Quanto è grande l'infinito?

Indice

Abbiamo visto che tutti i linguaggi noti per la descrizione e soluzione di problemi sono *computazionalmente equivalenti* al linguaggio delle Macchine di Turing, ossia che sono in grado di descrivere (o calcolare) tutto e solo ciò che può essere descritto (o calcolato) da una macchina di Turing. Abbiamo anche visto come Church e Turing hanno generalizzato tale questione, enunciando la tesi che porta il loro nome: se un problema può essere ridotto in una serie finita di passi elementari, allora esisterà una macchina di Turing in grado di risolverlo. O, in altri termini,

è calcolabile tutto (e solo) ciò che può essere calcolato da una macchina di Turing.

A questo punto, però, è naturale chiedersi: ma cosa è che può essere calcolato da una macchina di Turing? O meglio, alla luce della tesi di Church-Turing: cosa è che può essere calcolato? O, ancor più precisamente: esiste qualcosa che *non* può essere calcolato?

Esiste un problema che non può essere risolto?

Per poter rispondere a tale domanda dovremo acquisire strumenti la cui conoscenza ci richiede una piccola (ma significativa) deviazione dal percorso della calcolabilità in senso stretto.

4.1 Insiemi, relazioni, cardinalità

Intuitivamente, possiamo dire che un insieme è un aggregato di oggetti che verificano tutti una certa proprietà, la *proprietà caratteristica* o *legge di appartenenza*. In realtà, comunque, *il concetto di insieme è un concetto primitivo*, introdotto e studiato da un nutrito gruppo di eminenti logici matematici che operarono fre la seconda metà del XIX secolo e la prima metà del XX secolo[1]: dire che un insieme è un aggregato di oggetti non è darne una definizione, è soltanto utilizzare un sinonimo per il termine"insieme" .

Fra due insiemi A e B è possibile definire le seguenti operazioni:

- l'operazione di *unione*: $A \cup B$ è l'insieme di tutti e soli gli elementi che sono in A oppure in B;
- l'operazione di *intersezione*: $A \cap B$ è l'insieme di tutti e soli gli elementi che sono sia in A che in B;
- l'operazione *differenza*: $A - B$ è l'insieme di tutti e soli gli elementi che sono in A ma non in B.

L'*insieme vuoto* è l'insieme che non contiene alcun elemento.

In questo paragrafo ci riferiamo soltanto ad insiemi *finiti*. Un insieme A si dice finito quando il seguente procedimento ha termine: fino a quando A non è l'insieme vuoto, sottrai un elemento da A.

Una *corrispondenza* fra due insiemi (finiti) è una associazione fra gli elementi dei due insiemi.
Ad esempio, se A è l'insieme degli studenti iscritti ad una certa scuola e D è l'insieme dei docenti che insegnano in quella scuola, una corrispondenza fra A e B è quella che associa un elemento $a \in A$ ad un elemento $d \in D$ se (e soltanto se) d è uno degli insegnanti di a. In questo esempio, ad ogni elemento di A corrispondono numerosi elementi di B e, viceversa, ad ogni elemento di B corrispondono, in generale, numerosi elementi di A.
Se, invece consideriamo l'insieme R degli insegnanti di religione di quella scuola e la corrispondenza che associa un elemento $a \in A$ ad un elemento $r \in R$ se (e soltanto se) r è l'insegnante di religione di a, allora potrebbe esistere qualche elemento di A che non corrrisponde ad alcun elemento di R (gli studenti esonerati).

Una corrispondenza fra due insiemi si dice *biunivoca* se

- ogni elemento del primo insieme è in corrispondenza con uno ed un solo elemento del secondo insieme (in Figura 4.1.(i) è mostrato un esempio in cui questo non avviene) e
- ogni elemento del secondo insieme è in corrispondenza con uno ed un solo elemento del primo insieme (in Figura 4.1.(ii) è mostrato un esempio in cui questo non avviene).

Un esempio di corrispondenza biunivoca è illustrato in Figura 4.1.(iii).

Osserviamo che, dati due insiemi finiti qualunque, non è sempre possibile stabilire fra di essi una corrispondenza biunivoca.

[1] Fra tali logici ricordiamo Gottlob Frege (1848-1925), Bertrand Russell (1878-1932), Ernst Zermelo (1871-1953), nonché il protagonista di questa dispensa, Georg Cantor (1845-1918). Per una brevissima introduzione alla teoria degli insiemi, si veda l'Appendice B di questa dispensa.

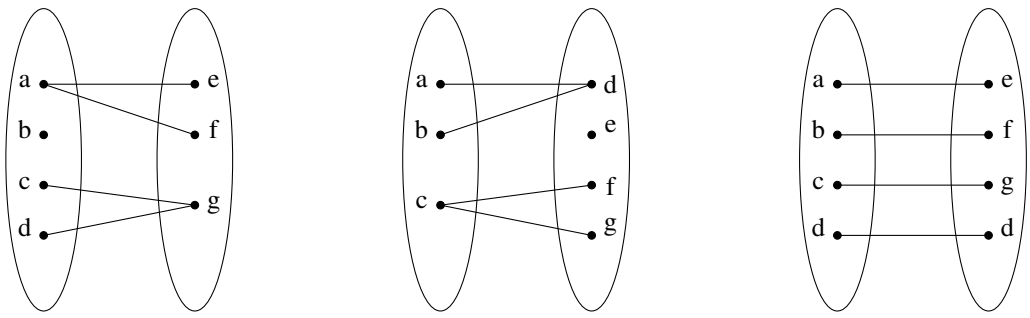

Figura 4.1: Le corrispondenze in (i) e (ii) sono esempi di corrispondenze non biunivoche. La corrispondenza in (iii) è biunivoca.

