Metodi Matematici per l'Informatica - Dispensa 10
(a.a. 23/24, I canale)

Docente: Lorenzo Carlucci (`lorenzo.carlucci@uniroma1.it`)

1 Cardinalità, equicardinalità

Se A e B sono insiemi finiti è piuttosto facile convincersi che esiste una biiezione tra A e B se e solo se A e B hanno lo stesso numero di elementi. In questo caso diciamo che hanno la stessa cardinalitù e scriviamo $\#(A) = \#(B)$.

Osservazione 1 *Se esiste una iniezione $f : A \to B$ allora $\#(A) \leq \#(B)$.*

Osservazione 2 *Se esiste una suriezione $f : A \to B$ allora $\#(A) \geq \#(B)$.*

Ne segue ovviamente che

Osservazione 3 *Se esiste una biiezione tra A e B allora $\#(A) = \#(B)$.*

In modo altrettanto semplici ci si convince (almeno intuitivamente) che valgono anche le implicazioni inverse.

Cosa accade se generalizziamo queste idee a insiemi arbitrari, in particolare a insiemi infiniti? L'idea, dovuta al matematico Georg Cantor (1845-1918), è una delle idee più rivoluzionarie della Matematica dell'Ottocento, e ha avuto grande impatto sulle scienze matematiche dei secoli successivi.

Poniamo, in analogia con il caso finito, la seguente definizione, che racchiude l'idea che due insiemi hanno lo stesso *numero di elementi* o la stessa *cardinalità* se possono essere posti in corrispondenza biiettiva.

Definizione 1 (Equipotenza, equicardinalità) *Siano A e B due insiemi. Diciamo che A e B hanno la stessa cardinalità se esiste una biiezione tra A e B. In questo caso scriviamo $\#(A) = \#(B)$.*

Osservazione 4 *La definizione di sopra definisce una* relazione *tra due insiemi A e B. La relazione sussiste se e solo se esiste una biiezione tra i due insiemi. In questo caso scriviamo $\#(A) = \#(B)$. Non dobbiamo però presupporre che questa relazione sia una vera identità tra due oggett $\#(A)$, $\#(B)$ (che non abbiamo neanche definito!). Possiamo però assicurarci che la relazione definita soddisfi alcune proprietà fondamentali dell'identità, ossia* si comporta *come una identità.*

Per ogni insieme A vale $\#(A) = \#(A)$, perché esiste sempre una biiezione tra A e A; per esempio l'identità. Si dice che la relazione di equicardinalità è *riflessiva*.

Per insiemi A, B se $\#(A) = \#(B)$ allora $\#(B) = \#(A)$ (si noti che questa implicazione non è scontata in base alle definizioni!!): $\#(A) = \#(B)$ significa che esiste una biiezione $f : A \to B$. Possiamo concludere che esiste una biiezione $h : B \to A$? Sì – lo abbiamo già osservato: ogni funzione biiettiva è invertibile. Dunque vale $\#(B) = \#(A)$. Si dice che la relazione di equicardinalità è *simmetrica*: se A è in relazione con B allora B è in relazione con A.

Per insiemi A, B, C, se vale $\#(A) = \#(B)$ e $\#(B) = \#(C)$ allora vale $\#(A) = \#(C)$. $\#(A) = \#(B)$ significa che esiste una biiezione $f : A \to B$; $\#(B) = \#(C)$ significa che esiste una biiezione $g : B \to C$. Possiamo concludere $\#(A) = \#(C)$, ossia che esiste una biiezione $h : A \to C$? Sì – lo abbiamo già osservato: la composizione di biiezioni è una biiezione; la h desiderata è $(g \circ f) : A \to C$. Si dice che la relazione di equicardinalità è *transitiva*: se A è in relazione con B e B è in relazione con C allora A è in relazione con C.

2 Insiemi numerabili

Abbiamo già dimostrato che esiste una biiezione tra $\mathbf{N} = \{1, 2, 3, 4, \dots\}$ e $P = \{2, 4, 6, 8, \dots\}$. Possiamo dunque scrivere

$$\#(\mathbf{N}) = \#(P).$$

Osservazione 5 *Si osservi che P è un sottinsieme proprio di $\mathbf{N}$, ossia è un sottinsieme di $\mathbf{N}$ ma non coincide con $\mathbf{N}$ — anzi, a P mancano più o meno la metà degli elementi di $\mathbf{N}$. Eppure, secondo la nostra definizione, i due insiemi hanno la stessa cardinalità, ossia lo stesso* numero di elementi*. Questa proprietà di $\mathbf{N}$ può essere scelta come* definizione *di insieme infinito, in una trattazione assiomatica rigorosa. Noi useremo infinito nel senso intuitivo, e* finito *come equivalente a essere in biiezione con $\{1, 2, 3, \dots, n\}$ per qualche $n \in \mathbf{N} \cup \{0\}$.*

Naturali e Interi Consideriamo l'insieme $\mathbf{Z}$ dei numeri interi. La seguente tabella definisce una biiezione tra $\mathbf{Z}$ e $\mathbf{N}$:

N	1	2	3	4	5	6	7	8	9	10	11	12	...
Z	0	1	-1	2	-2	3	-3	4	-4	5	-5	6	...

Possiamo dunque concludere che $\#(\mathbf{N}) = \#(\mathbf{Z})$.

