

UN PO' DI COMBINATORIA

GIOVANNI CUTOLO

1. Premessa: cosa significa contare?	1
2. Il principio di buon ordinamento per i naturali ed il principio di induzione	2
2.1. Dimostrazioni per controesempio minimo	2
2.2. Principio di induzione e di induzione completa	2
3. Biettività, equipotenza ed insiemi finiti	3
4. Unioni	5
4.1. Il principio di inclusione-esclusione	6
5. Contare applicazioni	8
5.1. Varianti: stringhe, parole	10
6. Parti	11
6.1. Coefficienti binomiali	12
7. Appendice	17
7.1. Dimostrazioni per controesempio minimo e per induzione	17

In queste note sono riportati alcuni risultati elementari ed idee relative a metodi per il conteggio del numero di elementi di insiemi finiti.

Diamo per noti l'insieme $\mathbb{N}$ dei numeri naturali e le operazioni elementari (addizione, moltiplicazione, elevazione a potenza) definite in esso.

1. PREMESSA: COSA SIGNIFICA CONTARE?

Iniziamo col dare un senso a questa espressione. Messi davanti ad una collezione finita di (sperabilmente pochi) oggetti, siamo (stati) abituati a contarli secondo una procedura che consiste nell'associare ciascuno di questi oggetti ad uno dei primi interi positivi, presi, consecutivamente, in sequenza: puntiamo (magari con un dito) ad uno di questi oggetti abbinandolo al numero 1 (magari pronunciando effettivamente 'uno'), poi puntiamo ad un altro oggetto abbinandolo al numero 2 ('due!'), poi ad un altro ancora e così via ('tre', 'quattro' etc.) finché non abbiamo esaurito gli oggetti da contare; a quel punto (così ci è stato detto) l'ultimo numero pronunciato è il numero degli oggetti nella collezione.

Possiamo dare un senso preciso a questa procedura. Pensiamo a questi oggetti come agli elementi di un insieme C e, per comodità, per ogni numero naturale n chiamiamo I_n l'insieme dei primi n interi positivi, vale a dire: $I_n = \{i \in \mathbb{N}^* \mid i \leq n\} = \{1, 2, \dots, n\}$. Se il nostro 'conteggio' è terminato col numero k (facendoci concludere che 'gli oggetti sono in tutto k '), abbiamo descritto un'applicazione, chiamiamola f , da I_k a C : ad ogni $i \in I_k$ abbiamo associato un elemento di C (quello a cui stavamo puntando, forse, il dito mentre pronunciavamo " i "). Quali sono le 'regole del gioco' che, più o meno consapevolmente, abbiamo imparato a seguire e che, se rispettate, ci fanno concludere che il risultato del nostro conteggio è corretto? Sono due. La prima: che 'contando' gli oggetti non ne abbiamo tralasciato nessuno, cioè che ciascuno degli elementi di C è stato associato ad almeno un numero in I_k ; questo significa precisamente che f è suriettiva. La seconda: che non abbiamo contato due volte lo stesso oggetto, cioè che f è iniettiva: numeri diversi in I_k sono stati sempre abbinati ad oggetti diversi. Dunque, siamo portati (dalle nostre abitudini) a dire che il conteggio è stato eseguito correttamente precisamente quando l'applicazione f è biettiva. È questo il senso che in matematica possiamo dare all'espressione 'contare'; in effetti questo ci può portare anche a dare una definizione (una delle tante possibili) di cosa si intenda per insieme finito.

Se a è un insieme, diciamo che a è finito se e solo se esiste $k \in \mathbb{N}$ tale che esista un'applicazione biettiva da I_k ad a . In questo caso, di un tale k diciamo anche che " a ha esattamente k elementi".⁽¹⁾

Vorremmo fare un ulteriore passo in avanti e, sempre nella stessa situazione, dire che un tale k è il numero degli elementi di a . Abbiamo però una difficoltà: per poter usare l'articolo determinativo "il" è necessario sapere che, per ogni assegnato a , di numeri naturali k con la proprietà richiesta (cioè tali che esista un'applicazione biettiva $I_k \rightarrow a$) ce n'è al massimo uno.⁽²⁾ Questa difficoltà si supera: dimostreremo nella sezione 3 che le cose stanno effettivamente così, e questo ci permetterà di dare un senso preciso all'espressione 'numero di elementi' di un insieme finito. Come vedremo [più avanti](#), la stessa idea di sfruttare la nozione di applicazione biettiva, qui utilizzata per gli valutare il numero di elementi di insiemi finiti si può estendere al caso insiemi arbitrari.

⁽¹⁾e talvolta, per scorrevolezza, omettiamo "esattamente" e diciamo più semplicemente che a ha k elementi, frase di per sé un po' ambigua.

⁽²⁾ad esempio, se per un qualche insieme a esistessero sia un'applicazione biettiva $I_{114} \rightarrow a$ che un'applicazione biettiva $I_{127} \rightarrow a$, allora, nel senso appena definito, a avrebbe sia esattamente 127 che esattamente 114 elementi.

2. IL PRINCIPIO DI BUON ORDINAMENTO PER I NATURALI ED IL PRINCIPIO DI INDUZIONE

Come detto all'inizio, assumiamo come noti l'insieme $\mathbb{N}$ dei numeri naturali ed alcune operazioni elementari in esso definite. In aggiunta, assumiamo di conoscere anche la relazione binaria $\leq$ (ordinamento usuale) in $\mathbb{N}$, con le sue proprietà che la qualificano come relazione d'ordine (per ogni $a, b, c \in \mathbb{N}$, $a \leq a$, $a \leq b \leq a \Rightarrow a = b$, $a \leq b \leq c \Rightarrow a \leq c$)⁽³⁾. Un'ulteriore, importantissima, proprietà è stabilita dal *principio di buon ordinamento dei naturali*:

ogni parte non vuota di $\mathbb{N}$ ha minimo.

Questa affermazione significa precisamente che per ogni parte non vuota X di $\mathbb{N}$ esiste $a \in X$ tale che $\forall x \in X (a \leq x)$. Tale a , che si vede facilmente essere unico,⁽⁴⁾ si chiama, appunto, il *minimo* di X e si indica come $\min X$. Un'altra ben nota proprietà della relazione binaria $\leq$, il fatto che per ogni $a, b \in \mathbb{N}$ vale $(a \leq b \vee b \leq a)$ (che, unitamente alle precedenti, qualifica $\leq$ come relazione d'ordine *totale*) segue come conseguenza dal principio del buon ordinamento: se $a, b \in \mathbb{N}$ e $X = \{a, b\}$ allora uno tra a e b è il minimo di X ; se $a = \min X$ allora $a \leq b$, se $b = \min X$ allora $b \leq a$.

2.1. Dimostrazioni per controesempio minimo. Il principio di buon ordinamento dei naturali rende disponibile un metodo molto potente per dimostrare proprietà relative ai numeri naturali, il metodo di dimostrazione *per controesempio minimo*. Informalmente, si tratta di questo: supponiamo che, per un qualche insieme N di numeri naturali, vogliamo provare che tutti gli elementi di N soddisfino una certa proprietà (P). Per farlo possiamo ragionare per assurdo, supponendo che ciò sia falso e che quindi esista qualche elemento di N che non soddisfa (P) (un cosiddetto *controesempio*). Allora l'insieme degli elementi di N che non soddisfano (P) è una parte non vuota di $\mathbb{N}$, quindi ha minimo (il cosiddetto controesempio minimo), chiamiamolo m . In molti casi, dal fatto che questo m non solo non verifica (P) ma ha la proprietà aggiuntiva che tutti gli elementi di N minori di esso verificano (P) è possibile trarre una contraddizione. Se ci riusciamo, questa contraddizione completa la nostra dimostrazione: abbiamo provato che assumere che qualche elemento di N non verifichi (P) porta ad una contraddizione e quindi possiamo concludere che ogni elemento di N verifica (P).

In modo più formale possiamo riassumere quanto appena detto in questo modo: se φ è un predicato unario, la negazione della formula $\forall n \in N (\varphi(n))$ si può rendere come $\exists n \in N (\neg \varphi(n))$ ovvero, in termini insiemistici, a $C \neq \emptyset$ se si è posto $C = \{n \in N \mid \neg \varphi(n)\}$. Ma il principio di buon ordinamento dei naturali garantisce che $C \neq \emptyset$ equivale a $\exists \min C$, cioè alla formula

$$\exists m \in N (\neg \varphi(m) \wedge \forall n \in N (n < m \Rightarrow \varphi(n))). \quad (\text{ECM})$$

In sintesi, questa formula (ECM) è equivalente alla negazione di $\forall n \in N (\varphi(n))$; provare che essa è falsa equivale a provare che vale $\forall n \in N (\varphi(n))$. Nei termini della precedente presentazione informale, φ è il predicato che esprime la proprietà (P) (nel senso che $\varphi(n)$ è la formula che esprime la frase: n verifica (P)) e C è l'insieme dei controesempi, quindi la formula (ECM) afferma che Esiste il Controesempio Minimo all'assunzione che tutti gli elementi di N verificano (P).

Un esempio di dimostrazione per controesempio minimo è nell'appendice (sottosezione 7.1, proposizione 36).

2.2. Principio di induzione e di induzione completa. Casi particolari di dimostrazioni per controesempio minimo sono le diverse forme di dimostrazioni per induzione. Per discuterle, fissiamo (temporaneamente) una notazione: per ogni $b \in \mathbb{N}$ poniamo $N_b = \{n \in \mathbb{N} \mid b \leq n\}$. Presentiamo qui due versioni del principio di induzione.

Teorema 1 (Principio di induzione). *Sia φ un predicato unario e sia $b \in \mathbb{N}$. Allora:*

$$\left(\varphi(b) \wedge \left(\forall n \in N_b (\varphi(n) \Rightarrow \varphi(n+1)) \right) \right) \Rightarrow \left(\forall n \in N_b (\varphi(n)) \right)$$

Teorema 2 (Principio di induzione completa). *Sia φ un predicato unario e sia $b \in \mathbb{N}$. Allora:*

$$\left(\forall n \in N_b \left(\left(\forall i \in N_b (i < n \Rightarrow \varphi(i)) \right) \Rightarrow \varphi(n) \right) \right) \Rightarrow \left(\forall n \in N_b (\varphi(n)) \right)$$

Questi due principi sono anche noti, nell'ordine, come principio di induzione nella prima e nella seconda forma. Prima di giustificarli, proviamo ad darne una illustrazione informale. Il primo dei due è estremamente intuitivo. L'idea che esprime è che se una certa proprietà (P) (che consideriamo essere espressa dal predicato φ) è verificata dal numero b e, per ogni intero n maggiore o uguale a b , se n verifica (P) anche il numero successivo $n+1$ verifica (P), allora (P) vale per tutti gli interi maggiori o uguali a b . Una metafora molto chiara è questa: se suppongo di avere una scala con infiniti gradini, numerati in ordine ascendente dai numeri interi positivi (il primo gradino, il secondo, il terzo e così via), se so di poter raggiungere il primo gradino e per ciascun gradino raggiunto so di poter salire al gradino successivo, allora so di poter raggiungere tutti i gradini. Oppure: se è data una pila formata da infiniti mattoncini, poggiati ordinatamente l'uno sull'altro, se so che un certo mattoncino (il b -esimo) è di colore rosso e so

⁽³⁾come di consueto, scritture come $a \leq b \leq c$ abbreviano $a \leq b \wedge b \leq c$

⁽⁴⁾se anche b è un elemento di X che gode della stessa proprietà: $\forall x \in X (b \leq x)$, allora $a \leq b$ per la proprietà attribuita ad a e perché $b \in X$ e, simmetricamente, $b \leq a$ per la proprietà analoga attribuita a b e perché $a \in X$. Ma da $a \leq b \leq a$ segue $a = b$

che ogni mattoncino poggiato immediatamente sopra un mattoncino rosso deve essere necessariamente rosso, allora so che tutti i mattoncini dal b -esimo in su sono rossi.

Si usa chiamare dimostrazione per induzione una dimostrazione che usi il teorema 1⁽⁵⁾ per provare una formula come $\forall n \in N_b(\varphi(n))$. Per completare la dimostrazione è dunque sufficiente provare (1): la cosiddetta ‘base d’induzione’, cioè la formula $\varphi(b)$ (talvolta ci si riferisce anche al numero b come alla ‘base d’induzione’) e (2): per ogni $n \in N_b$, l’implicazione $\varphi(n) \Rightarrow \varphi(n+1)$, anche detta ‘passo induttivo’. Nel farlo, spesso, ci si riferisce all’antecedente $\varphi(n)$ del passo induttivo come alla ‘ipotesi d’induzione’. Ovviamente è essenziale per la buona riuscita ed esposizione di una dimostrazione per induzione riuscire a formulare in modo chiaro il predicato qui chiamato φ a cui la dimostrazione fa riferimento.