Definizione 4.1: Due insiemi A e B fra i quali può essere definita una corrispondenza biunivoca si dicono *equipotenti*, o, equivalentemente, che hanno la stessa *cardinalità*, e si scrive

$$|A| = |B|.$$

Intuitivamente, se due insiemi finiti hanno la stessa cardinalità allora contengono lo stesso numero di elementi.

È immediato verificare che la relazione di equipotenza è una relazione di equivalenza: infatti, qualunque insieme è equipotente a sé stesso (proprietà riflessiva), se A è equipotente a B allora B è equipotente ad A (proprietà simmetrica - è sufficiente, in questo caso, invertire la corrispondenza biunivoca che associa gli elementi di A agli elementi di B), e, infine, se A è equipotente a B e B è equipotente a C allora A è equipotente a C (proprietà transitiva - è sufficiente osservare che la composizione di corrispondenze biunivoche è anch'essa una corrispondenza biunivoca). Allora, possiamo partizionare l'insieme di tutti gli insiemi finiti[2] in classi di equivalenza rispetto alla relazione di equipotenza.

Vediamo ora, a titolo di esempio, come, a partire dal concetto di insieme è possibile definire formalmente i numeri naturali (si rimanda all'Appendice A per una breve introduzione alla definizione assiomatica dei numeri naturali di Peano).

Definizione 4.2: Un numero naturale è una classe di equivalenza rispetto alla relazione di equipotenza contenente insiemi finiti. In particolare,

- 0 è la classe di equivalenza cui appartiene l'insieme vuoto $\emptyset$, ossia, $0 = [\emptyset]$;
- 1 è la classe di equivalenza cui appartiene l'insieme $\{a\}$, ossia, $1 = [\{a\}] = [\emptyset \cup \{a\}]$;
- in generale, il numero naturale $n+1$ è definito come $[X \cup \{a\}]$, dove $X \in n$.

In sostanza, si parte dalla proprietà (intuitiva) che tra due insiemi qualsiasi aventi lo stesso numero di elementi si può stabilire una corrispondenza biunivoca e la si riformula come definizione: tutti gli insiemi tra i quali si può stabilire una corrispondenza biunivoca vengono accomunati in una classe, che è come assegnare loro una "etichetta", e a questa etichetta viene dato il nome di numero naturale.

4.2 Insiemi infiniti: la cardinalità del numerabile

Tutto ciò di cui abbiamo parlato nel precedente paragrafo si riferisce ad insiemi che contengono un numero finito di elementi, ossia, ad insiemi *finiti*. D'altra parte, appare naturale estendere le stesse idee ad insiemi *infiniti*: analogamente

[2] In realtà, il paradosso di Russell mostra che parlare dell'insieme di tutti gli insiemi è una questione piuttosto delicata.

al caso finito, diciamo che due insiemi infiniti fra i quali è possibile stabilire una corrispondenza biunivoca sono *equipotenti* o, anche, che hanno la stessa *cardinalità*. In questo modo, definiamo la *cardinalità del numerabile*.

Definizione 4.3: Un insieme (infinito) che ha la stessa cardinalità dell'insieme $\mathbb{N}$ dei numeri naturali è detto *numerabile*.

Esempio. Mostriamo, ora, che $|\mathbb{Z}| = |\mathbb{N}|$, ossia, che l'insieme $\mathbb{Z}$ dei numeri interi relativi è numerabile. A questo scopo, dobbiamo definire una corrispondenza biunivoca fra i due insiemi, ossia, una *funzione invertibile* (o biezione) f dall'insieme $\mathbb{Z}$ all'insieme $\mathbb{N}$.
La funzione f richiesta è, semplicemente,

$$\forall z \in \mathbb{Z}\ f(z) \ = \ \begin{cases} -2z & \text{se } z \leq 0 \\ 2z-1 & \text{se } z > 0\ . \end{cases}$$

È immediato verificare che f è effettivamente una biezione. □

Il prossimo teorema mostra una proprietà degli insiemi infiniti, evidenziata già dal precedente esempio, che li distingue sostanzialmente da quelli finiti. Infatti, mentre evidentemente nessun insieme finito può essere messo in corrispondenza biunivoca con un suo sottoinsieme proprio, lo stesso non si può dire per gli insiemi infiniti.

Teorema 4.1: *Ogni sottoinsieme infinito di un insieme numerabile è numerabile.*

Dimostrazione: Sia A un insieme numerabile e $B \subset A$ un suo sottoinsieme infinito. Poiché A è numerabile, esiste una biezione f fra A ed $\mathbb{N}$. Poiché $B \subset A$, allora f è definita anche sugli elementi di B; definiamo, allora, la seguente relazione d'ordine in B:

$$\forall x, y \in B\ [\ x \prec y \Leftrightarrow f(x) < f(y)\ ].$$

Sia $u \in B$ l'elemento di B associato tramite f al numero naturale più piccolo: ossia, u è tale che

$$f(u) = \min\{f(b)\ :\ b \in B\}.$$

Ora, possiamo definire il predecessore $p(x)$ di qualunque elemento $x \in B - \{u\}$: $p(x) = y$ se $y \in B$, $f(y) < f(x)$ e non esiste alcun $b \in B - \{x, y\}$ tale che $f(y) < f(b) < f(x)$.