Esercizio 1 *Scrivere una forma chiusa per la funzione f.*

Coppie ordinate Consideriamo l'insieme $\mathbf{N}\times\mathbf{N}$ delle coppie ordinate di naturali (detto Prodotto Cartesiano di $\mathbf{N}$). Risulta naturale scriverlo in forma di diagramma Cartesiano:

...	...	...	...	...	...	...	...	...	...	...
(1,4)	(2,4)	(3,4)	(4,4)	(5,4)	(6,4)	(7,4)	(8,4)	(9,4)	(10,4)	...
(1,3)	(2,3)	(3,3)	(4,3)	(5,3)	(6,3)	(7,3)	(8,3)	(9,3)	(10,3)	...
(1,2)	(2,2)	(3,2)	(4,2)	(5,2)	(6,2)	(7,2)	(8,2)	(9,2)	(10,2)	...
(1,1)	(2,1)	(3,1)	(4,1)	(5,1)	(6,1)	(7,1)	(8,1)	(9,1)	(10,1)	...

Stabilire una biiezione tra $\mathbf{N}$ e $\mathbf{N} \times \mathbf{N}$ equivale a individuare un modo di *percorrere* la tabella di sopra toccando ogni suo punto una e una sola volta. Vi sono molti modi di farlo (visti in classe) e ognuno di essi corrisponde a una biiezione.

Per esempio possiamo percorrerla seguendo le diagonali da Nord Ovest a Sud Est, partendo dal punto più a Sud Ovest:

$$\underbrace{(1,1)}_{\text{prima diagonale}}, \underbrace{(1,2),(2,1)}_{\text{seconda diagonale}}, \underbrace{(1,3),(2,2),(3,1)}_{\text{terza diagonale}}, \underbrace{(1,4),(2,3),(3,2),(4,1)}_{\text{quarta diagonale}}, \dots$$

Oppure possiamo partire da $(1,1)$ e procedere secondo uno zig-zag sempre più ampio:

$$(1,1),(1,2),(2,2),(2,1),(3,1),(3,2),(3,3),(2,3),(1,3),(1,4),(2,4),(3,4),(4,4)$$

Dunque concludiamo che $\#(\mathbf{N}) = \#(\mathbf{N} \times \mathbf{N})$.

Esercizio 2 *Dimostrare che anche gli insiemi delle triple, quadruple, quintuple e in generale n-ple ordinate di $\mathbf{N}$ sono in corrispondenza biunivoca con $\mathbf{N}$. Questi insiemi si denotano con $\mathbf{N}\times\mathbf{N}\times\mathbf{N}$, $\mathbf{N}\times\mathbf{N}\times\mathbf{N}\times\mathbf{N}$ etc. (Suggerimento: ridurre le triple a coppie di una coppia e di un elemento).*

Esercizio 3 *Sia f la funzione da $\mathbf{N}\times\mathbf{N} \to \mathbf{N}$ definita come segue:*

$$f(m,n) = \frac{(m+n-2)\times(m+n-1)}{2} + m.$$

Si tratta di una iniezione? Si tratta di una biiezione? Corrisponde a un modo di percorrere la tabella esaurendola tutta e toccando ogni punto una volta soltanto?

Esercizio 4 *Consideriamo la funzione* $h : \mathbf{N} \times \mathbf{N} \to \mathbf{N}$ *definita come segue:*

$$h(m, n) = 2^{n-1}(2m - 1).$$

Si tratta di una iniezione? Si tratta di una biiezione? Corrisponde a un modo di percorrere la tabella esaurendola tutta e toccando ogni punto una volta soltanto?

L'argomento di sopra funziona in modo del tutto equivalente se consideriamo l'insieme $A \times B$ delle coppie ordinate (a, b) con $a \in A$ e $b \in B$ per A e B insiemi in corrispondenza biunivoca con $\mathbf{N}$. L'esistenza di una corrispondenza biunivoca tra un insieme X e $\mathbf{N}$ si traduce facilmente nella possibilità di *enumerare* gli elementi in una lista infinita (indicizzata dai naturali) in cui compaiono tutti e soli gli elementi di X senza ripetizioni: ossia possiamo scrivere X come $\{x_1, x_2, x_3, \dots\}$.

Se A e B sono in biiezione con $\mathbf{N}$, possiamo scrivere $A = \{a_1, a_2, a_3, \dots\}$ e $B = \{b_1, b_2, b_3, \dots\}$ e ordinare il loro prodotto $A \times B$ in una tabella come sopra:

$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
(a_1, b_4)	(a_2, b_4)	(a_3, b_4)	(a_4, b_4)	(a_5, b_4)	(a_6, b_4)	(a_7, b_4)	(a_8, b_4)	(a_9, b_4)	(a_10, b_4)	$\dots$
(a_1, b_3)	(a_2, b_3)	(a_3, b_3)	(a_4, b_3)	(a_5, b_3)	(a_6, b_3)	(a_7, b_3)	(a_8, b_3)	(a_9, b_3)	(a_10, b_3)	$\dots$
(a_1, b_2)	(a_2, b_2)	(a_3, b_2)	(a_4, b_2)	(a_5, b_2)	(a_6, b_2)	(a_7, b_2)	(a_8, b_2)	(a_9, b_2)	(a_10, b_2)	$\dots$
(a_1, b_1)	(a_2, b_1)	(a_3, b_1)	(a_4, b_1)	(a_5, b_1)	(a_6, b_1)	(a_7, b_1)	(a_8, b_1)	(a_9, b_1)	(a_10, b_1)	$\dots$

Possiamo poi percorrerla come abbiamo fatto per $\mathbf{N} \times \mathbf{N}$ stabilendo così una biiezione con $\mathbf{N}$.

