Appunti per il TFA

E. Paolini

24 giugno 2013

1 Contare

1.1 Insiemi finiti

Definizione 1.1 (insieme finito)**.** *Se un insieme A può essere posto in biezione con l'insieme*

$$I_n = \{1, \dots, n\}$$

di numeri naturali, diremo che A è un insieme finito *e denoteremo con $|A| = n$ il* numero di elementi *di A.*

La biezione $I_n \to A$ rappresenta il procedimento del *contare*.

Osservazione 1.2. Osserviamo che spesso nella costruzione dei numeri naturali si pone $0 = \emptyset = \{\}$, $n + 1 = n \cup \{n\}$ da cui si ricava $n = \{0, \dots, n-1\}$. Con questa (strana?) notazione $|A| = n$ se esiste $f\colon n \to A$ biettiva.

Esempio 1.3. *L'insieme $A = \{a, b, c\}$ ha tre elementi, cioe $|A| = 3$ in quanto $f\colon I_3 \to A$ definita da:*

$$1 \mapsto a, \qquad 2 \mapsto b, \qquad 3 \mapsto c$$

è una biezione.

Vedremo ora che se l'insieme di cui vogliamo conoscere il numero di elementi ha una qualche particolare struttura, è spesso possibile *calcolare* il numero di elementi dell'insieme senza dover presentarne esplicitamente una enumerazione. Nel seguito supporremo sempre che gli insiemi considerati siano finiti.

1.1.1 Insieme prodotto e parole

Se A e B sono insiemi finiti si ha:

$$|A \times B| = |A| \cdot |B|.$$

Infatti se $f\colon I_n \to A$ con $n = |A|$ e $g\colon I_m \to B$ con $m = |B|$ si può definire $h\colon I_{nm} \to A \times B$

$$h((k-1)m + j) = (f(k), g(j))$$

osservando che ogni numero p in I_{mn} può essere scritto in modo univoco nella forma $(k-1)m + j$ con $k \in I_n$ e $j \in I_m$ (basti prendere per k e j il quoziente e il resto della divisione di p per m).

In particolare si avrà

$$|A^m| = |A|^m$$

dove A^m è l'insieme delle m-uple ordinate di elementi di A. L'insieme A^m rappresenta anche le parole formate da m lettere scelte dall'insieme A.

Esempio 1.4. *Il numero di parole formate da 3 vocali è* $5^3 = 125$. *Ad esempio la parola aia può essere rappresentata dalla tripletta* (a, i, a) *che è un elemento dell'insieme* A^3 *dove* $A = \{a, e, i, o, u\}$.

Esempio 1.5. *Qual è la probabilità di indovinare il PIN di un bancomat con 3 tentativi? Il PIN è formato da* 5 *cifre decimali e quindi è un numero compreso tra* 0 *e* 99999. *I possibili PIN sono quindi* $100000 = 10^5$. *Scegliendone a caso 3 diversi ho 3 possibilità su 100000 di indovinare.*

Modellizzare l'insieme A^n con le parole di n lettere scelte da un insieme A formato da m simboli ci permette anche di comprendere la formula $|A^n| = m^n$. Infatti la prima lettera di una parola può essere scelta in m modi diversi, la seconda lettera anch'essa in m modi diversi e così via fino all'm-esima lettera. Moltiplicando tra loro ogni possibilità otteniamo m^n.

Un'altra possibile interpretazione degli elementi dell'insieme A^m sono le estrazioni di m palline da un'*urna* A.

Esempio 1.6. *Una urna contiene una pallina verde* v, *una pallina rossa* r *e una pallina gialla* g. *Rappresentiamo l'urna con l'insieme* $A = \{v, r, g\}$. *Se estraiamo due palline con* reimbussolamento *(cioè dopo aver estratto la prima pallina la rimettiamo nell'urna), la probabilità di ottenere due volte la pallina gialla è* 1 *sul numero di possibili estrazioni (tutte equiprobabili). Cioè* $1/|A^2| = 1/9$.

Esempio 1.7. *Quanti sono i* files *da* 1 *Mbyte? Un file può essere rappresentato come una sequenza di bytes. L'insieme dei bytes ha* 2^8 *elementi. Quindi l'insieme dei* files *da* 1 *Mbytes (*$1M = 2^{20}$ *bytes) ha* $(2^8)^{(2^{20})} = 2^{(2^{23})}$ *elementi.*

Osserviamo ora che se B è un qualunque insieme si può fare l'identificazione

$$A^B = \{f \colon B \to A\} \approx A^{|B|}$$

e quindi abbiamo una formula per contare tutte le funzioni $B \to A$:

$$|A^B| = |A|^{|B|}.$$

In particolare osserviamo che $A^\emptyset = \{\emptyset\}$ in quanto la funzione vuota (cioè la funzione con grafico l'insieme vuoto) è effettivamente una funzione $\emptyset \to A$ ed è l'unica possibile. Dunque

$$|A^\emptyset| = |\{\emptyset\}| = 1.$$

Questo permette di giustificare e dare significato alla formula $0^0 = 1$. Osserviamo invece che $\emptyset^B = \emptyset$ se $B \neq \emptyset$ in quanto una funzione $B \to \emptyset$ non può essere definita in alcun modo. E infatti $0^m = 0$ se $m > 0$.

1.1.2 Parole senza ripetizioni

Sia $\mathrm{Inj}(B, A)$ l'insieme delle funzioni *iniettive* da B ad A. Quanti elementi ha tale insieme?

Se $|A| = n$ e $|B| = k$ osserviamo che una funzione iniettiva $B \to A$ corrisponde ad una parola formata da k simboli scelti in A senza ripetizione. Per scegliere il primo simbolo abbiamo $|A| = n$ possibilità, per scegliere la seconda lettera abbiamo $n - 1$ diverse possibilità (dovendo escludere la prima lettera già scelta) per il terzo simbolo $n - 2$ e così via fino al k-esimo simbolo che può essere scelto in $n - k + 1$ modi diversi. Le parole formate da simboli distinti si chiamano *disposizioni* e il loro numero totale è quindi dato da:

$$D_{n,k} = |\mathrm{Inj}(B, A)| = n(n-1)\dots(n-k+1) = \frac{n!}{(n-k)!}.$$

Le disposizioni corrispondono alle estrazioni da una urna *senza* reimbussolamento.

Esempio 1.8. *Qual è la probabilità di fare cinquina al lotto?*

Al lotto vengono estratti 5 numeri da una urna con 90 numeri, senza reimbussolamento. Dunque la probabilità richiesta è

$$1/C_{90,5} = \frac{1}{90 \cdot 89 \cdot 88 \cdot 87 \cdot 86} = \frac{1}{5273912160}$$

L'esempio precedente ci fa capire che nel calcolare $C_{90,5}$ non conviene usare la formula $90!/85!$ che ci porterebbe a fare una divisione tra numeri enormi.

Una banale osservazione ci permette di asserire che se $k > n$ non è possibile trovare alcuna funzione iniettiva dall'insieme B con k elementi all'insieme A che ha $n < k$ elementi. In effetti nel conteggio fatto precedentemente $n(n-1)(n-2)\dots$ si arriverebbe fino a zero, annullando l'intero prodotto: $D_{n,k} = 0$ se $k > n$.

Teorema 1.9 (principio dei cassetti)**.** *Sia $|B| > |A|$ e sia $f\colon B \to A$ una funzione. Allora esistono $x, y \in B$ con $x \neq y$ tali che $f(x) = f(y)$.*

Dimostrazione. Se così non fosse la funzione f dovrebbe essere iniettiva... ma l'insieme delle funzioni iniettive $B \to A$ è vuoto in quanto $|B| > |A|$. □

Esempio 1.10. *A Roma ci sono due persone con lo stesso numero di capelli. Per dimostrarlo basta stimare che il numero massimo di capelli che può avere una persona è inferiore al numero di abitanti di Roma.*

Esempio 1.11. *In un cassetto ci sono 15 calze blu e 12 calze rosse. Quante calze devo scegliere (al buio) per avere la sicurezza di avere due calze dello stesso colore? Basta prendere 3 calze, la funzioe che associa ad ogni calza il suo colore non può essere iniettiva.*

Esempio 1.12. *Qual è la probabilità che in una classe di 20 studenti ci siano due studenti che compiono gli anni lo stesso giorno? Tale probabilità è complementare alla probabilità che la funzione che associa ad ogni studente il suo compleanno sia iniettiva. Se A è l'insieme degli studenti e B è l'insieme dei giorni dell'anno si ha dunque*

$$p = 1 - \frac{|\mathrm{Inj}(A,B)|}{|B^A|} = 1 - \frac{C_{365,20}}{365^{20}} = 1 - \frac{365}{365}\frac{364}{365}\dots\frac{346}{365} \approx 59\%.$$

1.1.3 Divagazione: approssimabilità dei numeri irrazionali

In questa sezione presentiamo un problema non banale che può essere risolto tramite il principio dei cassetti. Tale principio, per quanto banale, può infatti risultare molto potente in quanto ci permette di dimostrare l'esistenza di una soluzione al problema $f(x) = f(y)$ senza dover esibire esplicitamente la soluzione.