Il secondo principio (quello di induzione completa) è un po’ più complesso nella formulazione ma anche più potente del primo.⁽⁶⁾ Ciò che la formula esprime è che per stabilire che tutti i numeri interi maggiori o uguali ad un assegnato naturale b verificano una data proprietà (P) è sufficiente verificare che, qualsiasi sia il numero intero $n \geq b$, se tutti gli interi i tali che $b \leq i < n$ verificano (P) allora anche n verifica (P). Tornando alla metafora della pila di mattoncini: se so che è rosso ogni mattoncino M tale che siano rossi tutti i mattoncini posti più in basso di M , allora sono rossi tutti gli infiniti mattoncini della pila. Discorso analogo ma appena un po’ più complicato vale se si decide di ignorare i mattoncini che precedono il b -esimo tra essi, chiamiamolo B : per essere certi che tutti i mattoncini da B in su sono rossi basta sapere che ogni mattoncino da B in su sia rosso se sono rossi tutti i mattoncini che siano posti più in basso di questo ma non più in basso di B .

Passiamo alle dimostrazioni. Entrambi i principi si possono facilmente provare con una dimostrazione per controesempio minimo, vediamole.

Dimostrazione del teorema 1. Assumiamo l’antecedente dell’implicazione, cioè: assumiamo vera $\varphi(b)$ (la base di induzione) e, per ogni $n \in N_b$, l’implicazione $\varphi(n) \Rightarrow \varphi(n+1)$ (il passo induttivo). Supponiamo falso il conseguente $\forall n \in N_b(\varphi(n))$. Allora l’insieme $C = \{n \in N_b \mid \neg\varphi(n)\}$ non è vuoto ed esiste $m = \min C$. Poiché $m \in C$, sicuramente $\varphi(m)$ è falsa e quindi, essendo $\varphi(b)$ vera, $m \neq b$. Questo comporta $m > b$, cioè $m-1 \geq b$, ovvero $m-1 \in N_b$. Poiché $m-1 < m = \min C$, certamente $m-1 \notin C$. Ma allora, per definizione di C , vale $\varphi(m-1)$. Sostituendo $m-1$ ad n nel passo induttivo otteniamo che vale l’implicazione $\varphi(m-1) \Rightarrow \varphi(m)$, ma questa è una contraddizione perché abbiamo appena visto che $\varphi(m-1)$ è vera ma $\varphi(m)$ è falsa. Questa contraddizione è derivata dall’aver assunto falsa la formula $\forall n \in N_b(\varphi(n))$, che quindi è vera. $\square$

Dimostrazione del teorema 2. Per chiarezza, chiamiamo $\alpha(n)$ la formula $\forall i \in N_b (i < n \Rightarrow \varphi(i))$ e β la formula $\forall n \in N_b(\varphi(n))$, in modo che l’implicazione nell’enunciato, chiamiamola γ , sia $(\forall n \in N_b(\alpha(n) \Rightarrow \varphi(n))) \Rightarrow \beta$.

Se β è falsa, esiste il minimo $m \in N_b$ che non verifica φ , vale a dire: $m = \min C$, dove $C = \{n \in N_b \mid \neg\varphi(n)\}$. Ma allora $\varphi(i)$ è vera per ogni $i \in N_b$ tale che $i < m$, quindi $\alpha(m)$ è vera, ma $\varphi(m)$ è falsa, quindi l’antecedente in γ è falso e così γ è vera. $\square$

Troveremo in queste note molte dimostrazioni per induzione (nella prima forma), l’appendice ne contiene una (proposizione 37) che si consiglia di leggere come esempio iniziale. Per quanto riguarda il principio di induzione completa, quasi sempre risulta più semplice effettuare una dimostrazione per controesempio minimo piuttosto che usare esplicitamente il teorema 2, che ne è, in sostanza, una riformulazione.

3. BIETTIVITÀ, EQUIPOTENZA ED INSIEMI FINITI

Prima di entrare in argomento, ricordiamo due possibili costruzioni di applicazioni a partire da un’applicazione data. Se $f: a \rightarrow b$ è un’applicazione, c è una qualsiasi parte di a e d è una parte di b contenente $\text{im } f$ (che è il sottoinsieme $\{f(x) \mid x \in a\}$ di b), sono ben definite le applicazioni:

$$f|_c: x \in c \mapsto f(x) \in b; \quad f|_d: x \in a \mapsto f(x) \in d$$

che si chiamano, nell’ordine, la *restrizione* di f a c e la *ridotta* di f a d . Evidentemente $\text{im } f|_d = \text{im } f$, quindi una ed una sola delle ridotte di f è suriettiva: la ridotta all’immagine di f , cioè $f|_{\text{im } f}$, che viene anche indicata semplicemente con $f|$. Invece, se f è iniettiva, anche le restrizioni e le ridotte di f sono iniettive, dal momento che le immagini dei singoli elementi dei loro domini sono le immagini degli stessi elementi mediante f . Un’utile conseguenza di queste osservazioni è il prossimo lemma 3.

Prima di enunciarlo, ricordiamo che se $f: a \rightarrow b$ è un’applicazione, l’applicazione immagine definita da f è l’applicazione $\vec{f}: c \in \mathcal{P}(a) \mapsto \{f(x) \mid x \in c\} \in \mathcal{P}(b)$. Già che ci siamo richiamiamo anche l’applicazione antiimmagine definita da f , cioè $\check{f}: c \in \mathcal{P}(b) \mapsto \{x \in a \mid f(x) \in c\} \in \mathcal{P}(a)$.

Lemma 3. *Sia $f: a \rightarrow b$ un’applicazione iniettiva e sia c una parte di a . Allora la ridotta all’immagine della restrizione di f a c , cioè l’applicazione $x \in c \mapsto f(x) \in \vec{f}(c)$, è biettiva.*

⁽⁵⁾o anche, talvolta, il teorema 2.

⁽⁶⁾usando una terminologia non sviluppata in queste note, il principio di induzione ‘nella prima forma’ vale solo in insiemi ordinati isomorfi a quello dei naturali, o, in una opportuna riformulazione, a parti di questo. Invece il principio di induzione completa si può applicare in insiemi ordinati di tipo molto più generale: a tutti gli insiemi ben ordinati.

La dimostrazione è ovvia dalle considerazioni precedenti. Diciamo che l'applicazione biettiva g definita nel lemma è *indotta per restrizione* da f .

Se a e b sono insiemi (finiti o meno), si dice che a è *equipotente* a b se e solo se esiste un'applicazione biettiva $a \rightarrow b$. Ad esempio, il lemma precedente garantisce che se f è un'applicazione iniettiva ogni parte c del dominio di f è equipotente a $\vec{f}(c)$. Abbiamo:

Lemma 4. *Siano a, b e c insiemi. Allora:*

- (i) a è equipotente ad a ;
- (ii) se a è equipotente a b , allora b è equipotente ad a ;
- (iii) se a è equipotente a b e b è equipotente a c , allora a è equipotente ad c .⁽⁷⁾

Dimostrazione. L'applicazione identica di a , cioè $\text{id}_a: x \in a \mapsto x \in a$ è biettiva, quindi a è equipotente ad a . Se a è equipotente a b , esiste un'applicazione biettiva $f: a \rightarrow b$, allora l'inversa di f è un'applicazione biettiva $b \rightarrow a$, quindi b è equipotente ad a . Infine, se a è equipotente a b e b è equipotente a c , esistono applicazioni biettive $f: a \rightarrow b$ e $g: b \rightarrow c$, quindi $g \circ f$ è un'applicazione biettiva $a \rightarrow c$, sicché a è equipotente ad c . $\square$

La (ii) ci consente di usare in modo non ambiguo l'espressione ' a e b sono equipotenti' come sinonimo di ' a è equipotente a b ', o anche di ' b è equipotente ad a '.

La definizione di insieme finito data nella sezione introduttiva si può riformulare dicendo che un insieme è finito precisamente quando esista $n \in \mathbb{N}$ tale che a sia equipotente ad I_n . Affrontiamo ora la questione, a cui già si è accennato nella stessa sezione, dell'unicità di tale n ; farlo ci permetterà di definire in modo corretto e sensato la cardinalità (il "numero degli elementi") degli insiemi finiti.

Il risultato fondamentale è contenuto nel prossimo lemma.

Lemma 5. *Per ogni numero naturale n ed ogni $J \subset I_n$ non esistono applicazioni iniettive $I_n \rightarrow J$.*

Dimostrazione. La dimostrazione procede per induzione su n ; vale a dire utilizzando il teorema 1 con riferimento al predicato $\varphi(n)$: non esistono applicazioni iniettive di dominio I_n e codominio una parte propria di I_n . Se $n = 0$, l'insieme I_n è vuoto e quindi non ha sottoinsiemi propri; $\varphi(0)$ è dunque banalmente vera. Occupiamoci ora del passo induttivo. Sia $n \in \mathbb{N}$ ed assumiamo l'ipotesi d'induzione $\varphi(n)$; deduciamone $\varphi(n+1)$. Supponiamo, per assurdo, $\varphi(n+1)$ falsa; esistano dunque $J \subset I_{n+1}$ ed un'applicazione iniettiva $f: I_{n+1} \rightarrow J$. Consideriamo prima il caso in cui $n+1 \in \vec{f}(I_n)$. Allora esiste $i \in I_n$ tale che $f(i) = n+1$; sia τ la trasposizione di I_{n+1} che scambia tra loro i e $n+1$.⁽⁸⁾ Sia $g = f \circ \tau$. Allora g è un'applicazione iniettiva $I_{n+1} \rightarrow J$ e $g(n+1) = f(i) = n+1$. Dal momento che g è iniettiva, per ogni $j \in I_n$ si ha $g(j) \neq g(n+1) = n+1$, quindi $g(j) \in I_n$. Pertanto $\vec{g}(I_n) \subseteq I_n$. Nell'altro caso, quello in cui $n+1 \notin \vec{f}(I_n)$, poniamo invece $g = f$. In entrambi i casi esiste dunque un'applicazione iniettiva $g: I_{n+1} \rightarrow J$ tale che $n+1 \notin \vec{g}(I_n)$. Posto $J_1 = \vec{g}(I_n)$, allora $J_1 \subseteq J \cap I_n \subseteq I_n$. Sia h la ridotta di $g|_{I_n}$ a J_1 , cioè l'applicazione $x \in I_n \mapsto g(x) \in J_1$; per il lemma 3, h è biettiva. L'ipotesi d'induzione $\varphi(n)$ comporta che J_1 non può essere un sottoinsieme proprio di I_n , quindi $J_1 = I_n$. Poiché g è iniettiva, $g(n+1) \notin \vec{g}(I_n) = J_1 = I_n$, quindi $g(n+1) \in I_{n+1} \setminus I_n$, ovvero $g(n+1) = n+1$. Ovviamente $g(n+1) \in J$, quindi J contiene $J_1 \cup \{n+1\} = I_n \cup \{n+1\} = I_{n+1}$, dunque $J = I_{n+1}$. Questo contraddice la scelta iniziale di J ; la contraddizione così ottenuta mostra che $\varphi(n)$ implica $\varphi(n+1)$. A questo punto, per il teorema 1, l'asserto è dimostrato. $\square$

Corollario 6. *Se n ed m sono numeri naturali distinti, I_n e I_m non sono equipotenti*

Dimostrazione. Supponiamo, per assurdo, che esista un'applicazione biettiva $f: I_n \rightarrow I_m$. Se $m < n$, allora $I_m \subset I_n$, e questo contraddice il lemma 5. Se invece $n < m$ si può duplicare il ragionamento, scambiando i ruoli di f e di n con quelli di $f^{-1}: I_m \rightarrow I_n$ e di m . $\square$

Proposizione 7. *Per ogni insieme finito a esiste uno ed un solo $n \in \mathbb{N}$ tale che a ed I_n siano equipotenti.*

Dimostrazione. Per definizione, se a è finito esiste $n \in \mathbb{N}$ tale che a ed I_n siano equipotenti. Se $m \in \mathbb{N}$ ed a è equipotente anche a I_m , allora, in conseguenza del lemma 4, I_n ed I_m sono equipotenti tra loro. Il corollario 6 mostra però che questo è possibile solo se $m = n$. $\square$

Con questa proposizione abbiamo provato che è possibile dare una definizione corretta e non ambigua del 'numero degli elementi' di un insieme finito: quella che è stata anticipata nella sezione introduttiva. Facciamolo:

Definizione. Si chiama *cardinalità* (o *numero degli elementi*) di un insieme finito a quell'unico $n \in \mathbb{N}$ tale che I_n sia equipotente ad a . La cardinalità di a viene indicata col simbolo⁽⁹⁾ $|a|$.

Come di abitudine che sicuramente chi legge già ha, si usano espressioni come "insieme di n elementi" per riferirsi ad un insieme di cardinalità n . Ovviamente $|I_n| = n$; inoltre possiamo dedurre dal lemma 4 il:

⁽⁷⁾ con la terminologia delle relazioni binarie, questo lemma stabilisce che, in qualunque insieme, la relazione di equipotenza è una relazione di equivalenza.

⁽⁸⁾ dunque: τ è l'applicazione $I_{n+1} \rightarrow I_{n+1}$ definita da $\tau(i) = n+1$, $\tau(n+1) = i$ e $\tau(x) = x$ per ogni $x \in I_{n+1} \setminus \{i, n+1\}$. Poiché $\tau \circ \tau = \text{id}_{I_{n+1}}$, τ è biettiva.

⁽⁹⁾ purtroppo lo stesso utilizzato per il valore assoluto di un numero reale; cercare di evitare di confondersi.

Corollario 8. Se a e b sono insiemi finiti, a e b sono equipotenti se e solo se $|a| = |b|$.