Naturali e Razionali Sembrerebbe che tutti gli insiemi finiti abbiamo la stessa cardinalità di $\mathbf{N}$.

Definiamo *infinito numerabile* un insieme in biiezione con $\mathbf{N}$.

Consideriamo $\mathbf{Q}$, l'insieme dei razionali. Da un certo punto di vista, intuitivamente, $\mathbf{Q}$ è più ricco di elementi rispetto a $\mathbf{N}$: l'ordine in $\mathbf{Q}$ è denso (tra ogni coppia di razionali esiste un altro razionale), mentre l'ordine su $\mathbf{N}$ è discreto. Vediamo però che i due insiemi hanno la stessa cardinalità.

Consideriamo la seguente tabella:

0	1	-1	2	-2	3	-3	4	-4	5	-5
$0/1$	$1/1$	$(-1)/1$	$2/1$	$(-2)/1$	$3/1$	$(-3)/2$	$4/1$	$(-4)/1$	$5/1$	$\dots$
	$1/2$	$(-1)/2$	$2/3$	$(-2)/3$	$3/2$	$(-3)/2$	$4/3$	$(-4)/3$	$5/2$	$\dots$
	$1/3$	$(-1),3$	$2/5$	$(-2)/5$	$3/4$	$(-3)/4$	$4/5$	$(-4)/5$	$5/3$	$\dots$
	$1/4$	$(-1)/4$	$2/7$	$(-2)/7$	$3/5$	$(-3)/5$	$4/7$	$(-4)/7$	$5/4$	$\dots$

La tabella è costruita così: la colonna etichettata con l'intero k contiene tutte le frazioni con numeratore k, avendo cura di non ripetere frazioni equivalenti. Risulta chiaro che la tabella contiene tutti e soli i razionali senza ripetizioni. Possiamo percorrere questa tabella in modo esattamente analogo a quanto fatto per le tabelle precedenti. Stabiliamo così una biiezione tra $\mathbf{Z}$ e $\mathbf{Q}$, concludendo $\#(\mathbf{Z}) = \#(\mathbf{Q})$. Poiché abbiamo già stabilito una biiezione tra $\mathbf{N}$ e $\mathbf{Z}$, possiamo concludere che $\#(\mathbf{N}) = \#(\mathbf{Q})$, ossia che l'insieme dei numeri razionali è numerabile.

Unioni di numerabili Si osserva facilmente che se A è numerabile e B è finito, l'unione $A \cup B$ è numerabile. Posso infatti scrivere $A = \{a_1, a_2, a_3, \dots\}$ e $B = \{b_1, b_2, \dots, b_k\}$ e la loro unione come $A \cup B = \{b_1, b_2, \dots, b_k, a_1, a_2, a_3, \dots\}$ (NB: se A e B non sono disgiunti e voglio una lista senza ripetizioni devo solo badare a nonn ripetere gli elementi di B).

Analogamente se A e B sono numerabili, la loro unione è numerabile. Posso infatti scrivere $A = \{a_1, a_2, a_3, \dots\}$ e $B = \{b_1, b_2, b_3, \dots\}$, e la loro unione $A \cup B$ come $\{a_1, b_1, a_2, b_2, a_3, b_3, \dots\}$; anche in questo caso evitando le ripetizioni.

L'argomento si generalizza ovviamente a unioni di n termini di insiemi $A_1, \dots, A_n$ tutti numerabili.

Esercizio 5 *L'unione di una collezione numerabili di insiemi numerabili è numerabile? Ossia: dati $A_1, A_2, A_3, \ldots$ insiemi numerabili, la loro unione $A = \bigcup_{i \in \mathbf{N}} A_i$ è numerabile? L'unione A è l'insieme che contiene tutti e soli gli elementi che appartengono a qualche A_n.*

A questo punto potremmo sospettare che tutti gli insiemi infiniti sono numerabili.

3 Insiemi non-numerabili

Dimostriamo che esistono insiemi infiniti non-numerabili. Abbiamo visto che l'operazione di prodotto cartesiano e quella di unione non possono portarci dal numerabile al non-numerabile. Occorre pensare a un insieme che non si può ottenere in questi modi. Un'idea naturale è quella di considerare una sorta di prodotto cartesiano infinito

$$\mathbf{N} \times \mathbf{N} \times \mathbf{N} \times \mathbf{N} \ldots$$

che in altre parole è l'insieme delle sequenze *infinite* di naturali. Vediamo che basta considerare un insieme più semplice, ma che ha in comune con questo la caratteristica di non poter essere ottenuto come prodotto cartesiano con un numero finito di fattori.

Sequenze Binarie Infinite Consideriamo l'insieme SBI di tutte le sequenze binarie infinite. Questo insieme è numerabile? Potremmo provare a stabilire una funzione biiettiva tra SBI e $\mathbf{N}$ (è un buon esercizio provarci). Se sospettassimo che non esiste una biiezione conviene ricorrere a un ragionamento per assurdo (dato che dobbiamo escludere che qualunque funzione immaginabile tra $\mathbf{N}$ e SBI sia una biiezione!). Supponiamo dunque che esista una tale biiezione. Allora potremmo ordinare gli elementi di SBI in una tabella come la seguente:

$$\begin{array}{r|ccccccccccc}
s_1 = & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & \ldots \\
s_2 = & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & \ldots \\
s_3 = & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \ldots \\
s_4 = & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & \ldots \\
s_5 = & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots
\end{array}$$

Questa tabella contiene tutte e sole le sequenze binarie infinite (e ciascuna una volta soltanto — ma questo non è essenziale!)