Definizione 1.13. *Diremo che il numero $x \in \mathbb{R}$ è approssimabile di grado α se esiste C ed esistono $p_k, q_k \in \mathbb{Z}$ tali che $q_k \to \infty$ e*

$$0 \neq |x - \frac{p_k}{q_k}| \leq \frac{C}{q_k^\alpha} \qquad \text{per ogni } k \in \mathbb{N}$$

Teorema 1.14. *Sia $x \in \mathbb{R}$. Allora x è approssimabile (almeno) di grado $\alpha = 1$.*

Dimostrazione. Scegliamo $q_k = k$ e $p_k = \lfloor xq_k \rfloor$. Si ha dunque $0 \leq xq_k - p_k < 1$ e di conseguenza:

$$|x - \frac{p_k}{q_k}| \leq \frac{1}{q_k}$$

□

Teorema 1.15. *Dato $x \in \mathbb{R} \setminus \mathbb{Q}$. Allora x è approssimabile di grado $\alpha = 2$.*

Dimostrazione. Scelto $N > 0$ si consideri l'insieme di $N+1$ elementi: $A = \{0, 1, \dots, N\}$ e sia $f\colon A \to [0, 1)$ definita da

$$f(k) = kx - \lfloor kx \rfloor.$$

Dividendo l'intervallo $[0, 1)$ in N parti: $[0, 1/N) \cup [1/N, 2/N) \dots [(N-1)/N, 1)$ per il principio dei cassetti esistono due indici diversi k, j tali che $f(k)$ e $f(j)$ appartengono allo stesso intervallino e quindi:

$$|f(k) - f(j)| = |kx - \lfloor kx \rfloor - (jx - \lfloor jx \rfloor)| < 1/N.$$

Posto $q_N = k - j$ e $p_N = \lfloor kx \rfloor - \lfloor jx \rfloor$ si ha dunque

$$|q_N x - p_N| < 1/N.$$

Siccome x è irrazionale si ha $q_N \neq 0$. Inoltre essendo $k, j \leq N$ si ha anche $q_N < N$. Dunque

$$|x - \frac{p_N}{q_N}| < \frac{1}{q_N N} < \frac{1}{N^2}.$$

Per ogni N abbiamo dunque trovato la frazione che approssima x all'ordine $\alpha = 2$. Si osservi che necessariamente, a meno di sottosuccesioni, $q_N \to \infty$ perché $p_N/q_N \to x$ e x non è razionale. □

Il teorema precedente può essere applicato per dimostrare che la successione $a_n = \sin n$ ammette sottosuccessioni convergenti a qualunque numero compreso nell'intervallo $[-1, 1]$. Per fare questo si sfrutta l'approssimabilità di π all'ordine $\alpha = 2$.

1.1.4 Permutazioni

Osserviamo che se A è finito e $f\colon A \to A$ richiedere che f sia iniettiva è equivalente a chiedere che f sia suriettiva:

$$\{f\colon A \to A \quad f \text{ iniettiva}\} = \{f\colon A \to A \quad f \text{ suriettiva}\} = \{f\colon A \to A \quad f \text{ biettiva}\}$$

Tali funzioni si chiamano *permutazioni* e l'insieme precedente può essere denotato con $S(A)$ (gruppo simmetrico). Per quanto visto prima se $|A| = n$

$$|S(A)| = D_{n,n} = n!$$

Esempio 1.16. *Non esiste un algoritmo di* zip *che comprime ogni* file*. Infatti se denotiamo con F_n l'insieme dei* files *di dimensione non superiore a n una funzione $z\colon F_n \to F_{n-1}$ non potrebbe essere iniettiva in quanto $|F_{n-1}| < |F_n|$ (le funzioni di* zip *devono essere iniettive se vogliamo poterle invertire per* decomprimere *i files).*

Si può dimostrare anche un risultato leggermente più forte e cioè che se la funzione di zip *comprime almeno un file, allora c'è almeno un altro file che viene allungato. Supponiamo infatti che esista f_0 tale che $z_0 \notin F_n$ ma $z(f_0) \in F_n$. Se fosse $z(F_n) \subseteq F_n$ si avrebbe anche $z(F_n) \subseteq F_n \setminus \{z(f_0)\}$ in quanto per l'iniettività di z non può esistere una funzione $f_1 \in F_n$ tale che $z(f_1) = z(f_0)$. Ma essendo $|z(F_n)| > |z(F_n) \setminus \{z(f_0)\}|$ otteniamo un assurdo.*

Esempio 1.17. *Quanti sono gli anagrammi della parola TIGRE? Risposta:* $5! = 120$*. Si supponga di mettere in ordine alfabetico tutti gli anagrammi della parola TIGRE. Qual è la prima parola dell'elenco? Qual è l'ultima? Quali sono le parole precedente e seguente la parola TIGRE?*

Esempio 1.18. *In quanti modi si può mescolare un mazzo di carte da briscola? Risposta:* 40! *Dimostrare che per essere sicuri che il mazzo sia completamente mescolato occorrono almeno 6* smazzate*. Suggerimento: dimostrare che servono almeno 6 smazzate per invertire l'ordine delle carte nel mazzo.*

1.1.5 Sottoinsiemi

L'insieme di tutti i sottoinsiemi di A si chiama *insieme delle parti* e si indica con:

$$\mathcal{P}(A) = \{X : X \subseteq A\}.$$

Osserviamo che $\mathcal{P}(A)$ può essere messo in corrispondenza con $\{0,1\}^A$ identificando un insieme X con la sua funzione caratteristica:

$$f_X(x) = \begin{cases} 1 & \text{se } x \in X \\ 0 & \text{se } x \notin X. \end{cases}$$

Dunque

$$|\mathcal{P}(A)| = |\{0,1\}^A| = 2^{|A|}$$

Esercizio 1.19. Elencare gli otto elementi dell'insieme delle parti di $A = \{a, b, c\}$.

La famiglia dei sottoinsiemi di k elementi di un insieme A di n elementi può essere assimilato alle *combinazioni* $C_{n,k}$ di k simboli scelti tra n. Le combinazioni sono disposizioni *non ordinate* ovvero possono essere assimilate alle funzioni iniettive $B \to A$ con $|B| = k$ modulo permutazioni dell'insieme di partenza. Queste considerazioni ci dicono che

$$C_{n,k} = \frac{D_{n,k}}{k!} = \frac{n!}{k!(n-k)!} = \binom{n}{k}.$$

Il legame con i coefficienti binomiali è pure interessante. Quando andiamo a sviluppare il binomio:

$$(a+b)^n = (a+b)\cdots(a+b)$$

otteniamo tutte le parole di n lettere scelte nell'insieme $\{a, b\}$. Per la commutatività del prodotto le parole che sono *anagrammi* possono essere sommate tra loro ottenendo una somma di termini del tipo $a^k b^{n-k}$ con opportuni coefficienti. I coefficienti corrispondono al numero di anagrammi della parola. Visto che abbiamo solo due simboli ogni anagramma della parola $a^k b^{n-k}$ può essere messo in corrispondenza con il sottoinsieme delle n posizioni in cui si trova il simbolo a, cioè con i sottoinsiemi di k elementi di un insieme di n elementi. Da questo otteniamo la formula:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Ponendo $a = b = 1$ si ottiene

$$2^n = \sum_{k=0}^{n} \binom{n}{k}$$

che semplicemente è una conferma del fatto che il numero totale di sottoinsiemi di un insieme di n elementi è uguale alla somma del numero di sottoinsiemi con k elementi al variare di k.

L'altra regola importante per la costruzione del ben noto *triangolo di Tartaglia* è la proprietà

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1} \tag{1}$$

dove usiamo la (naturale) convenzione

$$\binom{n}{k} = 0 \qquad \text{se } k < 0 \text{ o } k > n.$$

La dimostrazione della proprietà (1) può essere ottenuta facilmente per induzione osservando che:

$$\begin{aligned}(a+b)^{n+1} &= (a+b)(a+b)^n = (a+b)\sum_k \binom{n}{k} a^k b^{n-k} \\ &= \sum_k \binom{n}{k} a^{k+1} b^{n-k} + \sum_k \binom{n}{k} a^k b^{n-k+1} \\ &= \sum_k \binom{n}{k-1} a^k b^{n-k+1} + \sum_k \binom{n}{k} a^k b^{n-k+1} \\ &= \sum_k \left(\binom{n}{k-1} + \binom{n}{k} \right) a^k b^{n+1-k}.\end{aligned}$$

La proprietà (1), insieme alla assunzione $\binom{n}{k} = 0$ per $k < 0$ ci permette di determinare, formalmente, quali dovrebbero essere i valori di $\binom{n}{k}$ con n negativo. Infatti per $n = 0$ si ha

$$\binom{0}{0} = 1, \qquad \binom{0}{k} = 0 \text{ per } k \neq 0.$$

Quindi si dovrebbe avere

$$\binom{-1}{-1} + \binom{-1}{0} = \binom{0}{0} = 1$$

da cui $\binom{-1}{0} = 1$. Sempre applicando (1) si ottiene quindi

$$\binom{-1}{k} = (-1)^k$$

in quanto la somma di due termini consecutivi, per $k > 0$ deve essere nulla.

