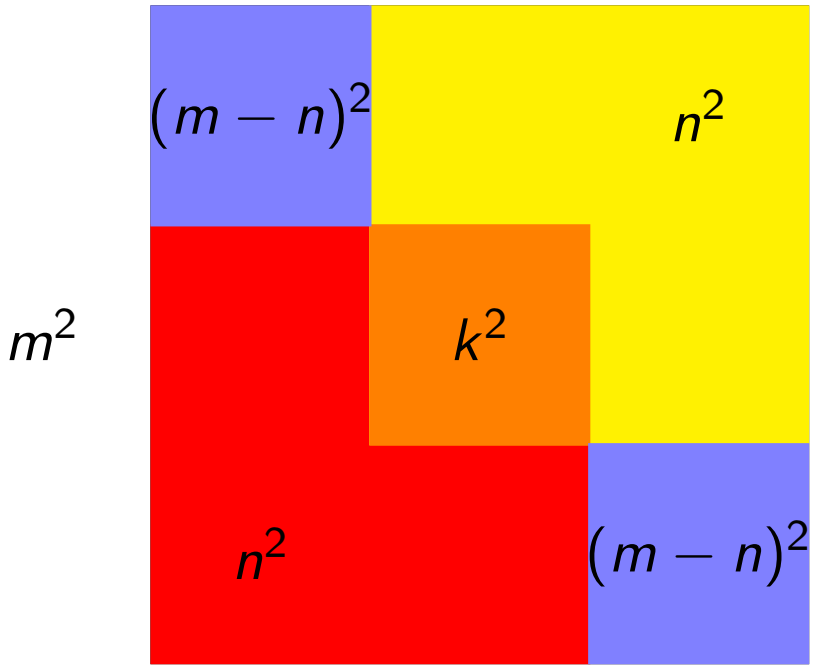
Poiché $m^2 = 2n^2$, allora m^2 è pari, quindi m è pari, cioè $m = 2k$. Quindi

$$4k^2 = m^2 = 2n^2$$

da cui $2k^2 = n^2$, cioè n è pari. Ma allora n e m non sono relativamente primi: contraddizione! □

Dimostrazione.

Come prima, ragioniamo per assurdo.
Supponiamo che esistano $n, m \in \mathbb{N} \setminus \{0\}$ tali che $2n^2 = m^2$ e supponiamo m sia il minimo numero siffatto.



$m^2 = n^2 + n^2 + 2(n-m)^2 - k^2$, cioè $0 = 2(n-m)^2 - k^2$, cioè $k^2 = 2(n-m)^2$. Ma $k < m$: contraddizione! □

Insiemi.

In matematica è uso comune considerare delle collezioni di oggetti e queste collezioni si dicono **insiemi**.
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.

Insiemi.

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.

Insiemi.

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

doppiainclusione 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 $A \subset B$.

Insiemi.

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.

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

Insiemi: 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.

Operazioni tra insiemi.

Operazioni tra 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.

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).

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.

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.

Insieme delle parti.

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.

Famiglie di 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 $\complement A = \{x \mid x \notin A\}$

Propositione. 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).

Dimostrazione

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

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

Dimostrazione.

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.

Prodotto cartesiano.

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.

Prodotto cartesiano.

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.

Relazione.

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:

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

Definition

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.

Relazione di equivalenza

Definition

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 $I(A) \subseteq E \subseteq A \times A$.

Classe di equivalenza e Insieme quoziente

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

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. □

Definition

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

se $X \in \mathcal{C}$ allora $\emptyset \neq X \subseteq A$,

se $X, Y \in \mathcal{C}$ e $X \neq Y$ allora $X \cap Y = \emptyset$,

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.

Relazione d'ordine

Definition

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

Definition

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.

Definition

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.

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 $[a] = [b]$. □

Definition

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 $b \in A$.

Examples

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

Definition

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

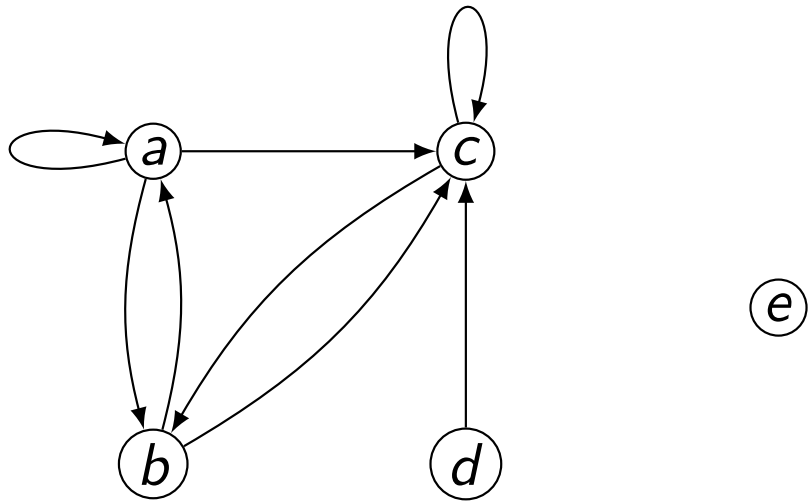
$$R \cup I(A)$$

è un ordine su A.