Possiamo, infine, definire (ricorsivamente) la seguente funzione $g : B \to \mathbb{N}$:

$$g(x) \ = \ \begin{cases} 0 & \text{se } x = u; \\ g(p(y)) + 1 & \text{se } x \neq u. \end{cases}$$

La funzione g è una biezione. Infatti, ad ogni elemento $x \in B$ associa uno ed un solo elemento di $\mathbb{N}$.
Inoltre, per induzione dimostriamo il viceversa, ossia, che per ogni $n \in \mathbb{N}$ esiste uno ed un solo $b_n \in B$ tale che $n = g(b)$: questo è vero per $n = 0$ in quanto u esiste ed è unico; supponiamo, allora, che per ogni $n \leq h$ esiste uno ed un solo $b \in B$ tale che $n = g(b)$ e dimostriamo che questo implica che esiste uno ed un solo $b_1 \in B$ tale che $h + 1 = f(b_1)$. In virtù dell'ipotesi induttiva, esiste uno ed un solo $b_2 \in B$ tale che $g(b_2) = h$; sia allora $b_1 \in B$ tale che $b_2 = p(b_1)$: allora, per costruzione, $g(b_1) = g(b_2) + 1 = h + 1$ e, poiché b_2 è l'unico predecessore di B_1 e b_2 è l'unico elemento di B tale che $g(b_2) = h$, allora b_1 è l'unico elemento di B tale che $g(b_1) = h + 1$.

Il teorema è ora completamente provato. □

Intutivamente, è chiaro che due insiemi finiti fra i quali è possibile definire una corrispondenza biunivoca hanno lo stesso *numero di elementi*. Se mettiamo in corrispondenza biunivoca due insiemi *infiniti*, non possiamo più affermare che hanno lo stesso numero di elementi (perché l'infinito non è un numero!). Però, il concetto è sostanzialmente lo stesso. Cantor definì *numeri transfiniti* le cardinalità degli insiemi infiniti.

Il Teorema 4.1 dimostra che tutti gli insiemi infiniti di un insieme numerabile sono, a loro volta, numerabili, ossia, che, ammettendo l'esistenza di insiemi infiniti non numerabili, tali insiemi non numerabili non possono essere contenuti in un insieme numerabile. In altri termini, prova che gli insiemi numerabili sono gli insiemi infiniti "più piccoli" a cui

possiamo pensare. Per questa ragione, Cantor individuò nella cardinalità del numerabile il primo, più piccolo, numero trasfinito, e lo indicò utilizzando la prima lettera dell'alfabeto ebraico, aleph, con indice 0:

$$|\mathbb{N}| = \aleph_0.$$

Il Teorema 4.1 risulta utile anche nelle dimostrazioni di numerabilità. Infatti, risulta spesso più agevole individuare corrispondenze biunivoche consottoinsiemi dei numeri naturali piuttosto che con l'intero insieme dei numeri naturali: il Teorema 4.1 garantisce che questo è sufficiente.

Esempio. Mostriamo, ora, che $\mathbb{Q}^+$ è numerabile. Per provare questa affermazione, dimostriamo preliminarmente che il prodotto cartesiano $\mathbb{N} \times \mathbb{N}$ è numerabile.
Definiamo nell'insieme $\mathbb{N} \times \mathbb{N}$ la seguente relazione d'ordine $\prec$: siano $(h,k),(x,y) \in \mathbb{N} \times \mathbb{N}$, allora

$$(h,k) \prec (x,y) \Leftrightarrow [h+k < x+y] \ \vee \ [\ (h+k = x+y) \ \wedge \ (h < k)\ ].$$

In altre parole, se rappresentiamo gli elementi di $\mathbb{N} \times \mathbb{N}$ in una matrice doppiamente infinita, gli elementi su ciascuna diagonale secondaria hanno somma di indice di riga e indice di colonna costante. Allora, tutte le coppie sulla diagonale secondaria in cui tale somma vale i precedono nell'ordinamento tutte le coppie sulla diagonale secondaria il cui indice è $j > i$, mentre una coppia (h,k) precede una coppia (x,y) che si trova sulla stessa diagonale secondaria se $h < x$. Tale tecnica di ordinamento è detta *a coda di rondine* ed è illustrata in Figura 4.2.

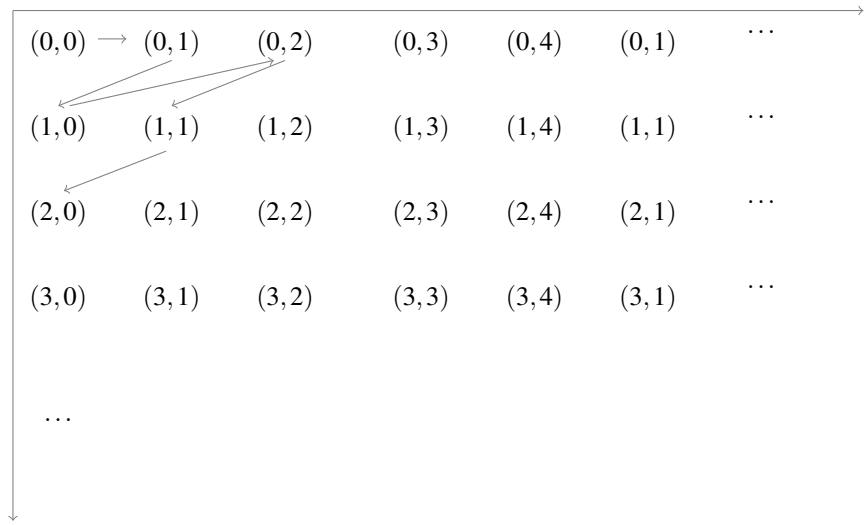

Figura 4.2: Ordinamento degli elementi dell'insieme $\mathbb{N} \times \mathbb{N}$ con la tecnica della coda di rondine.

Procediamo, ora, in maniera simile alla prova del Teorema 4.1.
Osserviamo che $(0,0)$ è l'elemento minimo in $\mathbb{N} \times \mathbb{N}$ rispetto a $\prec$. Definiamo il predecessore $p(x,y)$ di $(x,y) \in \mathbb{N} \times \mathbb{N}$ nella maniera seguente:

$$p(x,y) \ = \ \begin{cases} (x-1, y+1) & \text{se } x > 0 \\ (x+y-1, 0) & \text{se } x = 0. \end{cases}$$

In Figura 4.2 il predecessore di un elemento è quello da cui parte la freccia che lo punta.
A questo punto, come nel Teorema 4.1, definiamo ricorsivamente la biezione f fra $\mathbb{Q}$ e $\mathbb{N}$:

$$f(x,y) \ = \ \begin{cases} 0 & \text{se } (x,y) = (0,0); \\ f(p(x,y)) + 1 & \text{se } (x,y) \neq (0,0), \end{cases}$$

che esplicitata diventa

$$f(x,y) = \frac{(x+y)(x+y+1)}{2} + x + 1.$$

Questo prova che $\mathbb{N} \times \mathbb{N}$ è numerabile.