Dimostrazione. Poniamo $n = |a|$ e $m = |b|$. Se $n = m$, sia a che b sono equipotenti a I_n , quindi sono equipotenti tra loro, per il lemma 4 (iii). Viceversa, se a e b sono equipotenti, poiché a è equipotente a I_n e b lo è a I_m , applicando due volte lo stesso lemma abbiamo che I_n e I_m sono equipotenti, quindi $n = m$ per il corollario 6. $\square$

Possiamo già dimostrare un risultato importante, caratteristico degli insiemi finiti.

Teorema 9. Siano a e b insiemi finiti equipotenti e sia f un'applicazione da a a b . Sono allora equivalenti:

- (i) f è iniettiva;
- (ii) f è biettiva;
- (iii) f è suriettiva.

Dimostrazione. Posto $n = |a|$, esiste un'applicazione biettiva $\alpha: I_n \rightarrow a$; inoltre $n = |b|$, per ipotesi, quindi esiste anche un'applicazione biettiva $\beta: I_n \rightarrow b$. Se f è iniettiva, allora, è iniettiva anche $g := \beta^{-1} \circ f \circ \alpha: I_n \rightarrow I_n$. Posto $J = \text{im } g$, allora la ridotta di g a J è biettiva e quindi, $J = I_n$, vale a dire, g è biettiva, per il lemma 5. Ma da $g = \beta^{-1} \circ f \circ \alpha$ segue subito $f = \beta \circ g \circ \alpha^{-1}$, quindi dal fatto che g è biettiva segue che f è biettiva. Abbiamo provato che (i) implica (ii). Che (ii) implichi (iii) è ovvio; resta da provare che (iii) implica (i). Se f è suriettiva, f ha una sezione $s: b \rightarrow a$, e come tutte le sezioni s è iniettiva. Per la prima parte della dimostrazione (riferita alle applicazioni da b ad a), allora s è biettiva. Da $f \circ s = \text{id}_b$ segue allora $f = \text{id}_b \circ s^{-1}$, quindi f , in quanto composta tra due applicazioni biettive, è biettiva, quindi anche iniettiva. $\square$

Un caso particolare di questo teorema è il fatto che se a è un insieme finito, un'applicazione $a \rightarrow a$ è iniettiva se e solo se è suriettiva. Notare che questo è falso nel caso in cui a sia infinito; ad esempio l'applicazione $n \in \mathbb{N} \mapsto n + 1 \in \mathbb{N}$ è iniettiva ma non suriettiva, le sue retrazioni sono suriettive ma non iniettive.

4. UNIONI

La prima osservazione è estremamente intuitiva, forse la formalizzazione della dimostrazione è l'unica difficoltà che si possa incontrare nel discuterla.

Lemma 10. Siano a e b insiemi finiti. Se $a \cap b = \emptyset$, allora $|a \cup b| = |a| + |b|$.

Dimostrazione. Siano $n = |a|$ e $m = |b|$. Esistono applicazioni biettive $\alpha: a \rightarrow I_n$ e $\beta: b \rightarrow I_m$, le possiamo usare per costruire l'applicazione:

$$f: x \in a \cup b \mapsto \begin{cases} \alpha(x) & \text{se } x \in a \\ n + \beta(x) & \text{se } x \in b \end{cases} \in I_{n+m}.$$

Ovviamente f è bene definita, perché per ogni $x \in a \cup b$ si verifica esattamente una tra $x \in a$ e $x \in b$. È facile verificare che f è biettiva; per farlo basta mostrare che per ogni $i \in I_{n+m}$ esiste uno ed un solo $x \in a \cup b$ tale che $f(x) = i$. Osserviamo innanzitutto che, per ogni $x \in a \cup b$, si ha $f(x) \leq n$ se $x \in a$ e $f(x) > n$ se $x \in b$. Sia $i \in I_{n+m}$. Se $i \leq n$, cioè $i \in I_n$, allora, poiché α è biettiva, esiste uno ed un solo $x \in a$ tale che $f(x) = \alpha(x) = i$, mentre $f(x) \neq i$ per ogni $x \in b$. Se invece $i > n$, allora $i - n \in I_m$ e, poiché β è biettiva, esiste uno ed un solo $x \in b$ tale che $\beta(x) = i - n$, cioè $f(x) = n + \beta(x) = i$, mentre $f(x) \neq i$ per ogni $x \in a$. Questo prova il nostro asserto. $\square$

Può essere utile, per comprenderla meglio, pensare a questa dimostrazione in termini di elencazione degli elementi di $a \cup b$. Come in qualche modo osservato nella prima sezione di queste note, fissare un'applicazione biettiva α da I_n ad a significa elencare (tutti) gli elementi di a in una lista senza ripetizioni e di lunghezza n : di questa lista $\alpha(1)$ è il primo elemento, $\alpha(2)$ il secondo, $\alpha(3)$ il terzo e così via, sino all'ultimo (ed n -esimo) $\alpha(n)$. La biiezione β fornisce un analogo elenco, di lunghezza m , degli elementi di b . Se concateniamo queste due liste, partendo da quella degli elementi di a (descritta da α) e facendola seguire da quella degli elementi di b (descritta da β) otteniamo una lista di lunghezza $n + m$ in cui appaiono tutti gli elementi di $a \cup b$ e che è ancora priva di ripetizioni, perché $a \cap b = \emptyset$. Questa lista è proprio quella descritta dall'applicazione biettiva f della dimostrazione.

Un caso particolarmente ovvio del lemma precedente è quello in cui a è una parte dell'insieme finito c e $b = c \setminus a$. Ovviamente in questo caso $c = a \cup b$ e $a \cap b = \emptyset$, quindi $|c| = |a| + |b|$, ovvero $|a| = |c| - |b|$, dunque $|a| \leq |c|$ e $|a| = |c|$ se e solo se $a = c$.⁽¹⁰⁾

Generalizziamo il lemma precedente alla situazione di una unione tra un numero arbitrario (ma comunque finito) di insiemi finiti tra loro disgiunti.

Proposizione 11. Sia F un insieme finito di insiemi finiti a due a due disgiunti.⁽¹¹⁾ Allora $|\bigcup F| = \sum_{a \in F} |a|$.

⁽¹⁰⁾d'accordo, si tratta di banalità, ma osservarle ha comunque un senso, soprattutto perché queste affermazioni possono essere false, o magari addirittura prive di senso, nel caso in cui gli insiemi coinvolti non siano finiti. Ad esempio, l'applicazione $n \in \mathbb{N} \mapsto n + 1 \in \mathbb{N}^* := \mathbb{N} \setminus \{0\}$ è biettiva, quindi $\mathbb{N}$ è equipotente alla sua parte propria $\mathbb{N}^*$.

⁽¹¹⁾questa espressione significa: $\forall a, b \in F (a \neq b \Rightarrow a \cap b = \emptyset)$.

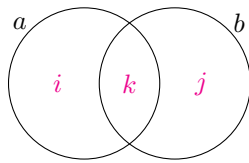
Dimostrazione. Procediamo per induzione su $|F|$. Questo significa che proviamo vera la formula $\forall n \in \mathbb{N}(\varphi(n))$ dove $\varphi(n)$ asserisce che vale $|\bigcup F| = \sum_{a \in F} |a|$ per ogni insieme F di cardinalità n costituito da insiemi finiti a due a due disgiunti. Se $|F| = 0$, allora $F = \emptyset$ e la l'uguaglianza richiesta, $|\bigcup F| = \sum_{a \in F} |a|$, vale perché $\bigcup \emptyset = \emptyset$ ha cardinalità 0 e la somma di interi estesa all'insieme vuoto (cioè con zero addendi) vale 0. Supponiamo, per un arbitrario $n \in \mathbb{N}$, che valga $\varphi(n)$. Se F è un insieme finito di insiemi finiti e $|F| = n + 1$, allora $F \neq \emptyset$ e possiamo fissare un suo elemento a . Allora $|F \setminus \{a\}| = n$ e gli elementi di $F \setminus \{a\}$ sono finiti e a due a due disgiunti, quindi, se poniamo $b = \bigcup(F \setminus \{a\})$, per ipotesi di induzione $|b| = \sum_{c \in b} |c|$. Chiaramente $\bigcup F = a \cup b$, inoltre $a \cap b = \emptyset$ per ogni $c \in b$, quindi $a \cap b = \bigcup_{c \in b} (a \cap c) = \emptyset$ e così, per il lemma 10, $|\bigcup F| = |a \cup b| = |a| + |b| = |a| + \sum_{c \in b} |c| = \sum_{c \in F} |c|$. Ciò mostra che, assunta vera $\varphi(n)$, vale anche $\varphi(n + 1)$; a questo punto la dimostrazione è completa. $\square$

Un esempio di applicazione:

Proposizione 12. Siano a e b insiemi finiti. Allora $|a \times b| = |a| |b|$.

Dimostrazione. Per ogni $x \in a$, sia $b_x = \{x\} \times b$; dovrebbe essere chiaro che l'applicazione $y \in b \mapsto (x, y) \in b_x$ è biettiva, quindi $|b_x| = |b|$. Inoltre, posto $F = \{b_x \mid x \in a\}$, si ha $\bigcup F = a \times b$. Per ogni $u, v \in a$, se $u \neq v$ allora $b_u \cap b_v = \emptyset$ (infatti gli elementi di b_u hanno prima coordinata u , quelli di b_v hanno prima coordinata v , quindi nessuna coppia può appartenere ad entrambi gli insiemi se $u \neq v$). Di conseguenza, la proposizione 11 garantisce che $|a \times b|$ è la somma delle cardinalità degli elementi di F . Ora, ciascuno degli elementi b_x di F ha cardinalità $|b|$, quindi questa somma è $|F| |b|$. Infine, l'applicazione $x \in a \mapsto b_x \in F$ è ovviamente suriettiva, e se $b \neq \emptyset$ essa è anche iniettiva (perché come detto sopra, se u e v sono elementi distinti di a si ha $b_u \cap b_v = \emptyset$, e quindi $b_u \neq b_v$ se $b \neq \emptyset$, perché in questo caso $b_u \neq \emptyset \neq b_v$). Dunque, se $b \neq \emptyset$ abbiamo $|a| = |F|$ e quindi $|a \times b| = |F| |b| = |a| |b|$; se $b = \emptyset$ si ha $a \times b = \emptyset$ e $|a| |b| = 0$, quindi anche in questo caso $|a \times b| = |a| |b|$. $\square$

4.1. Il principio di inclusione-esclusione. Torniamo al calcolo del numero degli elementi dell'unione $a \cup b$ tra due insiemi finiti a e b discusso nel lemma 10 nell'ipotesi che a e b siano tra loro disgiunti. Come è facile intuire, il risultato non sarà (necessariamente) lo stesso se quest'ultima ipotesi viene rimossa, cioè se ammettiamo la possibilità che $a \cap b$ non sia vuoto. Vediamo come. Poniamo $i = |a \setminus b|$, $j = |b \setminus a|$ e $k = |a \cap b|$. Dal momento che $a \setminus b$ e $a \cap b$ sono certamente disgiunti, segue dal lemma 10 che $a = (a \setminus b) \cup (a \cap b)$ ha esattamente $i + k$ elementi; similmente $|b| = j + k$. Infine, poiché $a \cup b = (a \setminus b) \cup b$ e $(a \setminus b) \cap b = \emptyset$, abbiamo $|a \cup b| = |a \setminus b| + |b| = i + j + k$. Possiamo rappresentare la situazione col diagramma di Venn in basso a sinistra, in cui le lettere in colore indicano il numero degli elementi nella porzione di diagramma in cui si trovano:



$$\begin{array}{ll} |a \setminus b| = i & |a| = i + k \\ |a \cap b| = k & |b| = j + k \\ |b \setminus a| = j & |a \cup b| = i + j + k \end{array}$$

Come si legge facilmente dalla colonna di destra, $|a \cup b| = |a| + |b| - k = |a| + |b| - |a \cap b|$. Abbiamo così provato:

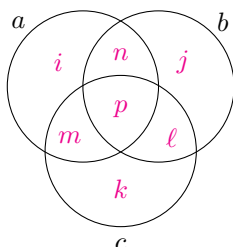
Lemma 13. Siano a e b insiemi finiti. Allora $|a \cup b| = |a| + |b| - |a \cap b|$.

È utile visualizzare questo risultato anche come conseguenza di un'argomentazione simile a quella esposta a proposito del lemma 10: se desideriamo compilare una lista degli elementi di $a \cup b$ possiamo elencare prima i $|a|$ elementi di a e, a seguire, i $|b|$ elementi di b . Nella lista così ottenuta abbiamo così $|a| + |b|$ voci; in essa, però, mentre gli elementi di $a \setminus b$ e quelli di $b \setminus a$ appaiono esattamente una volta ciascuno, i k elementi di $a \cap b$ appaiono due volte ciascuno. Dunque, per ottenere una lista priva di ripetizioni (in cui appaiano però tutti gli elementi di $a \cup b$), di ciascuno dei k elementi di $a \cap b$ va cancellata una delle due occorrenze nella lista. A questo punto la lista avrà lunghezza $|a| + |b| - k$ ed in essa apparirà, una volta ciascuno, ogni elemento di $a \cup b$ quindi, ancora, $|a \cup b| = |a| + |b| - |a \cap b|$.