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

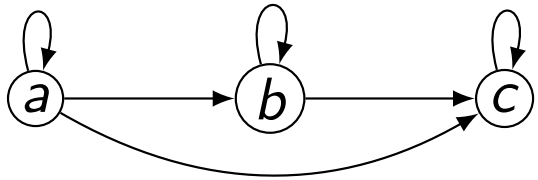
$$R = \{(a,a),(a,b),(a,c),(b,a),(b,c),(c,c),(d,c)\}$$

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



dove la freccia $x \longrightarrow y$ significa che $(x,y) \in R$.

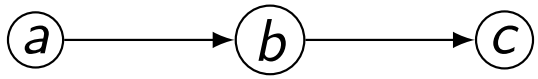
Quindi un ordine lineare con tre elementi $a \leq b \leq c$ è rappresentato da



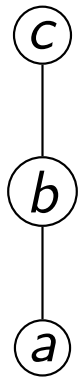
L'informazione contenuta in questo disegno è ridondante — dato che un ordine è una relazione è riflessiva e transitiva, è sufficiente considerare il diagramma della relazione di **successore immediato**

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

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**.

Funzioni.

Definition

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

per ogni $a \in A$ c'è un $b \in B$ tale che $(a, b) \in F$.

ogni qual volta $(a, b_1) \in F$ e $(a, b_2) \in F$ succede che $b_1 = b_2$.

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

Funzioni.

Definition

Una funzione $F: A \longrightarrow B$ 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.

Definition

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

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

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: **1.** Per ogni $n \in \mathbb{N}$,

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

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

$$Q(n) \leftrightarrow P \textit{ è vera dopo } n \textit{ iterazioni del ciclo while.}$$

Proprietà di questo tipo sono utilizzate per stabilire che P è una proprietà invariante del ciclo in questione.

3. 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 $E(n)$.

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* $\forall x \in \mathbb{N}\,(x \geq k \to P(x))$.

Vediamo subito il primo esempio di utilizzo del principio di induzione:

Example

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

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

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

Dimostrazione.

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. □

Example

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

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

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

Dimostrazione.

e dimostriamo che

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

Ora,

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

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

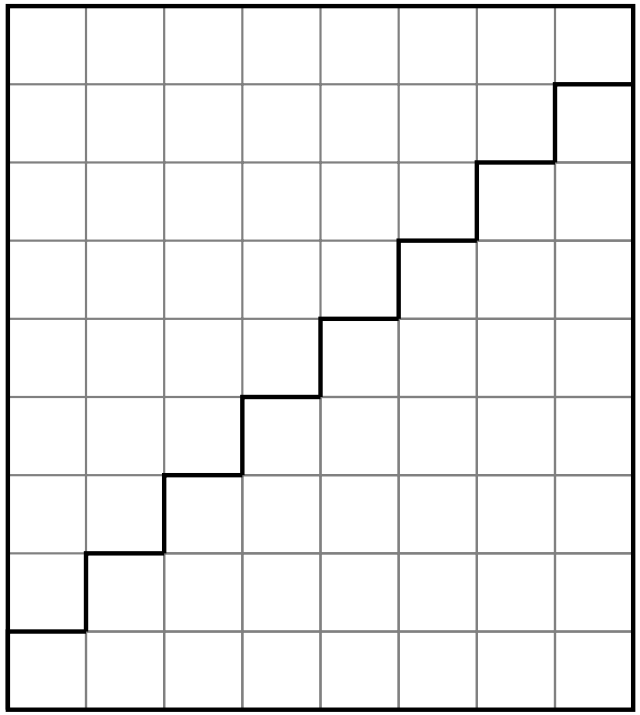
$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2} \tag{9}$$