Poiché $\mathbb{Q}^+ \subset \mathbb{N} \times \mathbb{N}$ e $\mathbb{Q}$ è un insieme infinito, dal Teorema 4.1 segue che $\mathbb{Q}^+$ è numerabile. □

Osserviamo, ora, con più attenzione i due esempi proposti in questo paragrafo, circa la numerabilità di $\mathbb{Z}$ e $\mathbb{Q}^+$. Se indichiamo con $\mathbb{N}^-$ l'insieme dei numeri interi *negativi*, è ovvio che $\mathbb{N}^-$ è numerabile. Dunque, $\mathbb{Z} = \mathbb{N}^- \cup \mathbb{N}$ e $\mathbb{Q}^+ = \mathbb{N} \times \mathbb{N}$: in altri termini, $\mathbb{Z}$ è l'unione di due insiemi numerabile ed è, a sua volta, numerabile, e $\mathbb{Q}^+$ è il prodotto cartesiano di due insiemi numerabili ed è, a sua volta, numerabile.

Vediamo ora come la numerabilità di $\mathbb{Z}$ e la numerabilità di $\mathbb{Q}^+$ siano solo casi perticolari dei due teoremi seguenti, le cui dimostrazioni consistono, sostanzialmente, negli stessi argomenti utilizzati per mostrare la numerabilità di $\mathbb{Z}$ e $\mathbb{Q}$, rispettivamente.

Teorema 4.2: *Siano A e B due insiemi numerabili. Allora, $A \cup B$ è numerabile.*

Teorema 4.3: *Siano A e B due insiemi numerabili. Allora, il prodotto cartesiano $A \times B$ di A e B è numerabile.*

I due Teoremi 4.2 e 4.3 sono facilmente generalizzabili, rispettivamente, ad unioni e prodotti cartesiani di un numero *finito* di insiemi numerabili.

Prima di procedere, osserviamo che, se un insieme A è numerabile, allora i suoi elementi sono i termini di una successione. Infatti, poiché A è numerabile, esiste una biezione $f : A \to \mathbb{N}$. Allora, per ogni $j \in \mathbb{N}$, denotiamo con

$$a_j = f^{-1}(j),$$

ossia, a_j è l'elemento di A corrispondente secondo f al numero intero j. Allora, possiamo denotare l'insieme A nella forma

$$A = \{a_j : j \in \mathbb{N}\}.$$

La precedente osservazione ci permette di generalizzare il Teorema 4.2 anche ad unioni numerabili, come illustrato nel seguente teorema.

Teorema 4.4: *Sia $\{A_i : i \in \mathbb{N}\}$ una successione di insiemi numerabili. Allora, $\cup_{i\in\mathbb{N}} A_i$ è un insieme numerabile.*

Dimostrazione: Per ogni $i \in \mathbb{N}$, poiché A_i è numerabile possiamo elencarne gli elementi in forma di successione: $A_i = \{a_{ij} : j \in \mathbb{N}\}$. Questo induce naturalmente una biezione fra $\cup_{i\in\mathbb{N}} A_i$ e $\mathbb{N} \times \mathbb{N}$ che, per il Teorema 4.3 è numerabile. Poiché la composizione di biezioni è una biezione, questo implica che esiste una biezione fra $\cup_{i\in\mathbb{N}} A_i$ e $\mathbb{N}$, ed il teorema è completamente provato. □

Osserviamo esplicitamente che rimane aperta, per il momento la questione circa la cardinalità del prodotto cartesiano di una infinità numerabile di insiemi numerabili. Questa questione verrà chiusa nel prossimo paragrafo.

4.3 Esistono insiemi più che numerabili?

La domanda cui intendiamo rispondere in questo paragrafo è la seguente: esistono insiemi che non sono numerabili, ossia, che non possono essere messi in corrispondenza biunivoca con l'insieme $\mathbb{N}$ dei numeri naturali?

Come abbiamo già osservato, gli insiemi numerabili sono gli insiemi infiniti "più piccoli" che possono essere definiti: infatti, intuitivamente, se aggiungiamo un elemento ad un insieme vuoto, poi un elemento a questo nuovo insieme, poi ancora un altro elemento, e così via, arriviamo, dopo una sequenza infinita di passi ad ottenere un insieme infinito e numerabile (infatti, per costruzione, abbiamo un primo elemento, un secondo elemento, e così via). In questo procedimento, prima di "raggiungere l'infinito" non avevamo altro che un insieme finito. Questo significa che ogni insieme infinito o è numerabile o è "più grande" di un insieme numerabile. In termini più formali,

Teorema 4.5: *Ogni insieme infinito è numerabile oppure contiene propriamente un insieme numerabile.*

Dimostriamo ora che esistono insiemi non numerabili utilizzando la tecnica di *diagonalizzazione*, una particolare tecnica di dimostrazione *per assurdo* introdotta da Cantor nell'articolo del 1874 "Über eine Eigenschaft des Inbegriffes aller reellen algebraischen Zahlen" (*Su una proprietà della collezione dei numeri reali algebrici*), il primo articolo a presentare una dimostrazione rigorosa dell'esistenza di più di un tipo di infinito. Cantor fu il primo a capire che gli insiemi infiniti possono avere diverse grandezze: dapprima mostrò che, dato un qualsiasi insieme A, esiste l'insieme di tutti i possibili sottoinsiemi di A, chiamato *insieme potenza* di A o *insieme delle parti* di A e che si indica con i simboli 2^A oppure $\mathscr{P}(A)$. Poi, dimostrò che l'insieme potenza di un insieme infinito ha una cardinalità maggiore della propria: questo risultato è oggi noto con il nome di *teorema di Cantor*. La conseguenza del teorema di Cantor è che

esiste una gerarchia infinita di grandezze di insiemi infiniti.