Esempio 14. Siano a e b insiemi tali che $|a| = 15$ e $b = 12$. Allora, applicando il lemma 13 vediamo che:

- se $|a \cap b| = 7$, allora $|a \cup b| = 15 + 12 - 7 = 20$;
- se $|a \cup b| = 23$, allora $|a \cap b| = |a| + |b| - |a \cup b| = 15 + 12 - 23 = 4$;
- supponiamo di sapere che a e b sono entrambi parti di un insieme c di cardinalità 25. Allora $a \cup b \subseteq c$, quindi $|a \cup b| \leq 25$ e così $|a \cap b| = |a| + |b| - |a \cup b| \geq 15 + 12 - 25 = 2$.

Occupiamoci ora dell'unione tra tre insiemi finiti. Come nel caso precedente, facciamo riferimento ad un diagramma di Venn con indicazione delle cardinalità:



$$\begin{array}{ll} |a \setminus (b \cup c)| = i & |(b \cap c) \setminus a| = \ell \\ |b \setminus (a \cup c)| = j & |(a \cap c) \setminus b| = m \\ |c \setminus (a \cup b)| = k & |(a \cap b) \setminus c| = n \\ & |a \cap b \cap c| = p \\ |a \cup b \cup c| = i + j + k + \ell + m + n + p \end{array}$$

Ragionando come fatto per una coppia di insiemi, se elenchiamo gli elementi di a , poi quelli di b e poi quelli di c otteniamo una lista di lunghezza $|a| + |b| + |c|$ con, però, possibili ripetizioni. Infatti, ad esempio, gli elementi di $a \cap b$ sono stati inseriti nella lista sia elencando gli elementi di a che quelli di b ; simile discorso vale per gli elementi di $a \cap c$ e di $b \cap c$. Potremmo allora pensare di correggere il risultato descrivendo $|a \cup b \cup c|$ in questo modo: conteggiamo separatamente gli elementi di a , di b e di c , poi al numero $|a| + |b| + |c|$ così ottenuto sottraiamo $|a \cap b|$, perché gli elementi in $a \cap b$ sono stati conteggiati (almeno) due volte, e, per il motivo analogo, sottraiamo poi anche $|a \cap c|$ e $|b \cap c|$. Otteniamo così $|a| + |b| + |c| - (|a \cap b| + |a \cap c| + |b \cap c|)$. Ma, a ben vedere, anche questo numero non è, in generale, corretto, nel senso che non è necessariamente uguale a $|a \cup b \cup c|$. Infatti, con la procedura seguita sino a questo punto, abbiamo contato una (sola) volta gli i elementi di $a \setminus (b \cup c)$, e lo stesso vale per i $j + k$ elementi appartenenti a $b \setminus (a \cup c)$ o a $c \setminus (a \cup b)$; per dirla informalmente abbiamo conteggiato ciascuno degli n elementi di $(a \cap b) \setminus c$ due volte “in positivo” (una volta come elemento di a , una come elemento di b) ed una “in negativo”, come elemento di $a \cap b$ (abbiamo infatti sottratto $|a \cap b|$), questi stessi n elementi non appartengono a c né, a maggior ragione, ad $a \cap c$ o $b \cap c$ e quindi, complessivamente, hanno contribuito al calcolo di $|a| + |b| + |c| - (|a \cap b| + |a \cap c| + |b \cap c|)$ per una unità ciascuno, come desiderato. Lo stesso vale per gli elementi di $(a \cap b) \setminus c$ o di $(b \cap c) \setminus a$. I conti non tornano invece per i p elementi di $a \cap b \cap c$. Se x è uno di essi, infatti, x appartiene sia ad a che a b che a c e quindi è conteggiato tre volte “in positivo” nel calcolo di $|a| + |b| + |c|$, ma appartiene anche ad $a \cap b$, $a \cap c$ e $b \cap c$, quindi viene conteggiato tre volte “in negativo” nel calcolo di $-(|a \cap b| + |a \cap c| + |b \cap c|)$; dà così contributo nullo al calcolo di $|a| + |b| + |c| - (|a \cap b| + |a \cap c| + |b \cap c|)$. In definitiva, gli elementi di $(a \cup b \cup c) \setminus (a \cap b \cap c)$ danno ciascuno contributo 1 al calcolo di $|a| + |b| + |c| - (|a \cap b| + |a \cap c| + |b \cap c|)$, quelli di $a \cap b \cap c$ invece non vi contribuiscono. Abbiamo così $|a| + |b| + |c| - (|a \cap b| + |a \cap c| + |b \cap c|) = |(a \cup b \cup c) \setminus (a \cap b \cap c)|$; per far tornare i conti bisogna allora aggiungere $p = |a \cap b \cap c|$ al primo membro per ottenere $|a \cup b \cup c|$. Abbiamo così il risultato del prossimo lemma, che dimostriamo però anche in forma meno intuitiva ma più schematica.

Lemma 15. *Siano a, b e c insiemi finiti. Allora $|a \cup b \cup c| = |a| + |b| + |c| - |a \cap b| - |a \cap c| - |b \cap c| + |a \cap b \cap c|$.*

Dimostrazione. Facendo riferimento alle notazioni nel diagramma di Venn precedente, ed utilizzando per l'ultimo passaggio la proposizione 11, abbiamo

$$\begin{aligned} |a| &= i + m + n + p & |a \cap b| &= n + p \\ |b| &= j + \ell + n + p & |a \cap c| &= m + p \\ |c| &= k + \ell + m + p & |b \cap c| &= \ell + p. \end{aligned}$$

Allora,

$$\begin{aligned} &|a| + |b| + |c| - |a \cap b| - |a \cap c| - |b \cap c| + |a \cap b \cap c| \\ &= (i + m + n + p) + (j + \ell + n + p) + (k + \ell + m + p) \\ &\quad - (n + p) - (m + p) - (\ell + p) + p \\ &= i + j + k + \ell + m + n + p = |a \cup b \cup c|. \end{aligned}$$

□

I lemmi 13 e 15 sono i primi due casi significativi di un risultato più generale, noto come *principio di inclusione-esclusione*, che permette di esprimere la cardinalità delle unioni finite tra insiemi finiti. In queste note non viene fornita una dimostrazione di questo principio se non nei due casi già visti; ci si limiterà ad enunciarlo. Siano n un intero positivo e $a_1, a_2, \dots, a_n$ insiemi finiti; per comodità di notazione poniamo $I = I_n$. Per ogni sottoinsieme non vuoto J di I chiamiamo λ_J il numero $(-1)^{|J|-1} |\bigcap_{i \in J} a_i|$. Come va letta questa espressione? Se J ha un numero dispari di elementi $(-1)^{|J|-1}$ vale 1, altrimenti $(-1)^{|J|-1} = -1$. Dunque λ_J si calcola contando gli elementi dell'intersezione $\bigcap_{i \in J} a_i$ tra i vari insiemi a_i al variare di $i \in J$; se $|J|$ è dispari λ_J è il numero di questi elementi, altrimenti, se $|J|$ è pari, λ_J è l'opposto di questo numero. Ad esempio, se $n = 4$ e $J = \{1, 3\}$, allora $\lambda_J = -|a_1 \cap a_3|$ (perché $|J| = 2$ è pari), se $J = \{1, 3, 4\}$, invece $\lambda_J = |a_1 \cap a_3 \cap a_4|$, perché ora $|J|$ è dispari. Il principio di inclusione-esclusione afferma che, con queste notazioni, l'unione tra gli insiemi a_i ha per cardinalità la somma tra gli interi λ_J :

$$\left| \bigcup_{i \in I} a_i \right| = \sum_{\emptyset \neq J \subseteq I} \lambda_J.$$

Ad esempio, se assumiamo $n = 2$, le parti non vuote di $I = \{1, 2\}$ sono $\{1\}$, $\{2\}$ e I , ed otteniamo $\lambda_{\{1\}} = |a_1|$, $\lambda_{\{2\}} = |a_2|$ e $\lambda_I = -|a_1 \cap a_2|$, da cui $|a_1 \cup a_2| = \lambda_{\{1\}} + \lambda_{\{2\}} + \lambda_I = |a_1| + |a_2| - |a_1 \cap a_2|$, in accordo col lemma 13. Chi legge può effettuare l'analoga verifica per il caso $n = 3$, ritrovando così il lemma 15.

I più temerari tra i lettori possono preferire esprimere la stessa formula, senza introdurre i numeri λ_J , in questo modo:

$$\left| \bigcup_{i \in I} a_i \right| = \sum_{i=1}^n (-1)^{i-1} \left(\sum_{J \in \mathcal{P}_i(I)} \left| \bigcap_{i \in J} a_i \right| \right),$$

dove, si ricorda, il simbolo $\mathcal{P}_i(I)$ indica l'insieme delle parti di I di cardinalità i .

Detto in modo molto meno preciso e piuttosto ambiguo, ma forse più facile da ricordare, il principio afferma che se $a_1, a_2, \dots, a_n$ sono insiemi finiti allora la cardinalità della loro unione si ottiene con questa procedura: si sommano tra loro le cardinalità dei singoli insiemi a_i , a questa somma si sottrae la somma di tutte le cardinalità

delle intersezioni tra gli insiemi a_i presi ‘a due a due’ (cioè le cardinalità delle intersezioni $a_i \cap a_j$, per i possibili valori distinti di i e j , ovviamente contando una sola volta $|a_i \cap a_j|$ e $|a_j \cap a_i|$; questa somma si può anche scrivere come $\sum_{1 \leq i < j \leq n} |a_i \cap a_j|$), si aggiunge poi la somma di tutte le cardinalità delle intersezioni tra gli insiemi a_i presi ‘a tre a tre’ e si prosegue in questo modo, alternando i segni, sino ad arrivare ad aggiungere (se n è dispari) o sottrarre (se n è pari) $|a_1 \cap a_2 \cap \dots \cap a_n|$.

Esempio 16. Siano dati gli insiemi finiti a, b, c e d . Utilizzando il principio di inclusione-esclusione possiamo esprimere la cardinalità di $a \cup b \cup c \cup d$ come:

$$\begin{aligned} |a \cup b \cup c \cup d| &= |a| + |b| + |c| + |d| \\ &\quad - (|a \cap b| + |a \cap c| + |a \cap d| + |b \cap c| + |b \cap d| + |c \cap d|) \\ &\quad + (|a \cap b \cap c| + |a \cap b \cap d| + |a \cap c \cap d| + |b \cap c \cap d|) \\ &\quad - |a \cap b \cap c \cap d|. \end{aligned}$$

5. CONTARE APPLICAZIONI

Siano, ancora, a e b insiemi finiti. Illustriamo qui un procedimento che permette di calcolare il numero delle applicazioni da a a b , ed anche di contare quelle, tra esse, che verificano condizioni limitative di vario genere.

Prima di farlo, anche se non è strettamente necessario, perché lo stesso risultato può essere ricavato come conseguenza di quelli che seguono, in particolare della proposizione 20, osserviamo come l’esistenza o meno di applicazioni iniettive, suriettive, biettive tra due assegnati insiemi finiti dipende solo dalle cardinalità di questi. Ancora prima, stabiliamo quando è che esistono applicazioni tra due dati insiemi (non necessariamente finiti). Ricordiamo che $\text{Map}(a, b)$ è l’insieme di tutte le applicazioni da a a b .

Lemma 17. Siano a e b insiemi. Allora $\text{Map}(a, b) = \emptyset$ se e solo se $a \neq \emptyset = b$.

Dimostrazione. Se $b \neq \emptyset$ esiste un elemento $y \in b$ e, qualunque sia a , esiste quindi l’applicazione costante $x \in a \mapsto y \in b$ definita da y . Se $a = \emptyset = b$, l’applicazione identica di $\emptyset$ è un’applicazione $a \rightarrow b$. In questi casi, dunque, esistono applicazioni da a a b , vale a dire: $\text{Map}(a, b) \neq \emptyset$. Nel caso rimanente, cioè quello in cui $a \neq \emptyset = b$, allora a ha almeno un elemento x e non esistono applicazioni da a a b , perché se ne esistesse una, chiamiamola f , dovrebbe esistere in b l’immagine $f(x)$ di x , cosa impossibile perché $b = \emptyset$. $\square$

Teorema 18. Siano a e b insiemi finiti. Allora:

- (i) esistono applicazioni iniettive $a \rightarrow b$ se e solo se $|a| \leq |b|$;
- (ii) esistono applicazioni suriettive $a \rightarrow b$ se e solo se $|a| \geq |b|$ e $|b| = 0 \Rightarrow |a| = 0$;
- (iii) esistono applicazioni biettive $a \rightarrow b$ se e solo se $|a| = |b|$.

Dimostrazione. Già conosciamo (iii), che è una riformulazione del corollario 8.

Verifichiamo (i). Se esiste un’applicazione iniettiva $f: a \rightarrow b$, allora la ridotta di f all’immagine è un’applicazione biettiva da a ad $\text{im } f$, che è contenuto in b , quindi $|a| = |\text{im } f| \leq |b|$. Viceversa, supponiamo $|a| \leq |b|$. Esistono (e fissiamo) applicazioni biettive $\alpha: I_{|a|} \rightarrow a$ e $\beta: I_{|b|} \rightarrow b$. Poiché $|a| \leq |b|$, vale $I_{|a|} \subseteq I_{|b|}$ ed esiste l’applicazione immersione $\iota: I_{|a|} \hookrightarrow I_{|b|}$, ovviamente iniettiva. Di conseguenza l’applicazione $\beta \circ \iota \circ \alpha^{-1}: a \rightarrow b$, composta tra applicazioni iniettive,

$$a \xrightarrow{\alpha^{-1}} I_n \xrightarrow{\iota} I_m \xrightarrow{\beta} b,$$

è iniettiva. Quindi esiste un’applicazione iniettiva $a \rightarrow b$. Con questo, (i) è dimostrata.