Analogamente si può determinare $\binom{n}{k}$ per ogni $n \in \mathbb{Z}$. Questa definizione puramente formale ha in realtà significato rispetto alla potenza del binomio. Infatti osserviamo che per $|x| < 1$ si ha (nella seconda uguaglianza usiamo la regola per la somma della serie geometrica)

$$(1+x)^{-1} = \frac{1}{1+x} = \sum_{k=0}^{\infty} (-x)^k = \sum_k \binom{-1}{k} x^k.$$

Regola analoga si può trovare per ogni esponente $\alpha \in \mathbb{R}$ utilizzando gli sviluppi di Taylor. Se $|x| < 1$ si ottiene infatti

$$f(x) = (1+x)^\alpha = \sum_{k=0}^{\infty} \frac{f^{(k)}(0)}{k!} x^k.$$

Calcolando le derivate successive di $f(x)$ si osserva che

$$\begin{gathered} f = (1+x)^\alpha, \qquad f' = \alpha(1+x)^{\alpha-1}, \qquad f'' = \alpha(\alpha-1)(1+x)^{\alpha-2} \dots \\ f(0) = 1, \qquad f'(0) = \alpha, \qquad f''(0) = \alpha(\alpha-1)\dots \end{gathered}$$

da cui ha senso definire

$$\binom{\alpha}{k} = \frac{\alpha(\alpha-1)\dots(\alpha-k+1)}{k!}$$

cosicché vale ancora la formula:

$$(1+x)^\alpha = \sum_{k\geq 0} \binom{\alpha}{k} x^k$$

se $|x| < 1$ e qualunque sia l'esponente $\alpha \in \mathbb{R}$. Ovviamente la formula si può applicare al binomio:

$$(a+b)^\alpha = b^\alpha (1+a/b)^\alpha = b^\alpha \sum_k \binom{\alpha}{k} \frac{a^k}{b^k} = \sum_k \binom{\alpha}{k} a^k b^{\alpha-k}$$

che risulta valida se $|a/b| < 1$ (in caso contrario si può raccogliere a^α).

1.1.6 Partizioni di n

Ci poniamo il problema di determinare in quanti modi il numero n può essere ottenuto come somma di k addendi (numeri naturali). Ad esempio per $n = 5$, $k = 3$ si ha:

$$\begin{aligned}
1+1+3&=5\\
1+2+2&=5\\
1+3+1&=5\\
2+1+2&=5\\
2+2+1&=5\\
3+1+1&=5
\end{aligned}$$

per un totale di 6 possibilità.

Il problema risulta più semplice se si ammette che gli addendi possano anche essere nulli. Possiamo ricondurci a questa situazione sottraendo 1 da ogni addendo e usando $n-k$ al posto di n. Nell'esempio precedente si avrebbe quindi

$$\begin{aligned}
0+0+2&=2\\
0+1+1&=2\\
0+2+0&=2\\
1+0+1&=2\\
1+1+0&=2\\
2+0+0&=2.
\end{aligned}$$

A questo punto possiamo identificare tutte le configurazioni possibili con il seguente stratagemma. Rimpiazziamo ogni numero con un corrispondente numero di palline $\circ$ e ogni segno $+$ con una sbarretta $|$

$$\begin{array}{ccccccc}
| & | & \circ & \circ & = & \circ & \circ\\
| & \circ & | & \circ & = & \circ & \circ\\
| & \circ & \circ & | & = & \circ & \circ\\
\circ & | & | & \circ & = & \circ & \circ\\
\circ & | & \circ & | & = & \circ & \circ\\
\circ & \circ & | & | & = & \circ & \circ
\end{array}$$

In generale se ho n palline da suddividere in k gruppi, devo inserire $k-1$ sbarrette in posizione qualunque. Ogni configurazione corrisponde quindi alla scelta di un sottoinsieme di $k-1$ elementi (le sbarrette) in un insieme di $n+k-1$ elementi. Nel caso $n = 2$, $k = 3$ si ottiene in effetti:

$$\binom{n+k-1}{k-1} = \binom{4}{2} = 6.$$

Per il problema originario (dove gli addendi nulli non sono ammessi) la formula risulta invece (dobbiamo rimettere n al posto di $n+k$):

$$\binom{n-1}{k-1}.$$

1.1.7 Principio di inclusione esclusione

Se vogliamo calcolare il numero di elementi di una unione finita di insiemi finiti, possiamo utilizzare la formula seguente.

Teorema 1.20.

$$|A_1 \cup \cdots \cup A_n| =$$
$$\sum_i |A_i| - \sum_{i_1<i_2} |A_{i_1} \cap A_{i_2}| + \sum_{i_1<i_2<i_3} |A_{i_1} \cap A_{i_1} \cap A_{i_3}| + \cdots + (-1)^n |A_1 \cap \cdots \cap A_n|$$

Nel caso di 3 insiemi la formula può essere facilmente verificata tramite i diagrammi di Venn. In generale la dimostrazione di può fare come segue.

Dimostrazione. Per dimostrare che la formula è valida verifichiamo che ogni ogni elemento $x \in A = A_1 \cup \cdots \cup A_N$ dà contributo esattamente pari a 1 nelle somme sul lato destro dell'eguaglianza. Fissato $x \in A$ denotiamo con $I_x = \{i\colon x \in A_i\}$ l'insieme degli indici degli insiemi A_i che contengono x. Sia $|I_x| = m$. Nella somma

$$\sum_{i_1<\cdots<i_k} |A_{i_1} \cap \cdots \cap A_{i_k}|$$

l'elemento x viene contato tante volte quanti sono i sottoinsiemi di k elementi dell'insieme I_x che ha m elementi. Dunque l'elemento x viene contato (tenendo conto dei segni alterni) per un totale di

$$\sum_{k=1}^{n} (-1)^{k+1} \binom{m}{k} = 1 - \sum_{k=0}^{m} (-1)^k \binom{m}{k} = 1 - (1-1)^m = 1$$

volte. Quindi la formula è corretta. □

1.1.8 Funzioni suriettive

Come applicazione del principio di inclusione-esclusione possiamo cimentarci nel conteggio delle funzioni suriettive tra due insiemi finiti. Se $|A| = n$ e $|B| = m$ vogliamo determinare il numero di elementi dell'insieme $\mathrm{Sur}(A,B) = \{f\colon A \to B \quad f \text{ suriettiva}\}$. Innanzitutto enumeriamo gli elementi di B:

$$B = \{b_1, \ldots b_m\}$$

e consideriamo gli insiemi

$$X_i = \{f \in \mathrm{Sur}(A,B)\colon f(A) \subseteq f(B \setminus \{b_i\})\}$$

delle funzioni che non hanno b_k nella loro immagine. Chiaramente si avrà

$$\mathrm{Sur}(A,B) = B^A \setminus \bigcup_{i=1}^{m} X_i$$

e per il principio di inclusione esclusione

$$|X_1 \cup \cdots \cup X_m| = \sum_i |X_i| - \sum_{i<j} |X_i \cap X_j| + \cdots + (-1)^m |X_1 \cap \cdots \cap X_m|.$$

Osserviamo ora che

$$|X_{i_1}\cap\cdots\cap X_{i_k}| = |\{f\in B^A\colon f(A)\subseteq B\backslash\{b_{i_1},\dots,b_{i_k}\}\}| = |(B\backslash\{b_{i_1},\dots,b_{i_k}\})^A| = (m-k)^n$$

e in ogni somma il numero di possibili scelte di sottoinsiemi di k indici su m posizioni è $\binom{m}{k}$, dunque si ha

$$|B^A| - |X_1\cup\cdots\cup X_m| = m^n - \sum_{k=1}^{k}\binom{m}{k}(m-k)^n$$

da cui, in conclusione

$$|\mathrm{Sur}(A,B)| = \sum_{k=0}^{m}(-1)^k\binom{m}{k}(m-k)^n.$$

1.1.9 Dearrangiamenti

Con un procedimento simile possiamo determinare il numero dei *dearrangiamenti* ovvero delle permutazioni $f\colon A\to A$ senza punti fissi. Denotiamo con $D(A)\subseteq S(A)$ questo insieme.