Consideriamo la diagonale NO-SE della tabella.

$s_1 =$	**1**	0	0	1	1	0	1	0	1	1	...
$s_2 =$	0	**0**	1	0	1	0	1	1	1	0	...
$s_3 =$	0	0	**0**	0	0	0	0	0	0	0	...
$s_4 =$	1	0	0	**1**	1	0	1	0	1	1	...
$s_5 =$	0	0	0	0	**1**	0	0	0	1	0	...
...	...	...	...	...	...	...	...	...	...	...	...

La diagonale è una sequenza binaria infinita, nel nostro esempio inizia così:

$$10011\ldots$$

Consideriamo la sequenza s^* ottenuta flippando i bit:

$$01100\ldots$$

Cosa sappiamo di s^*? Sicuramente è una sequenza binaria infinita, dunque $s^* \in SBI$. D'altra parte s^* non coincide con nessuna delle sequenze presenti in tabella: infatti differisce da s_1 per il primo bit, da s_2 per il secondo, da s_3 per il terzo. In generale, per ogni n, s^* differisce da s_n per il bit in posizione n. Da questo concludiamo che la tabella non può esistere! Dunque non esiste una biiezione tra $\mathbf{N}$ e SBI!

Possiamo dunque concludere che

$$\#(\mathbf{N}) \neq \#(SBI).$$

Esistono dunque almeno due insiemi infiniti di cardinalità diverse! In particolare SBI non è infinito numerabile (è ovviamente infinito).

Cosa possiamo dire della relazione tra la cardinalità di $\mathbf{N}$ e quesllaa di SBI? Risulta naturale dire che $\#(\mathbf{N}) \leq \#(SBI)$, perché è facile stabilire una iniezione $f : \mathbf{N} \to SBI$. Per esempio ponendo $f(n) =$ la sequenza con un singolo 1 in posizione n-esima.

In analogia a quanto vale per insiemi finiti poniamo: $\#(A) \leq \#(B)$ se e solo se esiste una iniezione di A in B. In base a questa definizione possiamo dire che $\#(\mathbf{N}) \leq \#(SBI)$.

D'altra parte abbiamo dimostrato sopra che non esiste una biiezione tra i due insiemi. Questo ci indurrebbe a dire che $\#(\mathbf{N}) < \#(SBI)$, intendendo che esiste una inizezione di $\mathbf{N}$ in SBI ma *non esiste* una biiezione di $\mathbf{N}$ in SBI. Vedremo più avanti come rendere precise queste idee. Per il momento ci limitiamo a dire che SBI non è numerabile.

Reali L'argomento visto sopra (detto argomento diagonale di Cantor) è molto flessibile e trova applicazione in molti contesti. Qui ci limitiamo a osservare che permette di stabilire la non-numerabilità di altri insiemi numerici.

Consideriamo l'insieme dei numeri reali, $\mathbf{R}$. Supponiamo che esista una biiezione con $\mathbf{N}$. Esisterebbe allora una tabella come la seguente:

$r_1 =$	5.	7	3	2	0	6	6	6	6	6	...
$r_2 =$	-20.	0	1	2	3	5	8	9	1	4	...
$r_3 =$	154.	3	3	3	5	9	0	2	0	5	...
$r_4 =$	81.	0	2	4	6	6	7	0	3	3	...
$r_5 =$	0.	0	3	3	8	3	3	3	3	3	...
...	...	...	...	...	...	...	...	...	...	...	...

In questa tabella abbiamo scritto i reali come decimali espansi, evitando di inserire le scritture che finiscono con una coda infinita di 9 e scrivendo una coda infinita di 0 per i casi in cui la parte decimale è finita. La tabella contiene così una rappresentazione unica per ogni reale. Se consideriamo come sopra la diagonale NO/SE otteniamo la sequenza

$$5.0348\ldots$$

Modifichiamola così: sostituiamo 5 con 2 (questa scelta è arbitraria). Per la parte decimale procediamo così: se il decimale è 3 lo sostituiamo con 4 e se il decimale è diverso da 3 lo sostituiamo con 3. Otteniamo

$$r^* = 2.343\ldots$$

r^* è un numero reale in forma di espansione decimale, ossia $r^* \in \mathbf{R}$. D'altra parte r^* non coincide con nessun r_n. Dunque la tabella non può esistere, e concludiamo che $\mathbf{N}$ non può essere posto in biiezione con $\mathbf{R}$, ossia che

$$\#(\mathbf{N}) \neq \#(\mathbf{R}).$$

Intervalli reali Consideriamo ora l'intervallo reale $[0, 1)$. Supponendo che esista una biiezione con $\mathbf{N}$, potremmo scrivere una tabella come la seguente:

$$\begin{array}{r|ccccccccccc}
r_1 = & 0. & 7 & 3 & 2 & 0 & 6 & 6 & 6 & 6 & 6 & \ldots \\
r_2 = & 0. & 0 & 1 & 2 & 3 & 5 & 8 & 9 & 1 & 4 & \ldots \\
r_3 = & 0. & 3 & 3 & 3 & 5 & 9 & 0 & 2 & 0 & 5 & \ldots \\
r_4 = & 0. & 0 & 2 & 4 & 6 & 6 & 7 & 0 & 3 & 3 & \ldots \\
r_5 = & 0. & 0 & 3 & 3 & 8 & 3 & 3 & 3 & 3 & 3 & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots
\end{array}$$