Infatti, se A_1 è un insieme infinito allora, per il teorema di Cantor, $A_2 = 2^{A_1}$ ha cardinalità maggiore di A_1. E l'insieme $A_3 = 2^{A_2}$ ha cardinalità maggiore di A_2 e così via.

In ciò che segue dimostreremo una versione più debole del teorema di Cantor, ossia, ci limiteremo a considerare l'insieme delle parti di un insieme numerabile.

Teorema 4.6: *Sia S un insieme numerabile. Allora 2^S non è un insieme numerabile.*

Dimostrazione: Sia A un qualunque sottoinsieme di S, e χ_A la sua funzione caratteristica: per ogni $x \in S$,

$$\chi_A(x) \;=\; \begin{cases} 0 & \text{se } x \in A, \\ 1 & \text{se } x \in S - A. \end{cases}$$

Poiché S è numerabile, esiste una biezione $f : S \to \mathbb{N}$; allora, per ogni $A \subseteq S$, rappresentiamo A mediante una sequenza binaria di lunghezza infinita $b_1^A b_2^A \ldots b_n^A \ldots$ tale che $b_i^A = \chi_A(f^{-1}(i))$. In altri termini, $b_i^A = 1$ se e solo se $i = f(\overline{x})$ e $\overline{x} \in A$).
Osserviamo anche che, poiché f è invertibile, allora vale anche l'inverso, ossia, che ogni sequenza binaria di lunghezza infinita corrisponde a qualche sottoinsieme di S.
Dunque, riassumendo: *ogni sottoinsieme di S è rappresentato da una sequenza binaria di lunghezza infinita e, viceversa, ogni sequenza binaria di lunghezza infinita rappresenta un sottoinsieme di S.*

Supponiamo ora che 2^S sia numerabile: allora, dovrebbe esistere una biezione g fra 2^S e $\mathbb{N}$. Costruiamo, allora, una matrice infinita M così definita: per ogni $i, j \in \mathbb{N}$,

$$M_{ij} = \chi_{g^{-1}(i)}(f^{-1}(j)),$$

ossia, per ogni $i \in \mathbb{N}$ se $A_i \in 2^S$ è l'elemento di S^S tale che $g(A_i) = i$ allora, per ogni $j \in \mathbb{N}$, $M_{ij} = b_j^{A_i}$.
Osserviamo che, con questa costruzione, per ogni $i \in \mathbb{N}$, la riga i della matrice corrisponde al sottoinsieme A_i di S, ossia, al sottoinsieme $A_i \in 2^S$ tale che $g(A_i) = i$. D'altra parte, poiché g è una biezione fra 2^S e $\mathbb{N}$, ogni elemento di S è rappresentato da una riga della matrice.

Consideriamo, ora, la sequenza binaria $c = c_1 c_2 \ldots$ costituita dagli elementi sulla diagonale di M complementati, ossia:

$$\forall i \in \mathbb{N} \; [\; c_i \;=\; 1 - M_{ii} \;].$$

Poiché c è una sequenza binaria di lunghezza infinita, anch'essa rappresenta un sottoinsieme C di S. D'altra parte, per costruzione, c è diversa da ogni riga della matrice M: infatti, per ogni $i \in \mathbb{N}$, $c_i \neq M_{ii}$ e, quindi, c è diversa dalla riga i di M.

Allora, abbiamo trovato un elemento $C \in 2^S$ che non è rappresentato in nessuna riga della matrice contraddicendo l'ipotesi che g fosse una biezione, ossia, che 2^S fosse numerabile. □

Il Teorema 4.6 si presta a diverse interpretazioni, una delle quali ci apprestiamo ad analizzare.

Indichiamo con U l'insieme dei numeri reali compresi fra 0 e 1 la cui parte decimale è costituita da sole cifre 0 e 1. Ad esempio, elementi di U sono i numeri $0,1$, $0,0101101$, che hanno un numero finito di cifre decimali, ma anche il numero

$$\frac{1}{10} + \frac{1}{1000} + \frac{1}{100000} + \ldots = \sum_{i=0}^{\infty} \frac{1}{10^{2i+1}} = 0,1010101\ldots$$

che ha un numero infinito di cifre decimali. Rappresentiamo,ora, *ogni* elemento di U mediante un numero infinito di cifre decimali, ossia, aggiungiamo una serie infinita di zeri ad ogni decimale finito in U: ad esempio, rappresentiamo il decimale finito $0,1 \in U$ nella forma $0,10000000\ldots$.
Osserviamo, ora, alla luce della dimostrazione del Teorema 4.6, che gli elementi di U sono in corrispondenza biunivoca (banale) con gli elementi di $2^{\mathbb{N}}$ e, quindi, $|U| = |\mathbb{N}| > \aleph_0$. Abbiamo, dunque, dimostrato che U non è numerabile. Osserviamo esplicitamente che, alla luce di quanto osservato all'inizio di questo paragrafo, questo significa che l'insieme U è "più grande" dell'insieme $\mathbb{N}$, ossia, che U, l'intervallo unitario, contiene propriamente un insieme che ha la stessa cardinalità di $\mathbb{N}$!

Da quanto osservato, segue direttamente il seguente corollario.