Posto $A=\{a_1,\dots,a_n\}$ definiamo

$$A_i = \{f\in S(A)\colon f(a_i)=a_i\}$$

si ha

$$D(A) = S(A)\setminus\bigcup_{k=1}^{n}A_k$$

da cui, utilizzando il principio di inclusione-esclusione, si ha

$$|D(A)| = n! - \sum_i |A_i| + \sum_{i<j}|A_i\cap A_j| - \cdots - (-1)^n|A_1\cap\dots A_n|.$$

Osserviamo ora che gli elementi dell'insieme $A_{i_1}\cap\cdots\cap A_{i_k}$ sono le permutazioni di A che fissano gli elementi $a_{i_1},\dots,a_{i_k}$. Il numero di queste permutazioni è pari alle permutazioni degli elementi non fissati e cioè a $(n-k)!$. Dunque si ha:

$$|D(A)| = n! - \sum_{k=1}^{n}(-1)^k\binom{n}{k}(n-k)! = \sum_{k=0}^{n}(-1)^k\frac{n!}{k!} = n!\sum_{k=0}^{n}\frac{(-1)^k}{k!}.$$

Osserviamo inoltre che per $n\to\infty$ si ha

$$\frac{|D(A)|}{|S(A)|} = \sum_{k=0}^{n}\frac{(-1)^k}{k!}\to e^{-1}. \tag{2}$$

Esempio 1.21. *In un gruppo di 10 bambini ogni bambino mette un giocattolo in un sacco. Dopodiché i giocattoli vengono estratti a caso e vengono ridistribuiti ai 10 bambini. Qual è la probabilità che a ogni bambino capiti un giocattolo diverso da quello che aveva portato? In base alla formula precedente si ha che questa probabilità è circa $1/e$ ovvero circa il 37%. Si osservi che la somma considerata in (2) è a segni alterni, quindi la differenza tra la somma della serie completa e la somma parziale fino al termine n-esimo è inferiore al primo dei termini trascurati. Per $n=10$ l'errore è quindi inferiore a $1/10!$*

2 Insiemi Infiniti

2.1 Cardinali

Astraendo il concetto di *numero di elementi* utilizzato per gli insiemi finiti, possiamo dare le seguenti definizioni, valide per insiemi qualunque.

Definizione 2.1 (cardinalità)**.** *Diremo che due insiemi A e B hanno la* stessa cardinalità *e scriveremo*

$$|A| = |B| \qquad o \qquad \#A = \#B$$

se esiste una corrispondenza biunivoca tra di loro. Cioè se esiste una funzione $f\colon A \to B$ biettiva. Diremo invece che la cardinalità di A è minore o uguale a quella di B e scriveremo

$$|A| \leq |B| \qquad o \qquad \#A \leq \#B$$

se esiste una funzione $f\colon A \to B$ iniettiva.

Se $\mathcal{U}$ è una famiglia di insiemi la relazione $|A| = |B|$ risulta essere una relazione di equivalenza su $\mathcal{U}$ e si può definire la *cardinalità* di un insieme A come la classe di equivalenza di A rispetto a tale relazione. La cardinalità di un insieme si indica quindi con $|A|$ (o con $\#A$) e gli elementi dell'insieme quoziente si chiamano *cardinali*.

A partire dalle relazioni $=$ e $\leq$ tra *cardinali* si possono definire in maniera ovvia le relazioni $<$, $\geq$ e $>$.

Tramite l'assioma della scelta si può dimostrare che $|A| \geq |B|$ (con $B \neq \emptyset$) risulta equivalente all'esistenza di una funzione $f\colon A \to B$ suriettiva.

Il seguente esempio è quello che può essere chiamato il *paradosso dell'infinito* e cioè l'esistenza di funzioni iniettive ma non suriettive da un insieme in sé.

Esempio 2.2 (Hotel Hilbert)**.** *All'Hotel Hilbert, come in tutti gli Hotel, ogni stanza è numerata da un numero naturale. Inoltre, cosa più rara, per ogni numero naturale c'è una stanza con quel numero (compreso il numero* 13*).*

Al mio arrivo scopro con delusione che l'Hotel è pieno: ogni stanza è occupata da un cliente. Nonostante questo il Sig. Hilbert, proprietario dell'albergo, riesce a liberarmi una stanza. Come ha fatto?

Semplicemente il Sig. Hilbert ha contattato tutti i clienti dell'albergo dicendo al cliente della stanza n di spostarsi gentilmente nella stanza $n+1$. La stanza 0 *si è quindi liberata.*

Nel precedente esempio si rappresenta la funzione $s\colon \mathbb{N} \to \mathbb{N}$ definita da $s(n) = n+1$. Tale funzione risulta essere iniettiva ma non suriettiva, come garantito dagli assiomi di Peano (numeri diversi non hanno lo stesso successore e 0 non è successore di nessuno).

Definizione 2.3 (insiemi infiniti)**.** *Un insieme A si dice* infinito *se esiste una funzione $f\colon A \to A$ iniettiva ma non suriettiva.*

Un insieme infinito può essere messo in corrispondenza biunivoca con un suo sottoinsieme proprio. Ad esempio: $n \mapsto 2n$ è una corrispondenza biunivoca tra tutti i naturali e i numeri pari; questo significa che i numeri *pari* sono *tanti quanti* tutti i numeri $|2\mathbb{N}| = |\mathbb{N}|$.

Si può verificare che gli insiemi *infiniti* sono esattamente gli insiemi *non finiti* (si veda la definizione 1.1). Cioè: gli insiemi infiniti sono gli insiemi che non possono essere messi in corrispondenza biunivoca con $I_n = \{1, \ldots, n\}$ per alcun $n \in \mathbb{N}$.

2.1.1 Il teorema di Cantor

Teorema 2.4 (Cantor)**.** *Sia A un insieme. Allora*

$$|\mathcal{P}(A)| > |A|.$$

Dimostrazione. Che $|A| \leq |\mathcal{P}(A)|$ è molto semplice in quanto basta osservare che la funzione

$$a \mapsto \{a\}$$

è una funzione iniettiva $A \to \mathcal{P}(A)$. La parte interessante è dimostrare che $|A| \neq |\mathcal{P}(A)|$ cioè che non esistono funzioni biettive $f\colon A \to \mathcal{P}(A)$.

Se $f\colon A \to \mathcal{P}(A)$ possiamo definire

$$C = \{x \in A\colon x \notin f(x)\}.$$

Supponiamo ora che esista $c \in A$ tale che $f(c) = C$. Osserviamo ora che $c \in C$ se, per definizione, $c \notin f(c)$. Visto che $C = f(c)$ questa è una contraddizione in termini. Dunque non esiste nessun $c \in A$ tale che $f(c) = C$ che significa che f non è suriettiva. □

La dimostrazione precedente è stata ripresa da Russel nel suo famoso paradosso: l'insieme $R = \{x \notin x\}$ non è ben definito.

Altra conseguenza del Teorema di Cantor è la non esistenza dell'*insieme universo*. Se $\mathcal{U}$ fosse l'insieme di tutti gli insiemi dovrebbe essere $\mathcal{P}(\mathcal{U}) \subseteq \mathcal{U}$. Ma questo è impossibile per il Teorema di Cantor.

2.1.2 Teorema di Cantor-Bernstein

Osserviamo che la relazione $\leq$ tra cardinali soddisfa banalmente la proprietà riflessiva $|A| \leq |A|$ e transitiva $|A| \leq B, |B| \leq |C| \Rightarrow |A| \leq |C|$. Non banale è invece la proprietà antisimmetrica che è quella che ci manca per avere una relazione d'ordine:

Teorema 2.5 (Cantor-Bernstein)**.** *Se $|A| \leq |B|$ e $|B| \leq |A|$ allora $|A| = |B|$.*

Per avere una intuizione della dimostrazione di questo teorema ne enunciamo una istanza in forma geometrica.

Proposizione 2.6 (trasmutazione di forma)**.** *Sia C un cerchio e Q un quadrato. É possibile partizionare questi due insiemi in un numero finito di parti disgiunte: $C = C_1 \cup \cdots \cup C_N$, $Q = Q_1 \cup \cdots \cup Q_N$ tali che esistono delle similitudini del piano $\phi_1, \ldots, \phi_N$ tali che $\phi_k(C_k) = Q_k$.*

La dimostrazione del precedente enunciato è evidente se guardiamo la figura 1: Il quadrato e il cerchio si suddividono in due regioni (la bianca e la nera) che risultano essere simili tra loro.