In questa tabella avremmo tutti i reali in $[0, 1)$ in forma decimale espansa, evitando di inserire le scritture che finiscono con una coda infinita di 9 e scrivendo una coda infinita di 0 per i casi in cui la parte decimale è finita. Se consideriamo come sopra la diagonale NO/SE otteniamo la sequenza

$$0.0348\ldots$$

e ne modifichiamo la parte decimale come sopra, otteniamo

$$r^* = 0.343\ldots$$

r^* è un numero reale nell'intervallo $[0, 1)$ (esercizio: perché?). D'altra parte r^* non coincide con nessun r_n. Dunque la tabella non può esistere, e concludiamo che $\mathbf{N}$ non può essere posto in biiezione con $[0, 1)$, ossia che

$$\#(\mathbf{N}) \neq \#([0, 1).$$

Esercizio 6 *Possiamo condurre l'argomento di sopra supponendo di avere una suriezione da* $\mathbf{N}$ *su SBI?*

Abbiamo già osservato che un insieme infinito può essere in corrispondenza biiettiva con un suo sottinsieme proprio (per es. $\mathbf{N}$ e i pari). Vediamo che questo accade anche per insiemi infiniti non numerabili.

Consideriamo l'intervallo reale $(0, +\infty)$ e l'intervallo reale $(0, 1)$. Uno è intuitivamente molto più piccolo dell'altro, eppure possiamo stabilire una corrispondenza biunivoca tra i due con un semplice ragionamento geometrico. Consideriamo il punto $p = (-1, 1)$. Per ogni $r \in (0, +\infty)$ tracciamo il segmento che congiunge r e p. Questo interseca l'asse delle Y in un unico punto tra 0 e 1 esclusi; sia questo punto $f(r)$. Abbiamo così stabilito una funzione $f : (0, +\infty) \to (0, 1)$. Questa funzione è una biiezione! Si osservi che i triangoli $(r, f(r), (0, 0)$ e $(r, p, (-1, 1)$ sono simili. Il primo ha cateti di lunghezza r e $f(r)$, il secondo di lunghezza $r + 1$ e 1; così che per similitudine possiamo concludere:

$$\frac{1}{r+1} = \frac{f(r)}{r}.$$

Dunque la forma chiusa di f è $f(r) = \frac{r}{r+1}$ (esercizio: dimostrare che è una biiezione).

Possiamo concludere che

$$\#((0, +\infty)) = \#((0, 1)).$$

Esercizio 7 *Definire una iniezione da* $\mathbf{R}$ *in* $(0, +\infty)$.

Esercizio 8 *Definire una iniezione da* $[0, 1)$ *in* $(0, 1)$ *e una iniezione da* $(0, 1)$ *in* $[0, 1)$.

Abbiamo dimostrato che esiste più di un tipo di cardinalità infinita: quella degli insiemi numerabili, quella dei reali, quella di SBI, quella di $(0, 1)$ etc. Come possiamo confrontarle tra loro? E: ne esistono altre? E se sì, quante?

4 Cardinalità del Continuo

Per quanto visto finora gli insiemi cadono in tre gruppi:

1. Insiemi **finiti**, i.e., in biiezione con qualche $\{1, 2, \dots, n\}$ o vuoti.
2. Insiemi **infiniti numerabili**, i.e., in biiezione con $\mathbf{N}$: $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{N} \times \mathbf{N}$, $\mathbf{N} \times \mathbf{N} \times \mathbf{N}$, etc.
3. Insiemi **infiniti non numerabili**, i.e., non in biiezione con $\mathbf{N}$: $\mathbf{R}$, SBI, $(0, 1)$.

Risulta naturale chiedersi se gli insiemi non numerabili hanno tutti la stessa cardinalità o no. E, se la risposta è no, quali altre cardinalità esistono.

4.1 Insieme potenza di N e SBI

Per un insieme finito A di n elementi abbiamo già osservato una corrispondenza (una traduzione) tra l'insieme delle sequenze binarie di lunghezza n e l'insieme di tutti i sottinsiemi di A. Se $A = \{a_1, \dots, a_k\}$, un sottinsieme S di A, sia $S = \{a_{i_1}, \dots, a_{i_p}\}$ corrisponde alla sequenza binaria che ha un 1 solo nelle posizioni $i_1, \dots, i_p$. Questa traduzione è una biiezione che abbiamo già usato per concludere che il numero di elementi di $\mathcal{P}(A)$ è uguale al numero di sequenze binarie di lunghezza n.

Si può definire una analoga traduzione per i sottinsiemi di $\mathbf{N}$ (e più in generale per insiemi numerabili): a un sottinsieme S di $\mathbf{N}$, sia $S = \{n_1, n_2, \dots, \}$ (o $\{n_1, n_2, \dots, n_k\}$ se è finito) facciamo corrispondere la sequenza binaria infinita che ha un 1 solo nelle posizioni $n_1, n_2, \dots$, ossia nelle posizioni i con $i \in S$. Per esempio, al sottinsieme $\{2, 4, 6, 8 \dots\}$ di $\mathbf{N}$ contenente tutti e soli i numeri pari facciamo corrispondere la sequenza $01010101\dots$ (NB stiamo cominciando a contare da 1 non da 0). La sequenza binaria infinita associata in questo modo a un sottinsieme viene detta la sua *sequenza caratteristica*.

Questa traduzione, come si vede facilmente, è una biiezione tra $\mathcal{P}$ e SBI. Abbiamo dunque che

$$\#(SBI) = \#(\mathcal{P}(\mathbf{N})).$$

4.2 Teorema di Cantor-Bernstein-Schroder

Stabilire che due insiemi hanno la stessa cardinalità richiede di definire una biiezione. In molti casi questo risulta piuttosto complicato. Vediamo come semplificare il compito.