Per provare (ii) osserviamo che se esiste un’applicazione suriettiva $a \rightarrow b$ allora quest’applicazione avrà una sezione, che è un’applicazione $b \rightarrow a$ e, come ogni sezione, è iniettiva. Allora, per la parte (i) di questo teorema, $|a| \geq |b|$. Inoltre, per il lemma 17, se $|b| = 0$ (cioè $b = \emptyset$), allora $a = \emptyset$ (cioè $|a| = 0$). Ciò prova che la condizione indicata nell’enunciato è necessaria. Viceversa, se $|a| \geq |b|$ esiste, ancora per (i), un’applicazione iniettiva $f: b \rightarrow a$, e se inoltre $|b| = 0 \Rightarrow |a| = 0$, allora f ha una retrazione, quindi un’applicazione suriettiva $a \rightarrow b$. $\square$

Procediamo ora con i conteggi. Iniziamo dal calcolo di $|\text{Map}(a, b)|$ per insiemi finiti a a b . L’idea che sta dietro il calcolo è questa: per definire un’applicazione f da a a b quello che serve è definire l’immagine $f(x)$ per ciascun elemento di a . Se $n = |a|$ e $x_1, x_2, \dots, x_n$ sono (tutti) gli elementi di a , per farlo possiamo scegliere un elemento y_1 di b che sia l’immagine $f(x_1)$ di x_1 , e per questo abbiamo $|b|$ possibili scelte a disposizione (ciascun elemento di b può essere scelto come y_1), poi scegliere un elemento y_2 di b (ed abbiamo ancora $|b|$ possibili elementi tra cui scegliere) che sia l’immagine di x_2 , un elemento y_3 di b che sia l’immagine di x_3 e così via, sino ad arrivare alla scelta dell’immagine y_n di x_n . Quante scelte, complessivamente, abbiamo a disposizione? A ciascuna delle possibili scelte di y_1 possiamo abbinare una delle possibili scelte di y_2 , se ci limitiamo a questi primi due passi, cioè solo alla scelta di immagini per x_1 e x_2 , vediamo che stiamo in effetti scegliendo una coppia ordinata (y_1, y_2) di elementi di b tra tutte quelle possibili, cioè tra gli elementi di $b \times b$. Siccome sappiamo (proposizione 12) che $|b \times b| = |b|^2$, abbiamo $|b|^2$ possibili scelte per le immagini dei primi due elementi x_1 e x_2 di a (in linguaggio insiemistico, effettuare questa scelta significa scegliere la restrizione di f ad $\{x_1, x_2\}$). Se $n > 2$, proseguiamo in modo simile: a ciascuna delle $|b|^2$ possibili scelte della coppia ordinata (y_1, y_2) abbiniamo una delle possibili $|b|$ scelte per y_3 : complessivamente, dunque, selezionare le immagini per x_1, x_2 e x_3 , cioè la restrizione di f ad $\{x_1, x_2, x_3\}$ significa di selezionare una terna ordinata di elementi di b , cioè un elemento in $(b \times b) \times b$; sempre per la proposizione 12 questo insieme

ha $|b|^3$ elementi, quindi abbiamo $|b|^3$ possibili scelte per le immagini dei primi tre elementi di a . Proseguendo allo stesso modo, scopriamo che, per ogni $i \in I_n$ abbiamo $|b|^i$ possibili scelte per le immagini dei primi i elementi di a . Vediamo così che le possibili scelte per le immagini $y_1, y_2, \dots, y_n$ degli n elementi di a sono in tutto $|b|^n$, quindi altrettante sono le applicazioni da a a b .

Chiarita l'idea, formalizziamo ora l'enunciato e la sua dimostrazione in modo più preciso.

Proposizione 19. *Siano a e b insiemi finiti. Allora $|\text{Map}(a, b)| = |b|^{|a|}$.*

Dimostrazione. Chiamiamo φ il predicato unario che, interpretato per un qualsiasi numero naturale n , afferma che scelti comunque insiemi finiti a e b si ha $|a| = n \Rightarrow |\text{Map}(a, b)| = |b|^n$. L'enunciato allora afferma esattamente questo: $\forall n \in \mathbb{N}(\varphi(n))$, formula che possiamo provare per induzione.

Dal momento che $|a| = 0$ equivale ad $a = \emptyset$, e $m^0 = 1$ per ogni numero naturale m ,⁽¹²⁾ la formula $\varphi(0)$ afferma che, per ogni insieme finito b , $|\text{Map}(\emptyset, b)| = 1$, la qual cosa è vera perché l'unica applicazione da $\emptyset$ ad un (qualsiasi) insieme b è quella con grafico vuoto. È così verificata la base d'induzione. Passo induttivo: sia $n \in \mathbb{N}$, assumiamo che valga $\varphi(n)$ e proviamo $\varphi(n+1)$. Siano a e b insiemi finiti e supponiamo $|a| = n+1$. Ciò che dobbiamo provare è che vale $|\text{Map}(a, b)| = |b|^{n+1}$. Allora $a \neq \emptyset$ e possiamo fissare un $u \in a$. Sia $c = a \setminus \{u\}$, dunque $|c| = n$ e, per ipotesi d'induzione, $|\text{Map}(c, b)| = |b|^n$. L'applicazione

$$\alpha: f \in \text{Map}(a, b) \mapsto (f|_c, f(u)) \in \text{Map}(c, b) \times b$$

è evidentemente ben definita ed è biettiva. Per verificarlo basta osservare che, per ogni $(g, y) \in \text{Map}(c, b) \times b$, l'unica applicazione f da a a b tale che $\alpha(f) = (g, y)$ è quella definita come:

$$x \in a \mapsto \begin{cases} g(x) & \text{se } x \neq u \\ y & \text{se } x = u \end{cases} \in b.$$

A questo punto $|\text{Map}(a, b)| = |\text{Map}(c, b) \times b| = |b|^n |b| = |b|^{n+1}$, come richiesto. La dimostrazione è completa. $\square$

Il fatto che valga la proposizione 19 spiega l'origine della notazione b^a che viene spesso usata per indicare l'insieme che qui chiamiamo $\text{Map}(a, b)$ delle applicazioni da a a b .

Passiamo ora al conteggio delle applicazioni iniettive. Stabiliamo una notazione: per ogni a e b , chiamiamo $\text{InjMap}(a, b)$ l'insieme delle applicazioni iniettive da a a b . Imitando l'approccio utilizzato per la proposizione 19, posto $n = |a|$, $m = |b|$ e $a = \{x_1, x_2, \dots, x_n\}$, osserviamo che definire un'applicazione iniettiva $f: a \rightarrow b$ significa scegliere in b le immagini $y_1 = f(x_1)$, $y_2 = f(x_2)$, $\dots$, $y_n = f(x_n)$ degli elementi di a in modo che sia soddisfatta la condizione di iniettività, cioè che, per ogni $i, j \in I_n$, se $j < i$ allora $y_j \neq y_i$. Dunque, assumendo $n \leq m$ (nell'altro caso $\text{InjMap}(a, b) = \emptyset$ per il teorema 18), possiamo scegliere come y_1 uno qualsiasi degli m elementi di b , come y_2 uno qualsiasi degli $m-1$ elementi di $b \setminus \{y_1\}$, come y_3 uno qualsiasi degli $m-2$ elementi di $b \setminus \{y_1, y_2\}$ e così via, sino ad arrivare alla scelta di y_n tra gli $m - (n-1) = m - n + 1$ elementi di $b \setminus \{y_1, y_2, \dots, y_{n-1}\}$. Otteniamo così che il numero delle applicazioni iniettive da a a b è il prodotto $m(m-1)(m-2) \cdots (m-n+1)$, come tra poco dimostreremo in modo più preciso. Diamo un nome (e un simbolo) a questo prodotto.

Definizione. Per ogni $n, m \in \mathbb{N}$, si indica col simbolo $m^{\underline{n}}$ il numero $\prod_{i=0}^{n-1} (m-i) = m(m-1)(m-2) \cdots (m-n+1)$ (qui, ed altrove, si segue la convenzione per cui un prodotto tra numeri interi con zero fattori vale 1, quindi $m^{\underline{0}} = 1$). Questo simbolo si legge ' m alla n discendente'; ogni numero di questa forma viene generalmente chiamato *fattoriale discendente*.

Inoltre, per ogni $m \in \mathbb{N}$, si chiama *fattoriale di m* , e si indica con $m!$, il prodotto dei primi m numeri interi positivi, cioè il numero $\prod_{i=1}^m i = 1 \cdot 2 \cdots m = m^{\underline{m}}$; in accordo con la convenzione appena menzionata, $0! = 1$.

Può aiutare a memorizzare la notazione il fatto che come una ordinaria potenza m^n tra numeri naturali indica il prodotto con n fattori tutti uguali ad m , il fattoriale discendente $m^{\underline{n}}$ è il prodotto con n fattori, il primo dei quali è m e gli altri si ottengono con la regola che a ciascun fattore segua lo stesso numero diminuito di una unità, ad esempio, $7^{\underline{3}} = 7 \cdot 6 \cdot 5 = 210$.

Osserviamo anche che, nelle notazioni della definizione, se $n > m$ si ha $m^{\underline{n}} = 0$, perché $m^{\underline{n}}$ è il prodotto tra tutti gli interi compresi tra $m-n+1$ e m , e dal momento che $m-n+1 \leq 0$, tra i fattori di questo prodotto c'è anche 0. Se invece $n \leq m$, allora si ha $m! = (\prod_{i=1}^{m-n} i) (\prod_{i=m-n+1}^m i) = (m-n)! m^{\underline{n}}$, dunque:

$$\forall m, n \in \mathbb{N} \quad \left(n \leq m \implies m^{\underline{n}} = \frac{m!}{(m-n)!} \right).$$

Proposizione 20. *Siano a e b insiemi finiti. Allora $|\text{InjMap}(a, b)| = |b|^{\underline{|a|}}$.*

In altri termini, $|\text{InjMap}(a, b)|$ vale 0 se $|a| > |b|$ e vale $|b|!/(|b|-|a|)!$ se $|a| \leq |b|$.

Dimostrazione. La dimostrazione è simile a quella della proposizione 19 e consiste nel provare, per induzione, che per ogni $n \in \mathbb{N}$ vale la formula $\varphi(n)$, dove $\varphi(n)$ è il predicato che afferma che, scelti comunque insiemi finiti a e b si ha $|a| = n \Rightarrow |\text{InjMap}(a, b)| = |b|^{\underline{|a|}}$. In altri termini, $\varphi(n)$ afferma che l'enunciato vale per tutti gli insiemi finiti a e b tali che $|a| = n$.

⁽¹²⁾si, anche per $m = 0$, va sempre ricordato: qui il calcolo dei limiti e le cosiddette 'forme indeterminate' non c'entrano nulla.

Se $n = 0$, cioè $a = \emptyset$, l'unica applicazione $a \rightarrow b$ è ovviamente iniettiva, quindi $|\text{InjMap}(a, b)| = 1$; d'altra parte $|b|^0 = 1$, quindi $\varphi(0)$ è vera e la base d'induzione è verificata. Sia ora n un arbitrario numero naturale, assumiamo $\varphi(n)$ e proviamo $\varphi(n+1)$. Siano a e b insiemi finiti e supponiamo $|a| = n+1$; per completare la dimostrazione dobbiamo verificare l'uguaglianza $|\text{InjMap}(a, b)| = |b|^{n+1}$. Come nella dimostrazione della proposizione 19, siccome $a \neq \emptyset$ possiamo fissare un $u \in a$. Posto $c = a \setminus \{u\}$, sia $\alpha: f \in \text{Map}(a, b) \mapsto (f|_c, f(u)) \in \text{Map}(c, b) \times b$ l'applicazione biettiva utilizzata per provare la proposizione 19. Se $f \in \text{InjMap}(a, b)$, ovviamente $f|_c$ è iniettiva e, inoltre, per ogni $x \in c$ si ha $f(u) \neq f(x)$ perché $u \neq x$, dunque $f(u) \notin \vec{f}(c)$. Pertanto $\alpha(f) \in \text{InjMap}(c, b) \times (b \setminus \vec{f}(c))$. Viceversa, se $h \in \text{InjMap}(c, b)$ e $y \in b \setminus \vec{f}(c)$, allora è chiaro (da quanto nella dimostrazione della proposizione 19) che $\alpha^{-1}((h, y))$ è un'applicazione iniettiva, cioè un elemento di $\text{InjMap}(a, b)$. Pertanto $\vec{\alpha}(\text{InjMap}(a, b)) = \text{InjMap}(c, b) \times (b \setminus \vec{f}(c))$. Ora, per ipotesi d'induzione, $|\text{InjMap}(c, b)| = |b|^n$ e, per il lemma 3 riferito alle applicazioni iniettive f e α , abbiamo $|\vec{f}(c)| = |c| = n$ e $|\text{InjMap}(a, b)| = |\text{InjMap}(c, b) \times (b \setminus \vec{f}(c))| = |\text{InjMap}(c, b)| |b \setminus \vec{f}(c)| = |b|^n (|b| - n) = |b|^{n+1}$, come richiesto. A questo punto la dimostrazione è completa. $\square$

Introduciamo due altri simboli: per ogni a e b , chiamiamo $\text{BijMap}(a, b)$ l'insieme delle applicazioni biettive da a a b e poniamo $\text{Sym}(a) = \text{BijMap}(a, a)$. Gli elementi di $\text{Sym}(a)$ sono dunque le applicazioni biettive da a ad a , queste prendono il nome di *permutazioni* (di a). Ovviamente $\text{BijMap}(a, b) \neq \emptyset$ se e solo se a e b sono equipotenti.