e

$$\sum_{i=0}^{n} (2i+1) = (n+1)^2 \tag{10}$$

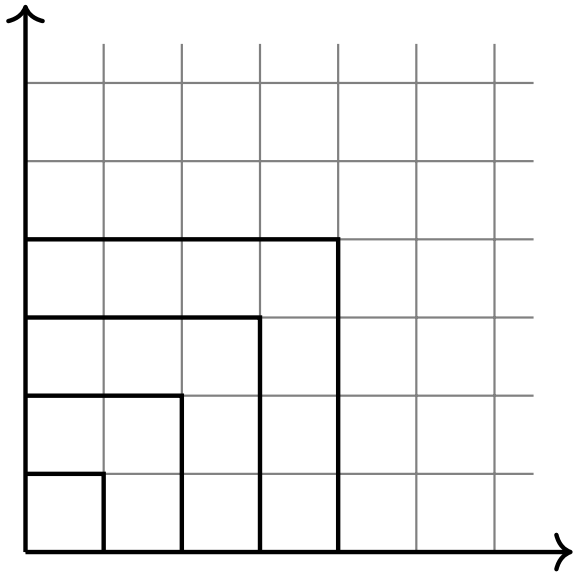
si possono dimostrare mediante argomenti geometrici.

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 9.

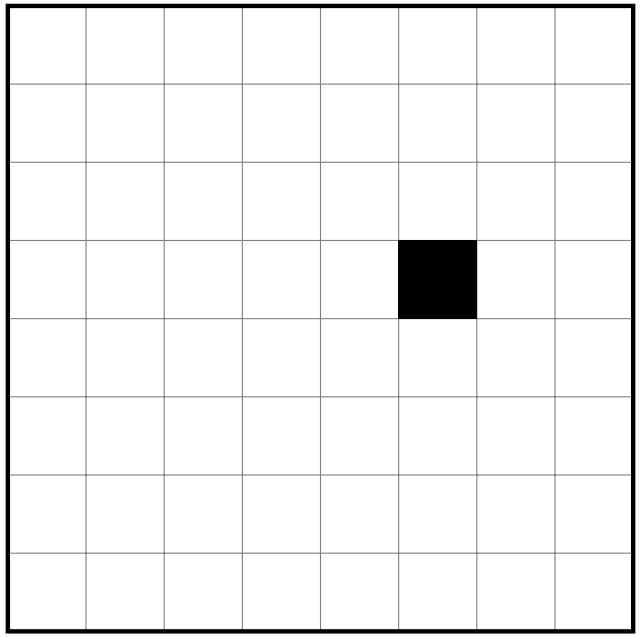
La figura



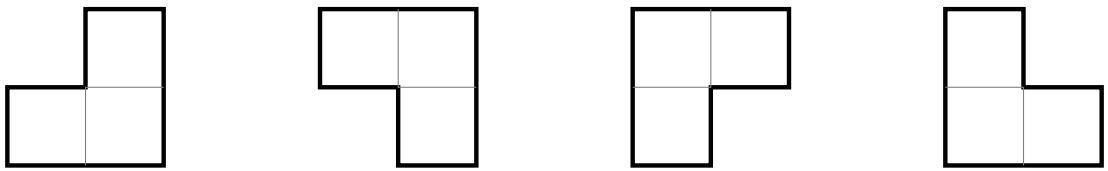
mostra come l'area del quadrato di lato n sia ottenibile sommando l'area delle "cornici" $1 + 3 + 5 + \cdots + (2n - 1)$, da cui la formula 10.

Esempio.

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

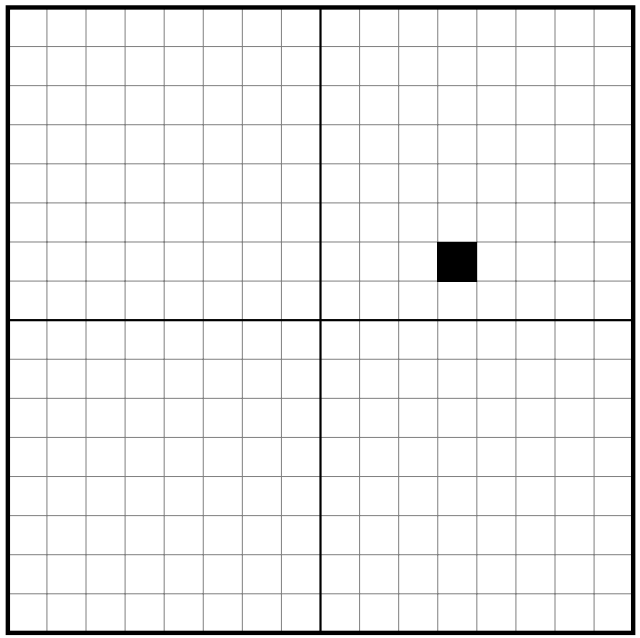


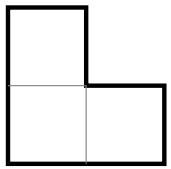
Dimostrazione.

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.