Per gli **insiemi finiti** vale la seguente proprietà: se A e B sono finiti, e

- Esiste una iniezione $f : A \to B$, e
- Esiste una iniezione $g : B \to A$,

allora A e B hanno lo stesso numero di elementi. Questo risulta evidente dalle considerazioni intuitive che abbiamo fatto all'inizio della nostra trattazione sulle cardinalità:

- Se esiste una iniezione $f : A \to B$ allora A ha al più tanti elementi quanti B.
- Se esiste una iniezione $g : B \to A$ allora B ha al più tanti elementi quanti A.

Risulta naturale chiedersi se queste osservazioni valgono anche per insiemi arbitrari. La risposta è sì, come enunciato nel seguente Teorema di Cantor-Bernstein-Schroder. La dimostrazione va oltre gli obiettivi di questo corso.

Teorema 1 (Cantor-Bernstein-Schroder) *Siano A e B insiemi arbitrari. Se esiste una iniezione $f : A \to B$ ed esiste una iniezione $g : B \to A$ allora esiste una biiezione $h : A \to B$.*

Il Teorema CBS, preso come *black-box*, è un utile strumento per dimostrare l'equicardinalità tra due insiemi A e B: il compito di produrre una biiezione tra A e B è ridotto al compito, spesso molto più semplice, di produrre una iniezioni di A in B e una iniezione di B in A.

4.3 Insiemi equipotenti a R

Stabiliamo l'equicardinalità di tutti gli insiemi non-numerabili introdotti finora, usando il Teorema CBS. Sappiamo già che $\#(0, 1) = \#(0, +\infty)$.

Esempio 1 *Dimostriamo che $(0, +\infty)$ è in biiezione con $\mathbf{R}$ usando il Teorema CBS. Dato che $(0, +\infty) \subseteq \mathbf{R}$, l'identità è una iniezione di $(0, +\infty)$ in $\mathbf{R}$. D'altra parte, la funzione $r \mapsto r^2$ è una iniezione di $\mathbf{R}$ in $(0, +\infty)$. Dunque, per il Teorema CBS, $\#\mathbf{R} = \#(0, +\infty)$.*

Esercizio 9 *Dimostrare che $(0, 1)$ è in biiezione con $[0, 1)$ usando il Teorema CBS: definire una iniezione $f : [0, 1) \to (0, 1)$. Una iniezione da $(0, 1)$ in $[0, 1)$ è data dall'identità, dato che $(0, 1) \subseteq [0, 1)$.*

Abbiamo dunque:
$$\#\mathbf{R} = \#(0, +\infty) = \#(0, 1) = \#[0, 1).$$
Mancano all'appello SBI e $\mathcal{P}(\mathbf{N})$.

Proposizione 1 *La cardinalità di $\mathbf{R}$ è uguale a quella di $\mathcal{P}(\mathbf{N})$.*

Dimostrazione Usiamo il fatto che $\mathbf{R}$ è in biiezione con $[0, 1)$. Per questo esempio consideriamo $\mathbf{N} = \{0, 1, 2, \dots\}$.

Definiamo la seguente funzione f da $[0, 1)$ in $\mathcal{P}(\mathbf{N})$: Sia $r \in [0, 1)$. Consideriamo la sua espansione decimale (trascurando sempre quella con coda infinita di 9):
$$r = 0.d_1 d_2 d_3 d_4 \dots$$
dove ogni d_i è una cifra tra 0 e 9. Associamo a r il sottinsieme $f(r)$ di $\mathbf{N}$ definito come segue:
$$\{10 \times d_1, 10^2 \times d_2, 10^2 \times d_3, \dots\}.$$
In breve: $f(r)$ contiene $10^i d_i$ per ogni d_i nell'espansione decimale di r.

Si dimostra facilmente che f è una iniezione (Esercizio).

Definiamo la seguente funzione g da $\mathcal{P}(\mathbf{N})$ in $[0, 1)$. Dato un sottinsieme $S = \{n_1, n_2, n_3, \dots\}$ di $\mathbf{N}$ consideriamo la stringa binaria infinita σ che ha un 1 in tutte e sole le posizioni n_i con $n_i \in S$ (la *stringa caratteristica* di S). Associamo a S il seguente numero reale $g(S)$:
$$0.\sigma$$
Si dimostra facilmente che g è una iniezione (Esercizio).

Per il Teorema CBS possiamo concludere che $\#(\mathbf{R}) = \#(\mathcal{P}(\mathbf{N}))$.

Q.E.D.

Dato che SBI è in biiezione con $\mathcal{P}(\mathbf{N}$, abbiamo che tutti gli esempi visti di cardinalità non numerabili sono equivalenti a $\mathbf{R}$:

$$\#(\mathbf{R}) = \#(\mathcal{P}(\mathbf{N})) = \#(0,1) = \#[0,1) = \#SBI = \#(0,+\infty).$$

Diamo un nome a questa "classe", dato che racchiude molti esempi interessanti:

Definizione 2 (Cardinalità del Continuo) *Un insieme ha la cardinalità del continuo se è in biiezione con* $\mathbf{R}$.