Corollario 21. *Siano a e b insiemi finiti, della stessa cardinalità n . Allora $|\text{BijMap}(a, b)| = |\text{Sym}(a)| = n!$.*

Dimostrazione. Per il teorema 9, $\text{BijMap}(a, b) = \text{InjMap}(a, b)$, quindi otteniamo dalla proposizione 20 l'uguaglianza $|\text{BijMap}(a, b)| = n^n = n!$. Nel caso particolare in cui $a = b$, questa diventa $|\text{Sym}(a)| = n!$. $\square$

5.1. Varianti: stringhe, parole. Sia $n \in \mathbb{N}$. Le applicazioni da I_n ad un fissato insieme X sono chiamate n -ple di elementi di X ; l'insieme $\text{Map}(I_n, X)$, ovvero X^{I_n} viene anche indicato, più sinteticamente, come X^n . Questa stessa nozione prende anche altri nomi in differenti contesti. Ad esempio: una stringa di lunghezza n , o anche una parola di lunghezza n , su un insieme X non è altro che una n -pla di elementi di X ; è appena il caso di specificare che si chiama semplicemente stringa (o parola) su X ogni oggetto che sia, per un opportuno $n \in \mathbb{N}$, una stringa di lunghezza n su X ; detto diversamente: l'insieme delle stringhe (o parole) su X è l'insieme $\bigcup \{X^n \mid n \in \mathbb{N}\}$. In simili contesti, X viene talvolta detto l'insieme dei caratteri o alfabeto delle stringhe. Possiamo indicare una stringa di lunghezza n su X con simboli come $'x_1 x_2 \dots x_n'$, dove ciascuno degli x_i è un elemento di X .

Se X è finito e ne conosciamo la cardinalità, per ogni $n \in \mathbb{N}$ sappiamo come contare le stringhe di lunghezza n su X : il loro numero è $|X|^n$, per la proposizione 19. Può capitare di dover contare le stringhe su X di assegnata lunghezza che soddisfino vincoli specifici; per questi scopi si possono usare varianti dei ragionamenti che abbiamo introdotto nelle pagine precedenti. Un caso (ormai) molto semplice è: quante sono le stringhe di lunghezza n su X in cui nessun carattere appaia più di una volta (cioè le stringhe $'x_1 x_2 \dots x_n' \in X^n$ tali che per ogni $i, j \in I_n$, se $i \neq j$ allora $x_i \neq x_j$)? Be', queste stringhe sono semplicemente le applicazioni iniettive da I_n a X ; il loro numero è dunque $|X|^n$, per la proposizione 20. Vediamo qualche esempio un po' più (ma solo un poco) elaborato. Il loro scopo è quello di mostrare come, per riuscire a rispondere a tante domande che sono simili a quelle a cui danno risposta gli enunciati in queste note, molto più che memorizzare gli enunciati stessi sia utile impadronirsi delle idee che stanno dietro ai ragionamenti svolti per dimostrarli.

Esempi 22. In questi esempi X è un insieme finito e n è un intero positivo.

- Quante sono le stringhe su X di lunghezza n in cui non si ripetono caratteri *in posizione consecutiva*? Si intende con questa espressione: stringhe $'x_1 x_2 \dots x_n' \in X^n$ tali che per ogni $i \in I_{n-1}$, si abbia $x_i \neq x_{i+1}$. Di una tale stringa possiamo scegliere il primo carattere x_1 in modo arbitrario tra i $|X|$ elementi di X , il secondo tra gli elementi di $X \setminus \{x_1\}$, il che ci lascia $|X| - 1$ possibilità di scelta, il terzo tra gli elementi di $X \setminus \{x_2\}$, e abbiamo ancora $|X| - 1$ possibilità di scelta, e proseguendo allo stesso modo, per ogni $i \in I_n$ tale che $i > 1$, scegliamo x_i tra i $|X| - 1$ elementi di $X \setminus \{x_{i-1}\}$. In conclusione, il numero delle stringhe cercate è $|X|(|X| - 1)^{n-1}$, dal momento che abbiamo $|X|$ possibilità di scelta per il primo carattere e $|X| - 1$ possibilità di scelta per ciascuno degli $n - 1$ caratteri rimanenti.
- Fissato un $a \in X$, quante sono le stringhe su X di prefissata lunghezza n in cui a appaia almeno una volta? E quelle in cui a appare esattamente una volta? Per rispondere, osserviamo che le stringhe in cui a non appare sono tante quante le stringhe di lunghezza n su $X \setminus \{a\}$, quindi $(|X| - 1)^n$.⁽¹³⁾ Sottraendo questo numero a quello $(|X|^n)$ di tutte le stringhe in X^n , otteniamo che il numero delle stringhe in X^n in cui a appaia almeno una volta è $|X|^n - (|X| - 1)^n$. Per rispondere alla seconda domanda osserviamo che una stringa di lunghezza n in cui a appaia esattamente una volta è determinata, in modo univoco, dalla posizione in cui a appare e dalla stringa di lunghezza $n - 1$ formata dai caratteri rimanenti, e questa è una (arbitraria) stringa in cui a non appare. Per quanto sopra, il numero di queste stringhe di lunghezza $n - 1$ e senza occorrenze di a è $(|X| - 1)^{n-1}$; siccome le possibili posizioni per a sono n , il numero cercato è $n(|X| - 1)^{n-1}$.
- Se $|X| = 8$ e $a \in X$, quante sono le stringhe su X di lunghezza 10 in cui a non appaia in posizione dispari (cioè: il primo, il terzo, il quinto, il settimo ed il nono carattere siano diversi da a)? Risposta: una tale stringa si

⁽¹³⁾La cosa è piuttosto evidente, per dimostrarla basta osservare che se $Y = X \setminus \{a\}$ e S è l'insieme delle stringhe 'prive di a ' considerato, allora S è l'insieme delle applicazioni $I_n \rightarrow X$ con immagine contenuta in Y , e se ι è l'immersione di Y in X , allora l'applicazione $f \in Y^n = \text{Map}(I_n, Y) \mapsto \iota \circ f \in S$ è biettiva.

ottiene scegliendo in ciascuna delle cinque posizioni pari un qualunque degli $|X|$ elementi di X , ed abbiamo complessivamente $|X|^5 = 8^5$ possibili modi di riempire queste posizioni; in ciascuna delle cinque posizioni dispari non possiamo inserire a ad abbiamo così solo $|X \setminus \{a\}| = 7$ caratteri a disposizione da usare in quella posizione, quindi abbiamo esattamente 7^5 possibilità per riempire le posizioni dispari. Nel complesso, dunque, il numero delle stringhe cercate è $8^5 7^5$.⁽¹⁴⁾

- iv. Quante sono le parole palindrome di lunghezza 9 su un alfabeto X di cardinalità 20? (Una parola palindroma è una parola che si legge allo stesso modo da destra verso sinistra come da sinistra verso destra. Più precisamente, se, per un qualche $n \in \mathbb{N}$, $w = \langle x_1 x_2 \dots x_n \rangle \in X^n$, w è palindroma se e solo se $x_i = x_{n+1-i}$ per ogni $i \in I_n$; ovvero, equivalentemente, per ogni $i \in I_n$ tale che $i < n/2$). Dal momento che le parole palindrome di lunghezza 9 sono determinate dai primi loro cinque caratteri (essendo i rimanenti quattro i primi quattro letti alla rovescia: vale a dire: queste parole hanno la forma $\langle x_1 x_2 x_3 x_4 x_5 x_4 x_3 x_2 x_1 \rangle$), ed i primi cinque caratteri sono del tutto arbitrari, il loro numero è 20^5 (più formalmente: l'applicazione che ad una parola associa la sua restrizione a I_5 , con dominio l'insieme delle parole palindrome di lunghezza 9 su X e codominio X^5 , è biettiva). Per esercizio, provare ad esprimere il numero delle parole palindrome di lunghezza n su un insieme finito di cardinalità k per n e k numeri naturali arbitrari e, ad esempio, il numero di quelle in cui ciascun carattere appare al massimo due volte.

6. PARTI

Esiste un modo molto semplice per codificare le parti di un insieme a utilizzando applicazioni da a ad un insieme di due elementi; vediamo come. Siano a un insieme e b una sua parte, e si fissi anche un insieme d di cardinalità 2; abitualmente si usa $d = \{0, 1\}$ e così faremo qui, ma qualsiasi altro insieme di due elementi andrebbe altrettanto bene. La *funzione caratteristica di b in a* (potremmo aggiungere: a valori in d) è l'applicazione $\chi_{b,a}$ così definita:

$$\chi_{b,a}: x \in a \mapsto \begin{cases} 1 & \text{se } x \in b \\ 0 & \text{se } x \notin b \end{cases} \in d.$$

Come abbastanza evidente, $b = \tilde{\chi}_{b,a}(\{1\})$. Abbiamo allora:

Teorema 23. Per ogni insieme a , l'applicazione

$$\alpha: b \in \mathcal{P}(a) \mapsto \chi_{b,a} \in \text{Map}(a, \{0, 1\})$$

è biettiva. La sua inversa è

$$\beta: f \in \text{Map}(a, \{0, 1\}) \mapsto \tilde{f}(\{1\}) \in \mathcal{P}(a).$$

Dimostrazione. Sia $M = \text{Map}(a, \{0, 1\})$. Basterà dimostrare le due uguaglianze $\beta \circ \alpha = \text{id}_{\mathcal{P}(a)}$ e $\alpha \circ \beta = \text{id}_M$. Per ogni $b \in \mathcal{P}(a)$ abbiamo $(\beta \circ \alpha)(b) = \beta(\chi_{b,a}) = \tilde{\chi}_{b,a}(\{1\}) = b$, per quanto appena osservato. Dunque, $\beta \circ \alpha = \text{id}_{\mathcal{P}(a)}$. Per provare l'altra uguaglianza, fissiamo $f \in M$ e sia $b = \beta(f)$, cioè $b = \tilde{f}(\{1\})$. Allora

$$(\alpha \circ \beta)(f) = \chi_{b,a}: x \in a \mapsto \begin{cases} 1 & \text{se } x \in b \\ 0 & \text{se } x \notin b \end{cases} \in \{0, 1\}.$$

Esaminiamo in dettaglio la descrizione di questa applicazione. Per la definizione di b , per ogni $x \in a$ si ha $x \in b \Leftrightarrow f(x) = 1$ e quindi, anche, $x \notin b \Leftrightarrow f(x) \neq 1$. Ma poiché $f(x) \in \{0, 1\}$ e $\{0, 1\}$ ha solo due elementi, $f(x) \neq 1 \Leftrightarrow f(x) = 0$, dunque $x \notin b \Leftrightarrow f(x) = 0$. Di conseguenza, per ogni $x \in a$ si ha $((\alpha \circ \beta)(f))(x) = f(x)$. Dal momento che $(\alpha \circ \beta)(f)$ ha, come f , dominio a e codominio $\{0, 1\}$, abbiamo così $(\alpha \circ \beta)(f) = f$. Pertanto $\alpha \circ \beta = \text{id}_M$, come richiesto. $\square$

Corollario 24. Per ogni insieme a , $\mathcal{P}(a)$ è equipotente a $\text{Map}(a, \{0, 1\})$. Se a è finito, allora $|\mathcal{P}(a)| = 2^{|a|}$.

Dimostrazione. Che a e $\mathcal{P}(a)$ siano equipotenti segue direttamente dal teorema 23; per la proposizione 19 abbiamo poi $|\mathcal{P}(a)| = |\text{Map}(a, \{0, 1\})| = 2^{|a|}$ se a è finito. $\square$

Una dimostrazione alternativa della seconda parte del corollario 24 si può ottenere per altra via, come conseguenza dell'osservazione che segue e che riportiamo perché anche di interesse indipendente.

Lemma 25. Siano a un insieme non vuoto e $x \in a$. Posto $A = \{y \subseteq a \mid x \in a\}$ e $B = \{y \subseteq a \mid x \notin a\}$ (dunque $B = \mathcal{P}(a) \setminus A$), le applicazioni

$$\alpha: y \in A \mapsto y \cup \{x\} \in B \quad \quad \quad \text{e} \quad \quad \quad \beta: y \in B \mapsto y \setminus \{x\} \in A$$

sono biettive, l'una inversa dell'altra. Inoltre, $B = \mathcal{P}(a \setminus \{x\})$.