Per dimostrare il teorema di Cantor-Bernstein si procede in maniera analoga. Supponiamo di avere le mappe iniettive $f\colon A \to B$ e $g\colon B \to A$. Si tratta semplicemente di identificare gli insiemi $N \subseteq A$ (nero in figura) e $M \subseteq B$ (bianco in figura) in modo che $A = N \cup g(M)$, $B = f(N) \cup M$ siano unioni disgiunte (cioè con intersezione vuota). Fatto ciò la mappa $h\colon A \to B$ definita da

$$h(x) = \begin{cases} f(x) & \text{se } x \in N \\ g^{-1}(x) & \text{se } x \in g(M) \end{cases}$$

si dimostra facilmente essere ben definita e biettiva.

L'insieme $N \subseteq A$ può essere definito come l'insieme di quei punti $x \in A$ tali che se prendo la successione di controimmagini $g^{-1}(x)$, $f^{-1}g^{-1}(x)$, $g^{-1}f^{-1}g^{-1}(x)\ldots$

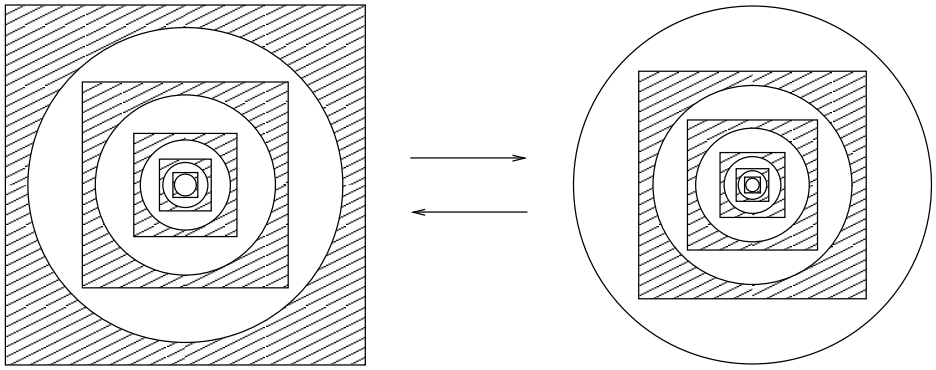


Figura 1: Si veda la proposizione 2.6

prima o poi finisco su un punto in A di cui non posso più fare la controimmagine tramite g (e invece sono sempre in grado di fare le controimmagini tramite f quando sono in B). L'insieme $f(N)$ è formato da quei punti di B tali che facendo a ripetizione le controimmagini mi ritrovo in un punto di A di cui non posso più fare la controimmagine. Il suo complementare $M = B \setminus f(N)$ è dunque composto da quei punti tali che facendo le controimmagini non mi fermo mai oppure mi fermo in un punto di B che non ha retroimmagine tramite f. Per definizione M e $f(N)$ formano una partizione di B. Dobbiamo solo dimostrare che $g(M)$ e N sono una partizione di A. Per fare questo consideriamo un punto $a \in g(M)$. Allora $a = g(b)$ e $b \in M$ significa che facendo a ripetizione le controimmagini di b o non mi fermo mai, oppure mi fermo in un punto di B che non ha controimmagine tramite f. Dunque prendendo a ripetizioni le controimmagini di a al primo passo trovo b e quindi a seguire non mi fermerò mai in un punto di A. Questo significa che $a \notin N$. D'altra parte se $a \in N$ sappiamo che $g^{-1}(a) \notin M$ e quindi $a \notin g(M)$.

Il teorema di Cantor-Bernstein è comodo per dimostrare, ad esempio, che gli insiemi $[0, 1]$, $(0, 1)$, $\mathbb{R}$, $[0, +\infty)$ hanno tutti la stessa cardinalità. E' sufficiente trovare delle mappe iniettive che mandano ognuno di questi insiemi in ognuno degli altri. Tali mappe iniettive possono essere cercate tra le funzioni continue. Se volessimo invece individuare delle mappe biettive, dovremmo cercare anche tra le funzioni non continue.

I cardinali sono anche *totalmente ordinati* in quanto vale la proprietà:

Teorema 2.7 (totale ordinamento dei cardinali)**.** *Se A e B sono insiemi qualunque o $|A| \leq |B|$ o $|B| \leq |A|$ deve valere.*

Dimostrazione. Questa proprietà è equivalente all'assioma della scelta. □

2.1.3 Cardinalità degli insiemi numerici

Osserviamo innanzitutto che l'insieme $\mathbb{N}$ dei numeri naturali non è finito, in quanto può essere messo in corrispondenza biunivoca con un suo sottoinsieme proprio, come abbiamo già osservato.

Per banale inclusione possiamo immediatamente affermare che

$$|\mathbb{N}| \leq |\mathbb{Z}| \leq |\mathbb{Q}| \leq |\mathbb{R}| \leq |\mathbb{C}|.$$

Vedremo ora che per i primi tre insiemi si ha l'uguaglianza. Gli insiemi che hanno la stessa cardinalità dei numeri naturali vengono detti *numerabili* in quanto la corrispondenza biunivoca con i naturali fornisce una numerazione degli elementi dell'insieme.

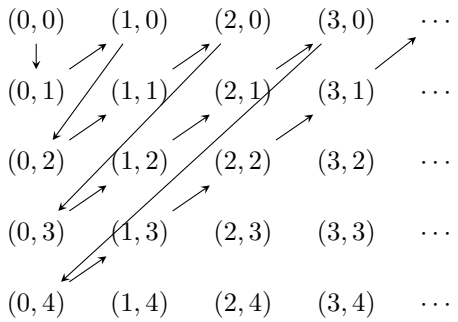
Una numerazione dei numeri interi si ottiene facilmente come segue:

$$0, 1, -1, 2, -2, 3, -3, \ldots$$

dunque si ha $|\mathbb{N}| = |\mathbb{Z}|$.

Teorema 2.8 (primo procedimento diagonale di Cantor)**.** $\mathbb{N}^2$ *è numerabile.*

Dimostrazione. Una biezione $f\colon \mathbb{N}^2 \to \mathbb{N}$ è data graficamente:



□

La mappa $(a, b) \to a/b$, $\mathbb{Z}^2 \to \mathbb{Q}$ è suriettiva, ma $|\mathbb{Z}^2| = |\mathbb{N}^2| = |\mathbb{N}|$ e quindi $|\mathbb{Q}| \leq |\mathbb{N}|$.

Per induzione abbiamo che $|\mathbb{N}^k| = |\mathbb{N} \times \mathbb{N}^{k-1}| = |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$, dunque tutte le potenze intere di un insieme numerabile sono numerabili. Ovviamente si ha invece $|\mathbb{N}^{\mathbb{N}}| \geq |2^{\mathbb{N}}| = |\mathcal{P}(\mathbb{N})| > |\mathbb{N}|$. D'altra parte $|\mathbb{N}^{\mathbb{N}}| \leq |2^{\mathbb{N}^2}|$ in quanto le funzioni $\mathbb{N} \to \mathbb{N}$ si possono rappresentare tramite i loro grafici che sono sottoinsiemi di $\mathbb{N}^2$. Dunque $|\mathbb{N}^{\mathbb{N}}| \leq |2^{\mathbb{N}^2}| = |2^{\mathbb{N}}|$.

Possiamo anche affermare che una unione numerabile di insiemi numerabili risulta essere numerabile. Infatti se A_k con $k \in \mathbb{N}$ sono insiemi numerabili, avremo $A_k = f_k(\mathbb{N})$ con $f_k\colon \mathbb{N} \to A_k$ biettiva. Dunque $(k, j) \mapsto f_k(j)$ risulta essere una funzione surgettiva $\mathbb{N}^2 \to \bigcup_k A_k$.

Questo ci permette di affermare, ad esempio, che la famiglia dei sottoinsiemi finiti di un insieme numerabile è a sua volta numerabile (ricordiamo che la famiglia di tutti i sottoinsiemi invece non lo è). Infatti la famiglia dei sottoinsiemi finiti è unione per $k \in \mathbb{N}$ delle famiglie di sottoinsiemi con k elementi. E i sottoinsiemi con k elementi di un insieme A sono meno di A^k, dunque se A è numerabile sono anch'essi numerabili per ogni $k \in \mathbb{N}$.

Allo stesso modo le parole finite con lettere prese da un alfabeto numerabile sono anch'esse numerabili. Se A è il nostro insieme numerabile di lettere, le parole di k lettere si identificano con A^k. Dunque l'insieme delle parole finite è unione numerabile di insiemi numerabili.

Come conseguenza abbiamo che l'insieme $\mathbb{Z}[x]$ dei polinomi a coefficienti interi è numerabile. Infatti i monomi sono una quantità numerabile (anche per polinomi in più variabili) in quanto sono coppie formate da un coefficiente intero e una parte letterale, e la parte letterale è una parola scritta con un alfabeto finito di simboli (le variabili). I polinomi sono a loro volta parole finite scritte con un numero finito di monomi.