Corollario 4.1: *L'insieme $\mathbb{R}$ dei numeri reali è non numerabile.*

Dimostrazione: L'insieme U sopra definito è un sottoinsieme proprio di $\mathbb{R}$: $U \subset \mathbb{R}$. Inoltre U non è numerabile.
In virtù del Teorema 4.1, ogni sottoinsieme di un insieme numerabile è numerabile.
Allora, $\mathbb{R}$ non è numerabile. □

Consideriamo, ora, l'insieme prodotto cartesiano di una infinità numerabile di insiemi binari, ossia,

$$\Pi_{i\in\mathbb{N}} U_i = U_1 \times U_2 \times \ldots$$

dove, per ogni $i \in \mathbb{N}$, $U_i = \{0,1\}$.
Osserviamo, ora, che tale insieme coincide con l'insieme $2^{\mathbb{N}}$. Questo prova il seguente corollario.

Corollario 4.2: *Se $\{A_i : i \in \mathbb{N}\}$ è una infinità numerabile di insiemi finiti o numerabili, allora il loro prodotto cartesiano $\Pi_{i\in\mathbb{N}} A_i$ non è numerabile.*

4.4 L'ipotesi del continuo

Cantor aveva scoperto i numeri transfiniti. In particolare:

1) aveva individuato il più piccolo numero transfinito $\aleph_0 = |\mathbb{N}$;
2) aveva dimostrato che $|\mathbb{R}| = 2^{\aleph_0}$ e aveva chiamato tale numero transfinito c, ossia, *cardinalità (o potenza) del continuo*;
3) aveva dimostrato che $c > \aleph_0$.

Con lo stesso procedimento utilizzato per ottenere la potenza del continuo, è poi possibile considerare tutti i sottoinsiemi di $\mathbb{R}$ ed ottenere un nuovo insieme la cui cardinalità è maggiore di quella di $\mathbb{R}$. Si potrebbe, poi, applicare lo stesso ragionamento a questo nuovo insieme, e così via. Cantor, cioè, aveva dimostrato che

la cardinalità dell'insieme delle parti di un qualunque insieme è maggiore della cardinalità dell'insieme stesso, ossia, per ogni insieme (finito o meno) A:

$$|A| < |2^A|.$$

Cantor aveva dimostrato, quindi, l'esistenza di una quantità infinita di numeri transfiniti, di grandezza crescente: $\aleph_0$, $2^{\aleph_0}$, $2^{2^{\aleph_0}}$, $\ldots$

Ma Cantor non era ancora soddisfatto: egli desiderava conoscere l'*ordine* dei suoi numeri cardinali transfiniti, ossia, voleva poterli elencare consecutivamente come

$$\aleph_0,\ \aleph_1,\ \aleph_2,\ \ldots$$

In particolare, egli si pose la seguente domanda: esiste un altro numero transfinito fra $\aleph_0$ e $c = 2^{\aleph_0}$? Se la risposta fosse stata no, egli avrebbe potuto concludere che $\aleph_1 = 2^{\aleph_0}$, ma, in assenza di una risposta Cantor non poteva ordinare

i numeri cardinali transfiniti perché non era in grado di dire quale fosse il successore immediato di $\aleph_0$. Quello che Cantor si proponeva di dimostrare, dunque, è che

$$2^{\aleph_0} = \aleph_1,$$

ossia, quella che è stata chiamata *l'ipotesi del continuo*.

Cantor si rese conto che, per sperare di dimostrare l'ipotesi del continuo doveva trovare un modo per confrontare ed *ordinare* i numeri cardinali transfiniti, ossia, dati comunque due numeri transfiniti, per poter dir se sono uguali o quale dei due è maggiore dell'altro. Mentre l'ordinamento è un concetto intuitivo quando si parla di numeri (finiti), per poterlo estendere ai numeri trasfiniti Cantor dovette definire una particolare proprietà degli insiemi, detta *principio del buon ordinamento*.
Un insieme si dice *bene ordinato* se ognuno dei suoi sottoinsiemi non vuoti ha un elemento più piccolo; il *principio del buon ordinamento* afferma che ogni insieme è bene ordinato.

Se fosse stato dimostrato il principio del buon ordinamento, allora l'insieme dei numeri transfiniti si sarebbe potuto rappresentare come una sequenza

$$\aleph_0,\ \aleph_1,\ \aleph_2,\ \ldots$$

ed il continuo c non avrebbe potuto essere che uno di questi aleph; ma, fino a quando non fosse stato dimostrato il principio del buon ordinamento, non sarebbe stato possibile collocare c all'interno del sistema degli aleph.

Cantor non riuscì a dimostrare il principio del buon ordinamento, ma vi riuscì, nel 1904, un altro eminente matematico tedesco, Ernst Zermelo (1871-1953), che dedicò gran parte della propria vita alla formalizzazione della teoria degli insiemi.
La dimostrazione iniziava associando un punto rappresentativo ad ogni sottoinsieme non vuoto di un dato insieme, che Zermelo chiamò *elemento distinto* del sottoinsieme.: il punto rappresentativo di un sottoinsieme, semplicemente, viene scelto fra tutti i punti del sottoinsieme. Per effettuare questa scelta, Zermelo si basò su un principio di selezione che chiamò *assioma di scelta*. Posto tale assioma, la sua dimostrazione del principio di buon ordinamento era semplice ed elegante.
Ma già pochi giorni dopo la pubblicazione della dimostrazione numerosi matematici sollevarono una serie di obiezioni, tutte generate dall'assioma di scelta. Se il numero di sottoinsiemi è finito, scegliere un elemento da ciascuno di essi è una procedura semplice. Le cose cambiano quando consideriamo un numero infinito di sottoinsiemi: anche nel caso in cui ciascun sottoinsieme contenga solo due elementi, se il numero di sottoinsiemi è infinito, non sembra così evidente che riusciremo ad effettuare le scelte giuste. Il problema identificato dai matematici consisteva in questo: Zermelo non illustrava alcun em metodo, alcuna *regola* per effettuare la scelta un numero infinito di volte, si limitava ad affermare che tale scelta poteva essere effettuata. Quindi l'assioma di scelta e la dimostrazione di Zermelo del principio di buon ordinamento divennero sospetti.