4.4 Confronto tra cardinalità

Il Teorema CBS ci assicura di poter definire un ordine sensato tra le cardinalità, generalizzando le proprietà che valgono nel finito. Poniamo la seguente definizione:

Definizione 3 *Diciamo che A ha al più tanti elementi quanto B, o che la cardinalità di A è al più quella di B, se e solo se esiste una iniezione $f : A \to B$. In tal caso scriviamo $\#(A) \leq \#(B)$.*

Con questa nuova notazione il Teorema CBS si traduce così:

$$\text{Se } \#(A) \leq \#(B) \text{ e } \#(B) \leq \#(A) \text{ allora } \#(A) = \#(B).$$

Possiamo anche definire sensatamente una versione stretta della relazione d'ordine tra cardinalità appena definita:

Definizione 4 *Diciamo che A ha (strettamente) meno elementi di B, o che la cardinalità di A è (strettamente) minore di quella di B se e solo se esiste una iniezione $f : A \to B$ ma non esiste una iniiezione $g : B \to A$. In tal caso scriviamo $\#(A) < \#(B)$.*

In simboli la definizione precedente si può scrivere così: $\#(A) < \#(B)$ se e solo se $\#(A) \leq \#(B)$ ma $\#(B) \not\leq \#(A)$.

La relazione $\#(A) < \#(B)$ si può anche definire in modo equivalente ponendo: esiste una iniezione $f : A \to B$ ma non esiste una suriezione $g : A \to B$.

5 Altre cardinalità?

Per quanto visto finora gli insiemi hanno cardinalità di tre tipi:

Finiti	Numerabili	Continui
$\emptyset, \{2,3,5\}, \{1,2,\ldots,2^{100}\}, \ldots$	$\mathbf{N}, \mathbf{Z}, \mathbf{Q}, \mathbf{N}\times\mathbf{N}, \ldots$	$\mathbf{R}, SBI, \mathcal{P}(\mathbf{N}), (0,1), [0,1), (0,+\infty)$

Risulta naturale chiedersi se esistono altri tipi di cardinalità. A priori, potrebbero situarsi in tre posizioni:

1. Tra i finiti e i numerabili,
2. Tra i numerabili e i continui,
3. Oltre i continui.

Ci si convince abbastanza facilmente che non possono esistere insiemi A di cardinalità non finita ma strettamente inferiore a quella di $\mathbf{N}$. Si tratterebbe di un insieme che non è in biiezione con nessun insieme del tipo $\emptyset$ o $\{1,2,\ldots,n\}$, si può iniettare in $\mathbf{N}$, ma tale che $\mathbf{N}$ non può iniettarsi in esso.

Restano a priori due possibilità: cardinalità oltre quella del continuo e cardinalità intermedie tra $\#(\mathbf{N})$ e $\#(\mathbf{R})$.

5.1 Oltre il continuo

Per tentare di trovare insiemi di cardinalità strettamente maggiore di quella di $\mathbf{R}$ possiamo provare a individuare delle operazioni che facciano crescere la cardinalità. Si osserva abbastanza facilmente che le operazioni di prodotto cartesiano e unione, come accade per il numerabile, non ci fanno uscire dalla cardinalità del continuo: per es., $\mathbf{R} \times \mathbf{R}$ (coppie ordinate di reali) ha la cardinalità di $\mathbf{R}$, e così tutti i prodotti cartesiani finiti (e anche qualcosa di più); analogamente le unioni di insiemi continui rimangono continue.

Una operazione che ha dato luogo a un significativo salto di qualità è quella che porta da un insieme A al suo insieme potenza $\mathcal{P}(A)$.

Se A è finito, sappiamo $\#(A) = 2^{\#(A)}$.

Se A è $\mathbf{N}$ (ma più in generale se A è numerabile), abbiamo visto che $\#(A) < \#(\mathcal{P}(A)$, e il salto è significativo: mentre $\mathbf{N}$ è numerabile, abbiamo dimostrato che $\mathcal{P}(\mathbf{N})$ è continuo.

Che succede se considero $\mathcal{P}(\mathbf{R})$, o $\mathcal{P}(\mathcal{P}(\mathbf{N}))$, o $\mathcal{P}([0,1))$? In generale, che cardinalità ha l'insieme potenza di un insieme continuo?

Il seguente Teorema, dovuto a Georg Cantor, è una pietra miliare della Teoria degli Insiemi: dimostra che la cardinalità dell'insieme potenza è *sempre* strettamente maggiore di quella dell'insieme di partenza. L'argomento è sorprendente.

Teorema 2 (Cantor) *Sia A un insieme qualunque. Non esiste una biiezione tra A e $\mathcal{P}(A)$.*

Dimostrazione Dimostriamo che non esiste una suriezione da A su $\mathcal{P}(A)$. Ragioniamo per assurdo. Sia dunque $f : A \to \mathcal{P}(A)$ una suriezione. La funzione f manda elementi di A in sottinsiemi di A. In generale, dato un elemento a di A e un sottinsieme S di A, ha senso chiedersi se $a \in S$ oppure no. Questa domanda ha senso anche per un arbitrario elemento a di A e la sua immagine $f(a)$ tramite f. Distinguiamo dunque in due tipi gli elementi di A:

Tipo 1 Elementi $a \in A$ tali che $a \in f(a)$.

Tipo 2 Elementi $a \in A$ tali che $a \notin f(a)$.

Consideriamo ora l'insieme di tutti e soli gli elementi $a \in A$ del secondo tipo, ossia

$$X = \{a \in A \, : \, a \notin f(a)\}.$$

X è un sottinsieme di A, ossia $X \in \mathcal{P}(A)$. Dato che f per ipotesi è suriettiva, deve esiste un elemento $x \in A$ tale che $f(x) = X$. Fissiamo un tale x.

Chiediamoci ora di che tipo è questo x.