Infine possiamo affermare che l'insieme dei numeri algebrici è numerabile. Gli algebrici infatti sono gli zeri di polinomi a coefficienti interi. Siccome ogni polinomio ha un numero finito di zeri e i polinomi sono numerabili, risulta che anche i loro zeri sono una quantità numerabile.

Più in astratto possiamo affermare che l'insieme dei *numeri che sono univocamente determinati come la soluzione di un qualche problema* è numerabile. Per *problema* si intende qualunque proprietà descrivibile tramite una proposizione scritta in un qualunque linguaggio formale che utilizzi una quantità numerabile di simboli.

Premesso tutto questo possiamo meglio apprezzare il seguente teorema.

Teorema 2.9 (secondo procedimento diagonale di Cantor)**.** *Si ha* $|\mathbb{R}| > |\mathbb{N}|$.

Dimostrazione. La dimostrazione originale di Cantor utilizza la rappresentazione decimale dei numeri reali. In particolare l'osservazione che ogni numero in $[0, 1]$ può essere rappresentato dalla sequenza infinita delle sue cifre decimali. Supponendo di avere una numerazione x_k dei numeri in $[0, 1]$ possiamo rappresentare ogni x_k tramite le sue cifre decimali:

$$x_k = \sum_{j \in \mathbb{N}} a_{kj} 10^{-j}.$$

Consideriamo allora il numero:

$$\bar{x} = \sum_{j \in \mathbb{N}} \bar{a}_{jj} 10^{-j}$$

dove $\bar{a}_{jj}$ è una qualunque cifra diversa da a_{jj} da 0 e da 9. Il numero $\bar{x}$ risulta diverso da ogni altro numero x_k perché alla posizione k hanno una cifra diversa. L'unico modo per avere due rappresentazioni decimali diverse dello stesso numero si ha con i numeri che terminano con infiniti 9, i quali possono essere rappresentati anche con un numero terminante con infiniti 0. Avendo escluso che $\bar{x}$ rientri in questa casistica (non ha mai le cifre 0 e 9) giungiamo dunque ad un assurdo.

Se osserviamo che i numeri in $[0, 1]$ si rappresentano con parole di infinite lettere scritte con un numero finito di simboli (escludendo 0 e 9 per avere rappresentazioni uniche) possiamo concludere immediatamente che $|\mathbb{R}| \geq |\{1, 2, 3, 4, 5, 6, 7, 8\}^{\mathbb{N}}| \geq |2^{\mathbb{N}}| > |\mathbb{N}|$.

Una dimostrazione alternativa può essere fatta osservando che i numeri reali contengono l'insieme di Cantor. E l'insieme di Cantor può essere rappresentato così:

$$C = \left\{ \sum_{k \in \mathbb{N}} \frac{c_k}{3^k} : c_k \in \{0, 2\} \right\}$$

Bisogna osservare che successioni c_k diverse corrispondono a numeri diversi (se la prima cifra diversa è la k-esima, i due numeri distano tra loro più di $1/3^{k+1}$). Dunque $|C| = |2^{\mathbb{N}}| > |\mathbb{N}|$. □

L'insieme delle funzioni $\mathbb{R} \to \mathbb{R}$ ha cardinalità non inferiore a quella di $2^{\mathbb{R}}$ e quindi ha cardinalità maggiore di $\mathbb{R}$. E' interessante osservare che invece le funzioni *continue* possono essere messe in corrispondenza biunivoca con $\mathbb{R}$. Infatti le funzioni continue sono univocamente determinate dal loro valore sull'insieme $\mathbb{Q}$ essendo $\mathbb{Q}$ denso in $\mathbb{R}$. Ma $\mathbb{R}^{\mathbb{Q}}$ è unione numerabile di copie di $\mathbb{R}$ ed ha quindi la stessa cardinalità di $\mathbb{R}$.

2.2 Ordinali

Definizione 2.10 (ordine parziale)**.** *Una relazione d'ordine (parziale) su un insieme A è una relazione riflessiva, antisimmetrica e transitiva:*

- *$a \leq a$ (riflessiva);*
- *$a \leq b$ e $b \leq a$ implica $a = b$ (antisimmetrica);*

- $a \leq b$ *e* $b \leq c$ *implica* $a \leq c$ *(transitiva).*

L'ordine si dice totale *se vale anche la proprietà*

- $a \leq b$ *o* $b \leq a$*.*

Gli elementi a, b tali che $a \leq b$ o $b \leq a$ si dicono *comparabili*. In un ordine parziale non si richiede che tutte le coppie di elementi siano comparabili.

Gli elementi di un insieme finito parzialmente ordinato possono essere rappresentati tramite il grafico di Hasse: unisco con un arco (diretto verso l'alto) i vertici x e y se $x < y$ e non ci sono z tali che $x < z < y$ (riduzione transitiva).

Un tipico esempio di ordine parziale è l'inclusione insiemistica. I sottoinsiemi totalmente ordinati di un insieme parzialmente ordinato si chiamano *catene*.

Ad esempio gli insiemi $\{\} \subseteq \{1\} \subseteq \{1, 2\}$ formano una catena rispetto all'inclusione. Gli insiemi $\{1\}$ e $\{2\}$ non sono invece comparabili.

Definizione 2.11 (estremi)**.** *Un elemento a tale che $b \leq a$ per ogni b si dice un* massimo*. In particolare un massimo è comparabile con ogni altro elemento. Un elemento a tale che non esiste $b \neq a$ con $a \leq b$ si dice* massimale*. Se c'è un massimo non ci possono essere altri elementi massimali. Un* maggiorante *di un sottoinsieme A è un elemento b tale che per ogni $a \in A$ si ha $a \leq b$.*

Definizioni analoghe si danno per minimo*,* minimale *e* minorante*.*

Definizione 2.12 (buon ordinamento)**.** *Un* buon ordinamento *è un ordinamento totale con la proprietà aggiuntiva che ogni sottoinsieme non vuoto ammette minimo.*

Ad esempio l'insieme dei numeri naturali è *ben ordinato*. Non lo sono invece gli altri insiemi numerici. Tutti gli insiemi ben ordinati hanno delle proprietà simili a quelle dei numeri naturali.

- un insieme ben ordinato ha elemento minimo che possiamo denotare con 0;
- ogni elemento che non sia il massimo dell'insieme ammette un *successore*. Il successore di a è il minimo degli elementi più grandi di a: $s(a) = \min\{b\colon a < b\}$.

Ricordiamo che ogni volta che abbiamo definita una relazione tramite il simbolo $\leq$ si intende che siano definite di conseguenza le relazioni $\geq$, $<$, $>$. Ad esempio $a < b$ significa $a \leq b$, $a \neq b$.

Gli elementi di un insieme totalmente ordinato possono essere denominati come segue:

- un elemento si dice *zero* se è il minimo di tutti gli elementi;
- un elemento si dice *successore* se è il successore di un'altro elemento;
- un elemento si dice *limite* se non è zero e non è successore.

2.2.1 induzione transfinita

Sia A un insieme ben ordinato e sia P una proprietà definita per ogni elemento $a \in A$.

Teorema 2.13 (induzione transfinita)**.** *Se per ogni a vale*

$$\text{se } P(b) \text{ è vera per ogni } b < a \text{ allora } P(a) \text{ è vera}$$

allora $P(a)$ è vera per ogni a.

Dimostrazione. Sia B l'insieme degli elementi per cui P è falsa. Se per assurdo B fosse non vuoto potremmo considerare a il minimo di tale insieme. Allora $P(b)$ è vera per ogni $b < a$ (altrimenti a non sarebbe il minimo) e dunque $P(a)$ è vera il che è assurdo. □

Osserviamo che per applicare l'induzione transfinita bisogna sapere che $P(0)$ è vera. Infatti per $a = 0$ l'insieme dei $b < a$ è vuoto e quindi $P(0)$ deve essere vera senza nessuna ipotesi ausiliaria

Definizione 2.14 (isomorfismo d'ordine)**.** *Se A e B sono insiemi parzialmente ordinati una funzione biettiva e crescente $f\colon A \to B$, si dice essere un* isomorfismo d'ordine*. Una funzione è crescente se mantiene la relazione d'ordine ovvero:*

$$a \leq b \Leftrightarrow f(a) \leq f(b).$$

Nota bene: nel seguito di questa sezione utilizzeremo il simbolo $\subset$ con il significato di $\subsetneq$, cioè per indicare l'inclusione stretta. Questo significato è spesso considerato ambiguo in quanto in molti testi si usa $\subset$ con il significato di $\subseteq$. Noi invece lo useremo molto in quanto, come vedremo subito, vogliamo mettere in evidenza una analogia tra i simboli $<, \leq$ e i simboli $\subset, \subseteq$.