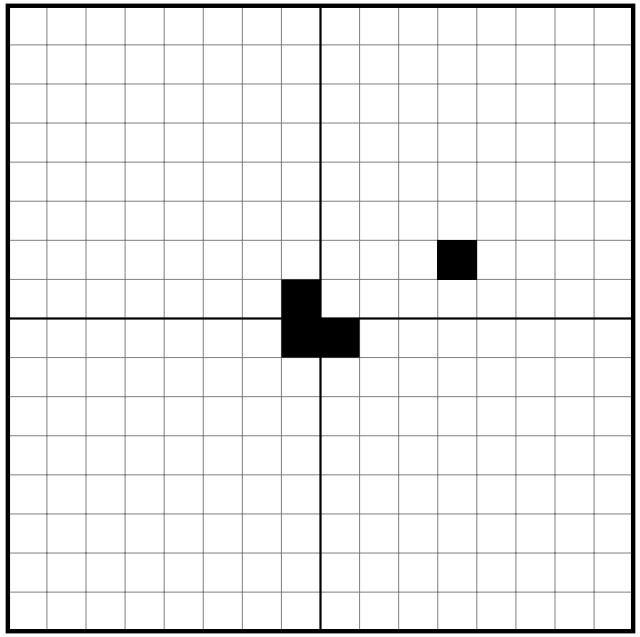
Dimostrazione.

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:

Dimostrazione.



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

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:

$$X = q * D + r \tag{11}$$

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 (11) 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 (11) 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 (11) 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 (11) è vera per qualsiasi numero di iterazioni del ciclo, quindi (11) è invariante.

Esempio: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

$$Y = X * X. \tag{12}$$

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 (12) è invariante.

Un programma Java che realizza questo algoritmo è il seguente:

```
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;
}
```

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

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

bisogna dimostrare che (12) 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 (12) 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.

Definizioni ricorsive di funzioni.

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

$$f(0) = a$$
$$f(n+1) = E(f(n))$$

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.)

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

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

$$q(0) = 0$$
$$q(n+1) = q(n) + 2 * n + 1$$

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 calcolarla per un valore arbitrario dell'argomento. Per esempio:

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

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.

Non esiste alcuna successione discendente infinita di numeri naturali

$$n_0 > n_1 > n_2 > \dots \tag{13}$$

Dimostrazione.

Per assurdo, se esistesse una successione come in (13), l'insieme $\{n_0, n_1, n_2, \dots\}$ non avrebbe un minimo elemento. □

Vediamo un'applicazione del principio del minimo: Proposizione.

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:

> n è primo: allora n ha una scomposizione in fattori primi, assurdo.
>
> 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. □

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

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

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.

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:

- se $i = n$: allora il secondo giocatore rimuove tutta la pila rimanente, e quindi l'ultima carta, vincendo.
- 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.

Theorem

Le seguenti affermazioni sono equivalenti:

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

Dimostrazione.

(PI)$\rightarrow$(PIF): Assumiamo che $\mathrm{Prog}(P)$. 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 $\mathrm{Prog}(P)$ 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 $\mathrm{Prog}(P)$. 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 $\mathrm{Prog}(P)$, $P(n)$ 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.

Dimostrazione.

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

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

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

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

(PIF)
| $P(0) \wedge \forall x\,(P(x) \rightarrow P(x+1))$ (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.

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. □

Esercizi.

1. Dimostrare che

$$\forall n > 0 \left[\sum_{i=1}^{n}(3i-2) = \frac{n(3n-1)}{2}\right].$$

2. Dimostrare che

$$\forall n \left[\sum_{i=1}^{n} i(i+1) = \frac{n(n+1)(n+2)}{3}\right].$$

3. Dimostrare che

$$\forall n \left[\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}\right].$$

4. Dimostrare che $\forall n > 0$ $\left(n^3 - n \text{ è divisibile per } 3\right)$.

5. Dimostrare che $\forall n$ $(n(n+1)$ è divisibile per $2)$.

6. Dimostrare che $\forall n\ (n(n+1)(n+2)$ è divisibile per $3)$.

7. Dimostrare che $\forall n \geq 1\ ((k+1)^n - 1$ è divisibile per $k)$, dove $k \geq 2$.

8. Dimostrare che $\forall n \geq 1\ \left(n! \geq 2^{n-1}\right)$.

9. Dimostrare che $\forall n \geq 4\ (n! > 2^n)$.

10. Dimostrare che $\forall n \geq 3\ \left(n^2 > 2n+1\right)$.

11. Dimostrare che $\forall n \geq 5\ \left(2^n > n^2\right)$.

12. Dimostrare che, per $\forall n \geq 3\ \left(n^2 > 2n+1\right)$.