Se x è di tipo 1, allora $x \in f(x)$. Dato che $f(x) = X$ abbiamo $x \in X$. Ma per definizione di X, questo implica che $x \notin f(x)$. Abbiamo dunque che: se $x \in f(x)$ allora $x \notin f(x)$. Questo è impossibile dunque x non è di tipo 1.

Se x è di tipo 2, allora $x \notin f(x)$, ossia $x \notin X$. Per definizione di X questo implica che $x \notin f(x)$ è falso, dunque $x \in f(x)$. Abbiamo dunque che: se $x \notin f(x)$ allora $x \in f(x)$.

Unendo le due parti del ragionamento abbiamo che $x \in f(x)$ se e solo se $x \notin f(x)$, il che è ovviamente contraddittorio. Dunque la nostra ipotesi per assurdo è falsa: non esiste una suriezione f da A su $\mathcal{P}(A)$.

Q.E.D.

Osservazione 1 *L'idea della dimostrazione del Teorema di Cantor è molto simile all'idea del Paradosso del Barbiere di Bertrand Russell. In un villaggio esistono persone che si fanno la barba da sole e persone che non si fanno la barba da sole. Il barbiere del villaggio fa la barba a tutte e sole le persone che non si fanno la barba da sole. Chiedersi: Il barbiere del villaggio si fa la barba da solo? dà luogo a un paradosso. Questa idea, per quanto semplice, ha una importanza storica di rilievo: con un esempio simile Russell diede il colpo di grazia a una teoria sviluppata dal logico Gottlob Frege per formalizzare rigorosamente tutta la Matematica. Mostrando che in questa teoria si può definire un analogo del Paradosso del Barbiere (per la precisione: l'insieme di tutti gli insiemi che non contengono sé stessi) Russell dimostrò che il sistema di Frege era incoerente. (La vicenda è raccontata in modo interessante nel fumetto LogiComix, An Epic Search for Truth, di da Apostolos Doxiadis e Christos Papadimitriou).*

Dal Teorema di sopra segue facilmente che *per ogni insieme A*, vale

$$\#(A) < \#(\mathcal{P}(A)).$$

Per definizione questa diseguaglianza significa che:

1. esiste una iniezione da A in $\mathcal{P}(A)$, ma
2. non esiste una suriezione da A su $\mathcal{P}(A)$ (o, equivalentemente, non esiste una iniezione da $\mathcal{P}(A)$ in A).

Il secondo punto è proprio quello che abbiamo dimostrato nel Teorema. Per il primo punto: si vede facilmente che la seguente mappa è una iniezione da A in $\mathcal{P}(A)$: basta associare a un elemento $a \in A$ il sottinsieme $\{a\}$.

Iterando il Teorema, a partire da $A = \mathbb{N}$, abbiamo una successione infinita di cardinalità infinite l'una strettamente maggiore della precedente:

$$\#(\mathbb{N}) < \#(\mathcal{P}(\mathbb{N})) < \#(\mathcal{P}(\mathcal{P}(\mathbb{N}))) < \#(\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))) < \dots$$

In altre parole, esistono infiniti numeri infiniti (detti *numeri transfiniti*).

5.2 Tra numerabile e continuo?

Il passaggio da A a $\mathcal{P}(A)$ fa sempre crescere la cardinalità. Nel caso di $\mathbf{N}$, sappiamo già che $\mathcal{P}(\mathbf{N})$ ha cardinalità di $\mathbf{R}$ (e in generale che l'insieme potenza di un numerabile ha la cardinalità del continuo). Resta da capire se possono esistere cardinalità intermedie tra $\#(\mathbf{N})$ e $\#(\mathbf{R})$ ossia tra numerabile e continuo. Queste non si possono ottenere come insieme potenza, ma potrebbe darsi che esistano sottinsiemi A di $\mathbf{R}$ per cui valga:

$$\#\mathbf{N} < \#A < \#\mathbf{R}.$$

Cantor credeva di no, e formulò verso la fine dell'Ottocento (1878) la seguente ipotesi:

Ipotesi del Continuo Non esistono insiemi di cardinalità strettamente maggiore di $\#(\mathbf{N})$ e strettamente minore di $\#(\mathbf{R})$.

Per Cantor dunque, numerabile e continuo sono i primi due ordini di infinito e nulla esiste tra loro.

L'Ipotesi del Continuo è a tutt'oggi, in un certo senso, irrisolta. Ha però uno statuto estremamente speciale: lo sviluppo della Logica Matematica moderna ha permesso di dimostrare che, in un senso molto preciso, non possiamo dimostrare l'Ipotesi del Continuo né dimostrare che è falsa. Questo significa che usando gli assiomi universalmente riconosciuti come sufficienti a formalizzare tutti i procedimenti matematici noti, è dimostrabilmente impossibile sia ottenere una dimostrazione dell'Ipotesi del Continuo sia una dimostrazione della sua negazione. Si dice che l'Ipotesi del Continuo è *indecidibile*.

In altre parole: relativamente agli assiomi normalmente usati per formalizzare più o meno l'intera Matematica:

1. È coerente che non esistano cardinalità intermedie tra $\#\mathbf{N}$ e $\#\mathbf{R}$ (questo fu dimostrato da Kurt Gödel nel 1940); ma

2. È anche coerente che ne esistano (questo fu dimostrato da Paul Cohen nel 1963)!

Un aspetto molto interessante della questione è che *possiamo dimostrare* in modo assolutamente rigoroso *che non possiamo dimostrare* né l'Ipotesi del Continuo né la sua negazione. Diciamo che "sappiamo di non sapere" e "sappiamo di non poter sapere".