Definizione 2.15 (ordinale)**.** *Se X è un insieme bene ordinato e $a \in X$ definiamo il* segmento X_a *come il sottolivello di a, ovvero:*

$$X_a = \{x \in X\colon x < a\}.$$

Un insieme X si dice un ordinale *se è un insieme ben ordinato rispetto all'inclusione e ogni suo elemento coincide con il proprio segmento, cioè per ogni $a \in X$ si ha*

$$a = X_a = \{x \in X\colon x \subset a\}.$$

Dalla definizione si osserva che se X è un ordinale e $a \in X$ si ha

$$x \in a \Leftrightarrow x \subset a.$$

Inoltre se $x \in a$ risulta che $x \in X$ in quanto a coincide con il proprio segmento, che è un insieme di elementi di X. Dunque sugli ordinali i simboli $\in$ e $\subset$ sono interscambiabili.

Un esempio di ordinale è l'insieme dei numeri naturali:

$$0 = \emptyset, \quad 1 = \{0\}, \quad 2 = \{0, 1\}, \quad \ldots \quad n + 1 = \{0, 1, \ldots, n\}, \quad \ldots$$

Osserviamo che per un ordinale (come per i numeri naturali) il successore $s(a)$ di un elemento a può essere definito come segue:

$$s(a) = a \cup \{a\}$$

infatti ricordiamo che $s(a) = \{x \in X\colon x < s(a)\} = \{x \in X\colon x < a\} \cup \{a\} = a \cup \{a\}$. Osserviamo inoltre che $a \cup \{a\}$ ci garantisce la particolare proprietà che a è sia un sottoinsieme che un elemento di $s(a)$.

Osserviamo anche che dato un qualunque insieme ben ordinato X possiamo definire tramite *induzione transfinita* un isomorfismo d'ordine $f\colon X \to A$ con un cardinale A. Si definisce infatti per $a \in X$

$$f(a) = \{f(x)\colon x < a\}$$

e si osserva che $a < b$ è equivalente a $f(a) \subset f(b)$.

Dunque ogni insieme bene ordinato è isomorfo ad un ordinale. Il seguente teorema ci dice che tale ordinale è unico, cioè che gli ordinali sono dei rappresentanti canonici delle classi di equivalenza degli insiemi bene ordinati rispetto agli isomorfismi d'ordine.

Teorema 2.16. *Se A e B sono ordinali e $f\colon A \to B$ è un isomorfismo d'ordine, allora $A = B$.*

Dimostrazione. E' sufficiente dimostrare che f è l'identità. Dimostriamo innanzitutto che $f(a) = a$ per ogni $a \in A$ utilizzando l'induzione transfinita. Supponiamo dunque che per ogni $x \subset a$ (ricordiamo che gli ordinali sono ordinati dall'inclusione) si abbia $f(x) = x$. Dobbiamo dimostrare che $f(a) = a$.

Per definizione di ordinale abbiamo che

$$a = \{x \in A\colon x \subset a\}, \qquad f(a) = \{y \in B\colon y \subseteq f(a)\}.$$

osserviamo ora che essendo f un isomorfismo d'ordine $x \subset a$ è equivalente a $f(x) \subseteq f(a)$, inoltre se $x \subset a$ sappiamo che $f(x) \subset f(a)$ (per ipotesi induttiva), dunque

$$a = \{f(x)\colon x \in A,\ f(x) \subset f(a)\}.$$

D'altra parte essendo f una funzione suriettiva, ogni $y \in B$ si può scrivere come $f(x)$ per qualche $x \in A$, dunque

$$b = \{f(x)\colon x \in A,\ f(x) \subset f(a)\}$$

da cui $a = b$.

Dunque abbiamo mostrato che $f(x) = x$ per ogni $x \in A$ ed essendo f biettiva se ne deduce che f è l'identità e dunque $A = B$. □

Abbiamo quindi messo in evidenza il fatto che l'isomorfismo d'ordine tra insiemi ha un rappresentante canonico dato dagli ordinali. Sarà quindi interessante investigare le proprietà della classe di tutti gli ordinali che denoteremo con Ord. Siamo nella posizione di dimostrare che l'inclusione tra ordinali risulta avere le proprietà del buon ordinamento nella classe Ord. Ovviamente la relazione $\subseteq$ soddisfa le proprietà di un ordinamento (parziale). La prima proprietà che ci interessa osservare è che l'ordine è totale, cioè che se A e B sono ordinali allora $A \subseteq B$ o $B \subseteq A$. Questo si dimostra con l'induzione transfinita in modo analogo a come abbiamo fatto per il Teorema 2.16. Inoltre l'ordinamento è *buono* in quanto dato un insieme X di ordinali, il minimo di tale classe è semplicemente $A = \cap X$.

Un'altra proprietà interessante è data dal seguente

Teorema 2.17 (principio di buon ordinamento)**.** *Ogni insieme A ammette un buon ordinamento.*

Dimostrazione. Si utilizza l'assioma della scelta. □

2.2.2 costruzione degli ordinali

Abbiamo già osservato che i numeri naturali sono un esempio di ordinali:

$$0 = \emptyset, \quad 1 = \{0\}, \quad 2 = \{0, 1\}, \quad \dots$$

Se non avessimo a disposizione l'assioma di infinito questi sarebbero gli unici ordinali che saremmo in grado di costruire (cioè per i quali gli assiomi ci garantiscono l'esistenza). Questi ordinali (cioè i numeri naturali) vengono chiamati *ordinali finiti* in quanto sono in effetti insiemi finiti.

Tramite l'assioma di infinito ci viene garantita l'esistenza di un ordinale infinito. Se prendiamo il minimo tra gli ordinali infiniti otteniamo l'ordinale ω dei numeri naturali:

$$\omega = \{0, 1, \dots, n, \dots\}.$$

Abbiamo già osservato che

$$s(\alpha) = \alpha \cup \{\alpha\}.$$

Ci convinciamo che la precedente definizione è coerente alla definizione dei numeri naturali in quanto:

$$n + 1 = \{0, 1, \ldots, n\} = \{0, 1, \ldots, n-1\} \cup \{n\} = n \cup \{n\} = s(n).$$

Ogni ordinale ha un successore, ma non tutti gli ordinali hanno un predecessore. Tra i numeri naturali solo 0 non ha predecessore. Ma anche ω non lo ha, ed è quindi un *ordinale limite*. Si può verificare che vale:

$$\omega = \lim_{n<\omega} n$$

avendo dato la seguente definizione di limite.

Definizione 2.18 (limite)**.** *Se α_ξ sono ordinali indicizzati da un ordinale $\xi < \xi_0$ diremo che*

$$\lim_{\xi<\xi_0} \alpha_\xi = \alpha$$

se per ogni ordinale $\beta < \alpha$ esiste $\zeta < \xi_0$ tale che $\xi < \zeta < \xi_0 \Rightarrow \beta < \alpha_\xi \leq \alpha$.

Abbiamo quindi una prima estensione dei numeri naturali:

$$0, 1, \ldots, n, \ldots, \omega.$$

D'altra parte ogni ordinale ha un successore, e quindi possiamo continuare la catena:

$$0, 1, \ldots, \omega, s(\omega), s(s(\omega)), s(s(s(\omega))) \ldots$$

Per avere una notazione più comoda possiamo dare la seguente.

Definizione 2.19 (somma di ordinali)**.** *Se α_t con $t \in \lambda$ sono ordinali indicizzati su un ordinale, definitamo l'ordinale*

$$\sum_{t\in\lambda} \alpha_t$$

come l'ordinale equivalente all'insieme

$$A = \bigcup_{t\in\lambda} \alpha_t \times \{t\}$$

dotato dell'ordine dato da

$$(\nu, t) <_A (\nu', t') \Leftrightarrow (t < t') \vee (t = t' \wedge \nu < \nu').$$

Nel caso particolare in cui $\lambda = 2$ stiamo facendo la somma di due ordinali, che scriveremo semplicemente $\alpha + \beta$

Sostanzialmente stiamo facendo delle copie distinte dei nostri ordinali α_t e e le stiamo affiancando una di seguito all'altra rispettando l'ordine degli indici t.

E' facile verificare che $\alpha + 1 = s(\alpha)$ e più in generale che vale $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$ cosicché possiamo dire che $s(s(\omega)) = \omega + 2$ e la nostra successione di ordinali diventa:

$$0, 1, \ldots, \omega, \omega + 1, \omega + 2, \ldots.$$

Osserviamo però che la somma non è commutativa. Ad esempio si ha $1 + \omega = \omega \neq \omega + 1$.

La successione di ordinali costruita fin'ora si può ulteriormente estendere prendendo l'unione di tutti gli ordinali già costruiti. Tale ordinale corrisponde proprio ad $\omega + \omega$ e in maniera analoga si può costruire $\omega + \omega + \omega$ etc.