⁽¹⁴⁾in termini, più formali: se chiamiamo M l'insieme delle stringhe di cui stiamo parlando (quindi M è un particolare sottoinsieme di $\text{Map}(I_{10}, X)$), se $P = \{2, 4, 6, 8, 10\}$ è l'insieme dei numeri pari in I_{10} e $D = I_{10} \setminus P$ (dunque D è l'insieme dei numeri dispari in I_{10}), se inoltre chiamiamo M_D l'insieme delle applicazioni da D ad X la cui immagine sia contenuta in $X \setminus \{a\}$ e poniamo $M_P = \text{Map}(P, X)$, si può vedere che è ben definita e biettiva l'applicazione da M a $M_P \times M_D$ che ad ogni $f \in M$ associa $(f|_P, f|_D)$. Ma $|M_P| = 8^5$ e $|M_D| = 7^5$, quindi $|M| = |M_P| |M_D| = 8^5 7^5$.

Dimostrazione. Che le due applicazioni indicate sono ben definite è ovvio. Per ogni $y \in A$ si ha $(\beta \circ \alpha)(y) = \beta(y \cup \{x\}) = (y \cup \{x\}) \setminus \{x\} = y \setminus \{x\} = y$ perché $x \notin y$. Dunque, $\beta \circ \alpha = \text{id}_A$. Simmetricamente, per ogni $y \in B$ si ha $(\alpha \circ \beta)(y) = \alpha(y \setminus \{x\}) = (y \setminus \{x\}) \cup \{x\} = y \cup \{x\} = y$ perché $x \in y$, quindi $\alpha \circ \beta = \text{id}_B$. Pertanto $\beta = \alpha^{-1}$. Infine, gli elementi di B sono gli insiemi i cui elementi appartengono ad a e sono diversi da x , quindi sono le parti di $a \setminus \{x\}$, dunque $B = \mathcal{P}(a \setminus \{x\})$. $\square$

Corollario 26. Siano a un insieme non vuoto e $x \in a$. Allora $|\mathcal{P}(a)| = 2|\mathcal{P}(a \setminus \{x\})|$.

Dimostrazione. Sia $\alpha: A \rightarrow B = \mathcal{P}(a \setminus \{x\})$ l'applicazione biettiva definita nel lemma 25. Poiché $B = \mathcal{P}(a) \setminus A$ e $|A| = |B|$, abbiamo $|\mathcal{P}(a)| = |A| + |B| = 2|B|$, dunque l'asserto. $\square$

Chiamiamo ora $\varphi(n)$ la formula $\forall a (|a| = n \Rightarrow |\mathcal{P}(a)| = 2^n)$. Anche se già sappiamo dal corollario 24 che vale $\forall n \in \mathbb{N} (\varphi(n))$, ridimostriamo questo fatto per induzione.

Certamente vale $\varphi(0)$, infatti se $|a| = 0$, cioè $a = \emptyset$, allora $\mathcal{P}(a) = \{\emptyset\}$, quindi $|\mathcal{P}(a)| = 1 = 2^0$, come richiesto da $\varphi(0)$. Sia ora $n \in \mathbb{N}$ e supponiamo che valga $\varphi(n)$. Se a è un insieme di cardinalità $n + 1$, allora $a \neq \emptyset$ e possiamo fissare $x \in a$. Ovviamente $|a \setminus \{x\}| = n$ e, per l'ipotesi d'induzione $\varphi(n)$, abbiamo $|\mathcal{P}(a \setminus \{x\})| = 2^n$. Dal corollario 26 segue allora $|\mathcal{P}(a)| = 2|\mathcal{P}(a \setminus \{x\})| = 2 \cdot 2^n = 2^{n+1}$. Abbiamo provato: $\forall n \in \mathbb{N} (\varphi(n) \Rightarrow \varphi(n+1))$; a questo punto la dimostrazione per induzione è completa.

6.1. Coefficienti binomiali. In questa sezione ci occuperemo della cardinalità dell'insieme delle parti di un assegnato insieme che abbiano un prefissato numero di elementi. Per ogni insieme a ed ogni $k \in \mathbb{N}$, chiamiamo $\mathcal{P}_k(a)$ l'insieme delle k -parti (cioè parti di cardinalità k) di a , dunque $\mathcal{P}_k(a) := \{x \in \mathcal{P}(a) \mid |x| = k\}$.⁽¹⁵⁾ Come primo passo, verifichiamo che se a e b sono insiemi equipotenti, allora, per ogni $k \in \mathbb{N}$, anche $\mathcal{P}_k(a)$ e $\mathcal{P}_k(b)$ sono equipotenti. A questo scopo sono utili le ovvie osservazioni che se f e g sono applicazioni componibili allora l'applicazione immagine $(f \circ g)^\rightarrow$ definita da $f \circ g$ coincide con $\vec{f} \circ \vec{g}$, ed inoltre, per ogni insieme a , l'applicazione immagine $(\text{id}_a)^\rightarrow$ definita da id_a è $\text{id}_{\mathcal{P}(a)}$.

Lemma 27. Sia $f: a \rightarrow b$ un'applicazione biettiva. Allora anche $\vec{f}$ è biettiva, con inversa $(f^{-1})^\rightarrow = \vec{f}$.

Dimostrazione. Sia $g = f^{-1}$. Allora, per le osservazioni appena fatte, $\vec{f} \circ \vec{g} = (f \circ g)^\rightarrow = (\text{id}_a)^\rightarrow = \text{id}_{\mathcal{P}(a)}$ e $\vec{g} \circ \vec{f} = (g \circ f)^\rightarrow = (\text{id}_b)^\rightarrow = \text{id}_{\mathcal{P}(b)}$. Pertanto, $\vec{g}$ è l'inversa di $\vec{f}$, quindi questa è biettiva. Resta da provare che $\vec{g}$ coincide con $\vec{f}$. Per farlo, osserviamo che per ogni $c \in \mathcal{P}(b)$ ed ogni $x \in a$ si ha $x \in \vec{f}(c)$ se e solo se $f(x) \in c$, ma, scelti comunque $x \in a$ e $y \in c$, si ha $f(x) = y$ se e solo se $x = g(y)$, quindi $\vec{f}(c) = \{x \in a \mid \exists y \in c (y = f(x))\} = \{x \in a \mid \exists y \in c (x = g(y))\} = \vec{g}(c)$. Pertanto $\vec{f} = \vec{g}$, come richiesto. $\square$

Corollario 28. Siano a e b insiemi equipotenti. Allora:

- (i) $\mathcal{P}(a)$ e $\mathcal{P}(b)$ sono equipotenti;
- (ii) per ogni $k \in \mathbb{N}$, $\mathcal{P}_k(a)$ e $\mathcal{P}_k(b)$ sono equipotenti.

Dimostrazione. Esiste un'applicazione biettiva $f: a \rightarrow b$. Allora, per il lemma 27 anche $\vec{f}: \mathcal{P}(a) \rightarrow \mathcal{P}(b)$ è biettiva, il che prova (i). Per ogni $x \in \mathcal{P}_k(a)$ e $y \in \mathcal{P}_k(b)$ si ha $\vec{f}(x) \in \mathcal{P}_k(b)$ e $(\vec{f})^{-1}(y) = \vec{f}(y) \in \mathcal{P}_k(a)$, quindi $\mathcal{P}_k(b) = (\vec{f})^\rightarrow(\mathcal{P}_k(a))$ e, come mostrato dal lemma 3, $\vec{f}$ induce l'applicazione biettiva $x \in \mathcal{P}_k(a) \mapsto \vec{f}(x) \in \mathcal{P}_k(b)$. Questo prova la (ii). $\square$

Notiamo che la prima parte del corollario 28 si può anche dedurre dal corollario 24.

Definizione. Se n e k sono numeri naturali, il *coefficiente binomiale* $\binom{n}{k}$ è $|\mathcal{P}_k(a)|$, dove a è un (qualsiasi) insieme di cardinalità n .

Per questa definizione è essenziale la seconda parte del corollario 28, che garantisce che $|\mathcal{P}_k(a)|$, il numero delle k -parti di a , non dipende dalla scelta di a tra gli insiemi di cardinalità n (cioè: $|\mathcal{P}_k(a)| = |\mathcal{P}_k(b)|$ per ogni $k \in \mathbb{N}$ ed ogni insieme finito b tale che $|b| = |a|$).

Alcuni coefficienti binomiali sono di calcolo pressoché immediato. Infatti, se a è un insieme finito e $n = |a|$, allora a ha esattamente un sottoinsieme di cardinalità 0 (cioè $\emptyset$) ed esattamente uno di cardinalità n (a stesso), quindi $\binom{n}{0} = \binom{n}{n} = 1$; inoltre $\binom{n}{k} = 0$ per ogni naturale $k > n$, dal momento che a non ha sottoinsiemi di cardinalità maggiore di n . Anche $\binom{n}{1}$ è facile da calcolare:

Lemma 29. Per ogni $n \in \mathbb{N}$ si ha $\binom{n}{0} = \binom{n}{n} = 1$, $\binom{n}{1} = n$ e $\binom{n}{k} = 0$ per ogni intero $k > n$.

Dimostrazione. Solo l'uguaglianza $\binom{n}{1} = n$ è ancora da verificare; per farlo basta osservare che l'applicazione $x \in a \mapsto \{x\} \in \mathcal{P}_1(a)$ è (ovviamente) biettiva. $\square$

⁽¹⁵⁾con una terminologia vecchia (che risale ad un'epoca precedente l'introduzione del linguaggio insiemistico) ma purtroppo ancora in uso, gli elementi di $\mathcal{P}_k(a)$ sono anche chiamati *combinazioni* di classe k degli n elementi di a .

Il coefficiente binomiale $\binom{n}{k}$ può essere descritto come il numero delle possibili scelte di un insieme di k oggetti estratti da un insieme di n oggetti (è meglio insistere su questo punto: ci riferiamo ad un *insieme* di k elementi, quindi è irrilevante l'ordine in cui li selezioniamo). Il prossimo lemma esprime la cosiddetta proprietà di simmetria dei coefficienti binomiali; l'idea è che selezionare i k oggetti che costituiscono il nostro insieme è concettualmente equivalente a selezionare gli $n - k$ oggetti da scartare (ad esempio, in una mano di poker, avendo cinque carte in mano, scegliere tre carte da conservare equivale a sceglierne due da scartare).

Lemma 30. Per ogni $n, k \in \mathbb{N}$ tali che $k \leq n$ si ha $\binom{n}{k} = \binom{n}{n-k}$.

Dimostrazione. Sia a un insieme tale che $|a| = n$. L'applicazione

$$c: x \in \mathcal{P}(a) \mapsto a \setminus x \in \mathcal{P}(a),$$

che ad ogni parte di a associa il suo complemento in a , è biettiva, perché $c \circ c = \text{id}_{\mathcal{P}(a)}$ (infatti per ogni $x \in \mathcal{P}(a)$ si ha $x = a \setminus (a \setminus x)$). Per ogni $x \in \mathcal{P}(a)$ si ha $|a \setminus x| = n - k$ se e solo se $|x| = k$, quindi $\vec{c}(\mathcal{P}_k(a)) = \mathcal{P}_{n-k}(a)$. Per il lemma 3, allora, c induce un'applicazione biettiva $\mathcal{P}_k(a) \rightarrow \mathcal{P}_{n-k}(a)$, quindi $|\mathcal{P}_k(a)| = |\mathcal{P}_{n-k}(a)|$, ovvero $\binom{n}{k} = \binom{n}{n-k}$. $\square$

Lemma 31. Per ogni $n \in \mathbb{N}$ si ha $\sum_{k=0}^n \binom{n}{k} = 2^n$

Dimostrazione. Sia ancora a un insieme tale che $|a| = n$. Ogni elemento x di $\mathcal{P}(a)$ appartiene a $\mathcal{P}_k(a)$, dove $k = |x| \in \{0, 1, \dots, n\}$, e non appartiene a $\mathcal{P}_i(a)$ per alcun intero $i \neq k$. Dunque $\mathcal{P}(a) = \bigcup_{k=0}^n \mathcal{P}_k(a)$ e gli insiemi $\mathcal{P}_0(a), \mathcal{P}_1(a), \dots, \mathcal{P}_n(a)$ sono a due a due disgiunti. Di conseguenza, il lemma 10 fornisce $|\mathcal{P}(a)| = \sum_{k=0}^n |\mathcal{P}_k(a)|$, ovvero, per il corollario 24, $2^n = \sum_{k=0}^n \binom{n}{k}$. $\square$

Un'altra importantissima proprietà dei coefficienti binomiali è descritta da una formula ricorsiva, che permette di calcolare i coefficienti binomiali relativi ad un intero positivo (inteso come cardinalità dell'insieme le cui parti di cardinalità data si stanno contando) come somme di coefficienti binomiali relativi all'intero precedente.

Teorema 32. Per ogni $n, k \in \mathbb{N}$ si ha $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$.