È a questo punto che entra in scena un altro dei grandi logici del novecento: Kurt Gödel (1906-1978). Gödel iniziò i suoi studi per il conseguimento del dottorato in matematica sotto la supervisione di Hans Hahn, uno dei due autori del teorema di Hahn-Banach, importante risultato nell'ambito dell'analisi superiore. La dimostrazione del teorema di Hahn-Banach utilizza il *lemma di Zorn*, un'asserzione secondo la quale, se ogni catena di un insieme parzialmente ordinato ha una delimitazione superiore, allora l'insieme parzialmente ordinato ha un elemento massimale. Ma il lemma di Zorn è equivalente all'assioma di scelta: dunque, il teorema di Hahn-Banach dipende dalla verità dell'assioma di scelta.
Studiando il teorema di Hahn-Banach, Gödel si rese conto dell'importanza e della potenza della teoria degli insiemi ed iniziò a studiare l'assioma di scelta, interessandosi anche all'ipotesi del continuo di Cantor. Gödel fece un importante passo avanti in questi studi, nella notte fra il 14 e il 15 giugno 1937, come si evince da una sua nota scritta in un quaderno, ma pubblicò il risultato soltanto qualche anno dopo: egli dimostrò che

l'assioma di scelta e l'ipotesi del continuo non sono incompatibili con gli altri assiomi della teoria degli insiemi,

ossia che, se considerati veri, non inducono alcuna contraddizione con gli altri assiomi della teoria degli insiemi (per i quali si rimanda all'Appendice B). La dimostrazione di Gödel non implica che l'assioma di scelta o l'ipotesi del continuo siano asserzioni vere: la dimostrazione significa soltanto che, se i fondamenti della matematica sono coerenti, allora essi rimangono tali anche *assumendo vere* entrambe le asserzioni.

In effetti, il risultato di Gödel è a metà strada nel dimostrare la completa *indipendenza* dell'assioma di scelta e della ipotesi del continuo dai rimanenti assiomi della teoria degli insiemi. L'altra metà della prova di indipendenza è dovuta a Paul Cohen (1934-2007), ed è datata 1963. Utilizzando un nuovo metodo, chiamato *forcing*, Cohen terminò la dimostrazione della *completa indipendenza* dell'ipotesi del continuo e dell'assioma di scelta dagli assiomi della teoria degli insiemi, ossia che

se i fondamenti della matematica sono coerenti, allora essi rimangono tali anche sia assumendo veri che assumendo falsi l'ipotesi del continuo e l'assioma di scelta.

L'unione dei risultati di Gödel e di Cohen viene solitamente considerato un esempio nella matematica di proposizioni indecidibili che il teorema di incompletezza di Gödel[3] aveva precedentemente dimostrato esistere. In effetti, Gödel e Cohen avevano definitivamente stabilito che la verità cantoriana dell'ipotesi del continuo non può essere determinata all'interno dell'attuale sistema di assiomi della teoria degli insiemi.
Questo non significa necessariamente che il teorema di incompletezza di Gödel sia applicabile all'ipotesi del continuo: è possibile che essa sia dimostrabile o confutabile partendo da un diverso sistema di assiomi. Quello che le dimostrazioni di Gödel e Cohen hanno provato è che *all'interno del presente sistema di assiomi* l'ipotesi del continuo potrebbe essere considerata sia vera che falsa senza che da ciò derivi alcuna contraddizione.

[3] Informalmente, il teorema di incompletezza di Gödel afferma che: dato un qualunque sistema formale, esistono sempre teoremi che non sono dimostrabili all'interno di quel sistema. Quindi, anche se il teorema è vero può essere impossibile dimostrarlo (in quel sistema). Sul teorema di incompletezza di Gödel torneremo più avanti.

Appendice A. Un linguaggio per l'aritmetica

Giuseppe Peano (1858-1932) era affascinato dall'ideale leibniziano della lingua universale. Uno dei grandi meriti dell'opera di Peano sta nella ricerca della chiarezza, della semplificazione, dello sviluppo di una notazione sintetica. Proprio in questa ottica va collocata la sua definizione di un'aritmetica dei numeri naturali.

Come abbiamo già visto, storicamente, la precisa definizione matematica dei numeri naturali ha incontrato alcune difficoltà. Peano propose una definizione assiomatica dei numeri naturali, che venne successivamente ripresa da Russell e Whitehead nei loro *Principia Mathematica*, di cui parleremo più avanti.

Peano cercò una definizione dei numeri naturali che partisse dal concetto di insieme e che utilizzasse soltanto operazioni della teoria degli insiemi. Seguendo questa direzione di pensiero, egli definì il numero 0 come l'insieme vuoto; allora, il numero 1 era l'insieme che conteneva l'insieme vuoto e, di seguito, il 2 l'insieme che conteneva l'insieme vuoto e l'insieme che conteneva l'insieme vuoto, e così via:

$$0 = \emptyset, \qquad 1 = \{\emptyset\}, \qquad 2 = \{\emptyset, \{\emptyset\}\}, \qquad 3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\},\} \qquad \ldots$$

Gli assiomi di Peano, presentati intorno al 1889, definiscono le condizioni che ogni definizione matematica precisa di una aritmetica dei numeri naturali deve soddisfare: per questa ragione ci si riferisce al sistema assiomatico di Peano come alla *Aritmetica di Peano*, in breve *PA*.

Il linguaggio di PA è il linguaggio dell'aritmetica del primo ordine, ovvero è costituito dai seguenti simboli:

- simboli per variabili: x, y, z, x_1, x_2, $\ldots$
- costanti individuali: 0;
- simboli per funzioni unarie: S;
- simboli per funzioni binarie: $+$, $\times$;
- simboli per relazioni binarie: $=$;
- simboli per connettivi logici, quantificatori e parentesi.