Per semplificare ulteriormente la notazione introduciamo il concetto di prodotto tra ordinali, semplicemente come somma ripetuta:

$$\alpha \cdot \beta = \sum_{t \in \beta} \alpha.$$

Anche la moltiplicazione risulta non essere commutativa. Ad esempio:

$$2 \cdot \omega = 2 + 2 + 2 + \cdots = \omega < \omega + \omega = \omega \cdot 2.$$

Risulta però valida la proprietà associativa: $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$ e distributiva $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$. La distributiva sul lato sinistro però non è valida, ad esempio:

$$(1 + 1) \cdot \omega = 2 \cdot \omega = \omega < \omega + \omega = 1 \cdot \omega + 1 \cdot \omega.$$

Si potrebbe procedere ulteriormente e definire la potenza tra ordinali, con una definizione *ricorsiva* che soddisfi le proprietà

$$\begin{aligned} \alpha^0 &= 1 \\ \alpha^{\beta+1} &= \alpha^\beta \cdot \alpha \\ \alpha^\beta &= \lim_{t<\beta} \alpha^t, \text{se } \beta \text{ è un ordinale limite.} \end{aligned}$$

Anche la potenza soddisfa alcune proprietà naturali:

$$\alpha^\beta \cdot \alpha^\gamma = \alpha^{\beta+\gamma}, (\alpha^\beta)^\gamma = \alpha^{(\beta \cdot \gamma)}.$$

Tramite queste operazioni è possibile costruire una sequenza transfinita di ordinali:

$$\begin{aligned} &0, 1, 2, \ldots, \omega, \omega + 1, \ldots, \omega \cdot 2, \ldots \omega \cdot 3, \cdot, \omega \cdot \omega, \ldots \\ &\omega^3, \omega^3 + 1, \ldots, \omega^3 + \omega, \ldots \omega^3 + \omega^2, \ldots, \omega^4, \omega^4 + 1, \ldots \\ &\omega^\omega, \omega^\omega + 1, \ldots, \omega^{\omega \cdot 2}, \ldots, \omega^{\omega \cdot 3}, \ldots, \omega^{\omega \cdot \omega}, \ldots \\ &\omega^{(\omega^2)}, \ldots, \omega^{(\omega^3)}, \ldots, \omega^{(\omega^\omega)}, \ldots \\ &\omega^{\omega^{\omega^\cdots}}, \ldots \end{aligned}$$

2.2.3 legame tra ordinali e cardinali

Osserviamo ora che dal punto di vista della cardinalità, tutti gli ordinali che abbiamo costruito sin'ora sono *numerabili*! La sequenza precedente, quindi, è solo un piccolo segmento iniziale di tutti gli ordinali, in quanto sappiamo che l'insieme $\mathcal{P}(\omega)$ non può essere messo in corrispondenza con nessuno di questi ordinali, e quindi il suo ordinale (che esiste per il principio di buon ordinamento) supera tutti questi.

Definizione 2.20 (cardinale)**.** *Se A è un insieme qualunque definiamo $|A|$ come il più piccolo ordinale equipollente ad A.*

A questo punto possiamo osservare che gli ordinali finiti sono tutti cardinali. Mentre gli ordinali elencati nella precedente sezione corrispondono tutti allo stesso cardinale ω. Risulta quindi che ω è il minimo cardinale infinito (essendo il minimo ordinale infinito). Per distinguere cardinali da ordinali useremo un nome diverso per i cardinali e chiameremo $\aleph_0 = |\omega| = \omega$.

Osserviamo che anche i cardinali sono bene ordinati, infatti se prendiamo la classe di tutti gli ordinali α tali che $|\alpha| > \aleph_0$ tale classe ha un minimo che potremo

chiamare $\aleph_1$ e così procedendo potremo costruire $\aleph_2, \aleph_3, \ldots, \aleph_\omega, \ldots$. Si osserva dunque come la classe dei cardinali è in corrispondenza biunivoca con la classe degli ordinali!

La questione naturale che già Cantor si pose arrivato a questo punto è (ipotesi di Cantor o ipotesi del continuo):

$$\aleph_1 \stackrel{?}{=} |\mathcal{P}(\aleph_0)|$$

Noi sappiamo infatti che $|\mathcal{P}(\aleph_0)| > \aleph_0$ ed essendo $\aleph_1$ il più piccolo cardinale maggiore di $\aleph_0$ sappiamo che $|\mathcal{P}(\aleph_0)| \geq \aleph_1$.

Per pura informazione enunciamo il seguente teorema la cui dimostrazione non verrà neanche accennata.

Teorema 2.21 (Gödel, Cohen)**.** *L'ipotesi del continuo non può essere dimostrata o refutata in ZFC.*

3 Misurare

Nel capitolo precedente abbiamo parlato del *contare*. Abbiamo visto che su insiemi senza alcuna struttura possiamo definire il concetto di *cardinalità* e sugli insiemi ordinati possiamo parlare di *ordinali*.

In realtà, né i *cardinali* né gli *ordinali* sono utili quando vogliamo parlare di lunghezze, aree e volumi. Per definire questi concetti useremo il termine di *misura*.

3.1 La misura: proprietà intuitive

Supponiamo di avere uno spazio ambiente in cui ci sono gli oggetti che vogliamo misurare. Per fissare le idee possiamo pensare al piano euclideo, che identifichiamo, oppure allo spazio tridimensionale. La struttura *geometrica* di questi spazi è determinata dalle *isometrie*.

In questo contesto pensiamo alle *isometrie* come ad un dato primitivo: cioè non le definiamo. Questo perché la definizione di *isometria* richiede di avere una *distanza* definita sullo spazio (le isometrie sono quelle trasformazioni che conservano la distanza). Tuttavia la *distanza* è per certi versi essa stessa una *misura* (e infatti gli spazi con distanza si chiamano *spazi metrici*) e noi vogliamo ottenere il concetto di misura a partire dalle trasformazioni geometriche.

Questo approccio è giustificato dall'esperienza. Per dire che due bastoni hanno la stessa lunghezza possiamo sovrapporli l'uno all'altro tramite un movimento rigido. Per dire che un bastone è lungo 1 metro, dobbiamo sovrapporre la nostra unità di misura (il metro) al bastone e verificarne la *congruenza*. Per affermare che un bastone è lungo 2 metri possiamo osservare che il bastone può essere spezzato in due parti distinte, ognuna delle quali è congruente al metro.

Questo approccio intuitivo può essere espresso dalle seguenti proprietà del concetto intuitivo di *misura*.

Una misura m deve soddisfare le seguenti proprietà:

1. oggetti *sovrapponibili* hanno la stessa misura:

$$m(A) = m(B) \qquad \text{se } B = \theta(A) \text{ dove } \theta \text{ è una isometria}$$

2. la misura è *additiva*:

$$m(A \cup B) = m(A) + m(B) \qquad \text{se } A \text{ e } B \text{ non si sovrappongono}$$

3. c'è una *unità* di riferimento, cioè un oggetto convenzionale U tale che:

$$m(U) = 1.$$

Osserviamo che se prendiamo come oggetto di riferimento $U_0 = \{p\}$ un singolo punto la misura m che se ne ottiene è il *numero di elementi*. Infatti ogni insieme formato da un solo punto può essere messo in corrispondenza tramite una isometria con l'unità U_0. Inoltre ogni insieme finito $A = \{a_1, \ldots, a_N\}$ può essere scritto come unione disgiunta dei suoi punti:

$$A = \{a_1\} \cup \{a_2\} \cup \cdots \cup \{a_N\}$$

e quindi $m(A) = m(\{a_1\}) + \cdots + m(\{a_N\}) = 1 + \cdots + 1 = N$.

Una misura di questo tipo verrà chiamata una misura 0-dimensionale, in quanto il punto geometrico U_0 intuitivamente *non ha dimensioni*. Possiamo quindi pensare al *contare* come ad un caso particolare di misura 0-dimensionale.

Più interessante è il concetto di *lunghezza* che si ottiene scegliendo come unità U_1 un segmento. Se costruiamo un quadrato sul lato U_1 possiamo affermare che ognuno dei quattro lati è congruente all'unità di misura U_1 e quindi la lunghezza del perimetro del quadrato di lato 1 è 4. Nella prossima sezione ci occuperemo del problema di capire se due lati consecutivi del quadrato si sovrappongono o meno (in quanto hanno un punto in comune).

Chiediamoci invece cosa succede se proviamo a misurare la lunghezza della diagonale del quadrato. Se A e C sono i due vertici opposti del quadrato, ruotando l'unità di misura $U_1 = AB$ otteniamo un punto A_1 sulla diagonale e la diagonale risulta divisa in due segmenti AA_1 e A_1C. Sapendo che $m(AA_1) = 1$ ci resta da misurare A_1C. Dividiamo l'unità U_1 in dieci parti uguali (che chiameremo *decimi*) e proviamo quindi a vedere quanti decimi stanno sul segmento A_1C.