Nella sintassi di PA, per indicare la funzione binaria $+$ calcolata sui termini x e y, anziché scrivere $+(x,y)$ (notazione funzionale) si è soliti scrivere $x+y$ (notazione operazionale). Una convenzione analoga vale per la funzione binaria $\times$.

Gli assiomi di PA sono costituiti dagli assiomi logici, gli assiomi per l'uguaglianza e i seguenti assiomi propri:

(PA1) $\forall x \neg(S(x) = 0)$

(PA2) $\forall x \forall y(S(x) = S(y) \rightarrow x = y)$

(PA3) $\forall x(x + 0 = x)$

(PA4) $\forall x \forall y(x + S(y) = S(x + y))$

(PA5) $\forall x(x \times 0 = 0)$

(PA6) $\forall x \forall y(x \times S(y) = x \times y + x)$

(PA7) $\varphi(0, x_1, \ldots, x_n) \wedge (\forall x(\varphi(x, x_1, \ldots, x_n) \rightarrow \varphi(S(x), x_1, \ldots, x_n))) \rightarrow \forall x(\varphi(x, x_1, \ldots, x_n))$ per ogni formula ben formata φ in cui $x_1, \ldots, x_n$ sono variabili libere (ossia, non quantificate). Una formula ben formata è una stringa di simboli che, intuitivamente, rappresenti un'espressione sintatticamente corretta e che viene definita mediante le regole della grammatica del sistema formale stesso.

L'assioma (PA7) definisce la chiusura universale del sistema di assiomi ed è chiamato *schema di induzione*. Si osservi che si ha un assioma distinto per ogni formula ben formata.

In realtà, Peano ha definito uno schema di assiomi appartenenti alla logica dei predicati del secondo ordine di cui lo schema sopra è solo una restrizione. Negli *assiomi di Peano*, l'ultimo assioma (il principio di induzione) richiede un uso di quantificatori sui sottoinsiemi dei numeri naturali:

$$\forall U[(\ (0 \in U)\ \wedge\ \forall x((x \in U) \rightarrow (S(x) \in U))) \rightarrow \forall x(x \in U).$$

Per questa ragione, si tratta di un sistema espresso nella logica del secondo ordine.

La versione degli assiomi di Peano nella logica del primo ordine (gli assiomi (PA1)-(PA7) descritti sopra) è chiamata *aritmetica di Peano* ed ha un ruolo molto importante nella teoria della calcolabilità e nella logica matematica poiché soddisfa le condizioni di validità dei teoremi di incompletezza di Gödel.

Appendice B. Gli assiomi della Teoria degli Insiemi

Lo scopo degli assiomi della Teoria degli Insiemi è quello di fornire le basi sulle quali fondare la Matematica. Gli assiomi vennero introdotti da Zermelo e da altri logici all'inizio del XX secolo; dopo anni di ricerche è stato individuato un insieme minimale di assunzioni che permettono di definire coerentemente numeri naturali, reli e complessi, con le rispettive operazioni e proprietà, ed a tale insieme facciamo riferimento in quel che segue.

Osserviamo esplicitamente che gli assiomi vennero in larga misura ispirati dal lavoro di Cantor, che utilizzò implicitamente alcuni di essi per lo sviluppo della Teoria degli Insiemi.

Assioma di esistenza: *esiste almeno un insieme.*
L'insieme vuoto è quello la cui esistenza è postulata dall'assioma. Altri insiemi possono poi essere costruiti a partire da questo (si veda l'Appendice A).

Assioma di estensione: *due insiemi sono uguali se e soltanto se hanno gli stessi elementi.*

Assioma di specificazione: *ad ogni insieme A e ad ogni condizione π corrisponde un insieme B i cui elementi sono tutti e soli gli elementi x di A per i quali $\pi(x)$ è vera.*
Come vedremo, è questo il principio di comprensione di Frege ed è quello che conduce al paradosso di Russell.

Assioma di coppia: *dati due insiemi esiste un insieme al quale entrambi appartengono.*

Assioma di unione: *dato un insieme di insiemi A esiste un insieme B che contiene tutti gli elementi che appartengono ad almeno uno degli insiemi appartenenti ad A.*

Assioma di insieme delle parti: *dato un insieme esiste un insieme di insiemi che contiene tra i suoi elementi tutti i sottoinsiemi dell'insieme dato.*
Cantor ha dimostrato che l'insieme delle parti di un insieme ha sempre cardinalità maggiore di quella dell'insieme. Questo condusse alla conclusione paradossale che non esiste un insieme che contiene *tutti* gli insiemi, o un numero cardinale più grande di tutti gli altri: infatti, in base a questo assioma, se esistesse un insieme che contiene tutti gli insiemi allora esisterebbe anche il suo insieme delle parti che lo conterrebbe.

Assioma dell'infinito: *esiste un insieme che contiene lo* 0 *ed il successore di tutti i suoi elementi.*

Questo assioma ci aiuta a definire i numeri naturali: iniziamo con 0, aggiungiamo 1 per ottenere 1, poi aggiungiamo ancora 1 per ottenere 2, e così via.

Assioma di scelta: *per ogni insieme A esiste una funzione di scelta f tale che, per ogni sottoinsieme non vuoto B di A, $f(B)$ è un elemento di B.*
La funzione f sceglie un elemento da ciascun sottoinsieme non vuoto di A: come abbiamo visto, la controversia su questo assioma nasce quando il numero di sottoinsiemi di A è infinito.

Nota

Il paragrafo 4.4 è stato largamente ispirato dai contenuti di A. D. Acziel, *Il mistero dell'alef* (Il Saggiatore), incentrato sulla vita e il lavoro di Georg Cantor. Dallo stesso libro, anche spunti per l'Appendice B.