Dimostrazione. Fissato un insieme a di cardinalità $n + 1$ (quindi non vuoto) ed un suo elemento x , consideriamo l'applicazione biettiva $\alpha: y \in A \mapsto y \setminus \{x\} \in B$ definita nel lemma 25, dove $A = \{y \in \mathcal{P}(a) \mid x \in y\}$ e $B = \mathcal{P}(a \setminus \{x\})$. Siano $k \in \mathbb{N}$ e $A_k = A \cap \mathcal{P}_{k+1}(a)$, dunque A_k è l'insieme delle $(k + 1)$ -parti di a a cui appartiene x . Per ogni $y \in A_k$, si ha $\alpha(y) = y \setminus \{x\} \in B_k := B \cap \mathcal{P}_k(a)$ e, viceversa, per ogni $y \in B_k$ si ha $\alpha^{-1}(y) = y \cup \{x\} \in A_k$. Quindi $\vec{\alpha}(A_k) = B_k$, sicché, per il lemma 3, $|A_k| = |B_k|$. Ora, $B_k = \mathcal{P}(a \setminus \{x\}) \cap \mathcal{P}_k(a) = \mathcal{P}_k(a \setminus \{x\})$, quindi $|A_k| = |B_k| = \binom{n}{k}$. Analogamente a quanto accade nella dimostrazione del lemma 25, $\mathcal{P}_{k+1}(a) \setminus A_k = \{y \in \mathcal{P}_{k+1}(a) \mid x \notin y\} = \mathcal{P}_{k+1}(a \setminus \{x\})$, quindi $|\mathcal{P}_{k+1}(a)| = |A_k| + |\mathcal{P}_{k+1}(a \setminus \{x\})|$, sicché $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$. $\square$

Come già suggerito, è possibile utilizzare il teorema 32 per calcolare, ricorsivamente, tutti i coefficienti binomiali. Se $n \in \mathbb{N}$, i coefficienti binomiali $\binom{n}{k}$ dove k è uno tra 0 e 1, oppure è maggiore o uguale a $n - 1$ si possono ottenere dai lemmi 29 e 30, osservandone la conseguenza $\binom{n}{n-1} = \binom{n}{1} = n$. Conosciamo dunque $\binom{n}{k}$ per ciascuna scelta di k se $n \leq 3$. Per $n = 4$ l'unico coefficiente binomiale che non rientra tra quelli appena descritti è $\binom{4}{2}$, che però si può ricavare come $\binom{3}{1} + \binom{3}{2} = 3 + 3 = 6$ dal teorema 32. Allo stesso modo, noti i coefficienti binomiali relativi a 4, troviamo quelli (non già descritti) relativi a 5: $\binom{5}{2} = \binom{4}{1} + \binom{4}{2} = 4 + 6 = 10$ e $\binom{5}{3} = \binom{4}{2} + \binom{4}{3} = 6 + 4 = 10$ (o, meglio, $\binom{5}{3} = \binom{5}{2}$ per il lemma 30). È chiaro come la procedura si possa iterare per calcolare ogni coefficiente binomiale desiderato. Sia il teorema 32 che il procedimento ricorsivo appena descritto sono ben visualizzati dal cosiddetto *triangolo di Tartaglia-Pascal* (nella figura che segue), che rappresenta in modo conveniente i coefficienti binomiali non nulli.

Il teorema 32 permette anche di dimostrare una formula (non ricorsiva) che descrive in modo esplicito i coefficienti binomiali.

Teorema 33. Per ogni $n, k \in \mathbb{N}$ tali che $k \leq n$ si ha $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

Dimostrazione. A vantaggio della chiarezza, conviene fissare alcune notazioni, dando un nome a due formule. Chiamiamo $\psi(n, k)$ la formula

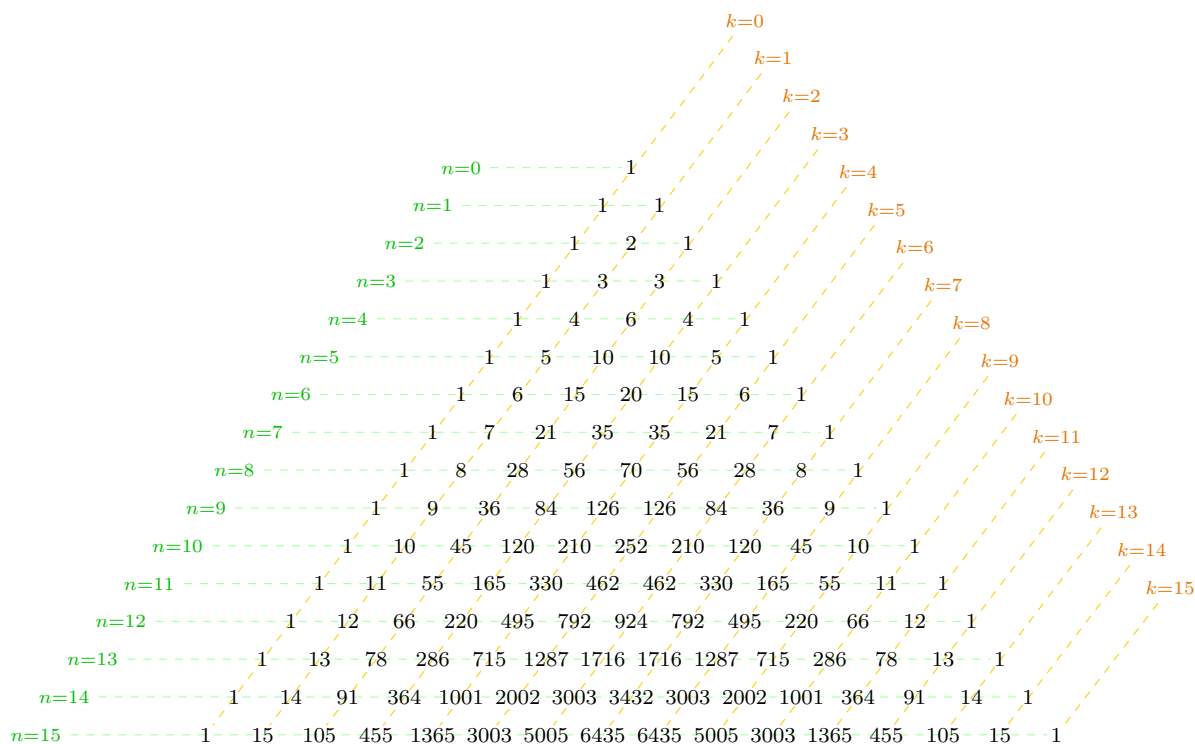
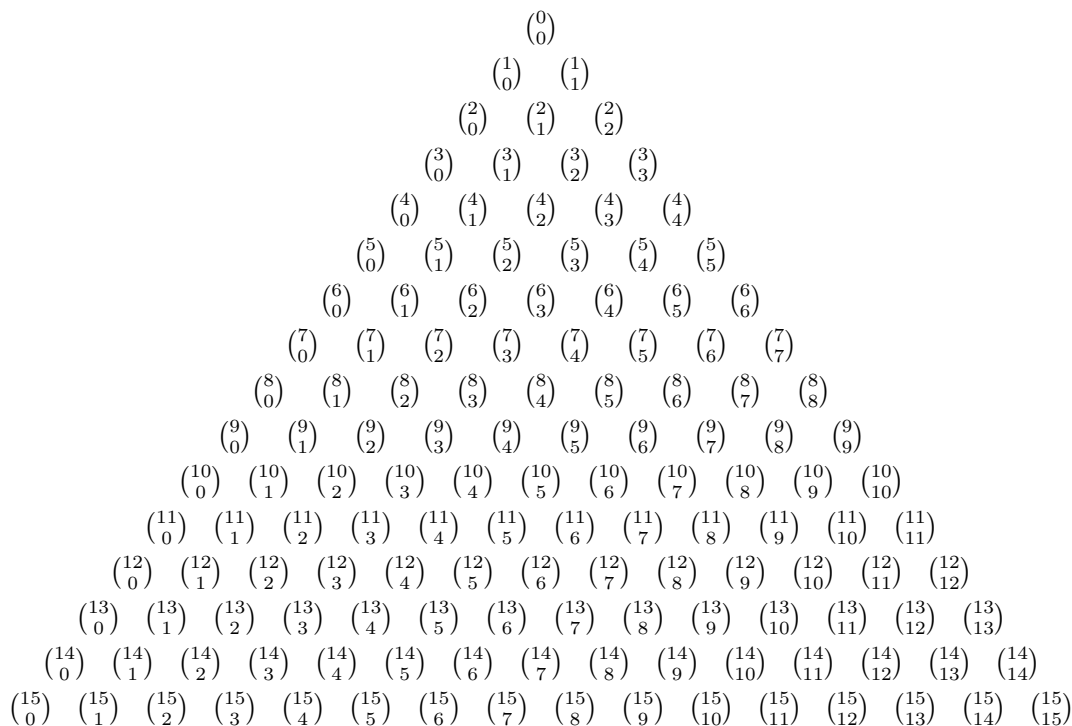
$$k \leq n \Rightarrow \binom{n}{k} = \frac{n!}{k!(n-k)!} \quad (\psi(n, k))$$

nelle variabili (libere) n e k , a cui è riferito l'enunciato. Osserviamo, innanzitutto, che se $n, k \in \mathbb{N}$, e $k = 0$ oppure $k \geq n$, allora $\psi(n, k)$ è vera. Infatti, se $k > n$, allora $\psi(n, k)$ è vera perché l'antecedente dell'implicazione in $\psi(n, k)$ è in questo caso falso; inoltre $n!/0!(n-0)! = n!/(1 \cdot n!) = 1 = \binom{n}{0}$, quindi è vera $\psi(n, 0)$ e, similmente, $n!/n!(n-n)! = n!/n!0! = 1 = \binom{n}{n}$, quindi è vera $\psi(n, n)$. Sia poi $\varphi(n)$ la formula⁽¹⁶⁾

$$\forall k \in \mathbb{N} (\psi(n, k)). \quad (\varphi(n))$$

L'asserto del teorema è che $\varphi(n)$ vale per ogni $n \in \mathbb{N}$, cosa che ci accingiamo a dimostrare ragionando per induzione. Iniziamo dalla base d'induzione: $\varphi(0)$ è la formula $\forall k \in \mathbb{N} (\psi(0, k))$, che è vera perché, come osservato sopra, qualsiasi sia n , vale $\varphi(n, k)$ per ogni $k \geq n$.

⁽¹⁶⁾Considerando $\mathbb{N}$ come simbolo di costante, $\varphi(n)$ è un predicato unario nella variabile n .



IL TRIANGOLO DI TARTAGLIA-PASCAL. Ciascuno dei coefficienti binomiali $\binom{n}{k}$ appare come $(k+1)$ -esimo termine della riga $(n+1)$ -esima. In accordo con il teorema 32, a parte i coefficienti che appaiono sui lati del triangolo (quelli della forma $\binom{n}{0}$ oppure $\binom{n}{n}$, che sappiamo essere uguali a 1), ciascun coefficiente è la somma dei due che appaiono nel rigo superiore, uno immediatamente a sinistra, l'altro immediatamente a destra. Ad esempio, $5005 = \binom{15}{6}$ è la somma tra $2002 = \binom{14}{5}$ e $3003 = \binom{14}{6}$. Come provato dal lemma 31, per ogni n la somma dei coefficienti al rigo intestato da n è 2^n , mentre il lemma 30 spiega il fatto che il triangolo sia simmetrico rispetto alla bisettrice verticale.

Proviamo ora che, per ogni $n \in \mathbb{N}$, vale $\varphi(n) \Rightarrow \varphi(n+1)$. Fissato n ed assunta $\varphi(n)$ come vera, dobbiamo dunque provare $\varphi(n+1)$, cioè: $\forall k \in \mathbb{N} (\psi(n+1, k))$. Sappiamo già che $\psi(n+1, k)$ vale per $k=0$ e per ogni intero $k \geq n+1$, quindi basterà provare $\psi(n+1, k)$, ovvero

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

per ogni intero positivo $k \leq n$. Per ogni tale k abbiamo $k-1 \in \mathbb{N}$ e possiamo dunque applicare il teorema 32 a n e $k-1$, ottenendo

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

e quindi, utilizzando prima $\varphi(n)$ e poi le uguaglianze $k! = (k-1)!k$ e $(n-(k-1))! = (n-k+1)! = (n-k)!(n-k+1)$,

$$\begin{aligned} \binom{n+1}{k} &= \binom{n}{k-1} + \binom{n}{k} = \frac{n!}{(k-1)!(n-(k-1))!} + \frac{n!}{k!(n-k)!} = \frac{n!}{(k-1)!(n-k)!} \left(\frac{1}{n-k+1} + \frac{1}{k} \right) \\ &= \frac{n!}{(k-1)!(n-k)!} \frac{n+1}{(n-k+1)k} = \frac{(n+1)!}{k!(n-k+1)!}; \end{aligned}$$

l'uguaglianza così ottenuta non è altro che il conseguente dell'implicazione in $\psi(n+1, k)$. A questo punto abbiamo effettivamente dimostrato l'implicazione $\varphi(n) \Rightarrow \varphi(n+1)$ per ogni $n \in \mathbb{N}$; la dimostrazione è così completa. $\square$

Come fatto per applicazioni e stringhe, vediamo alcuni esempi di applicazioni e varianti delle idee presentate in questa sezione.

Esempio 34. Per comodità di esposizione, fissiamo un insieme a cui riferirci nei nostri esempi: $a = \{n \in \mathbb{N} \mid n < 20\}$, dunque $|a| = 20$.

- i. Sia b un sottoinsieme di a , ad esempio, $b = \{4, 9, 17\}$. Quante sono le parti x che contengono b , vale a dire: quanti elementi ha $v := \{x \in \mathcal{P}(a) \mid b \subseteq x\}$? Vediamo due modi per fornire una risposta. Si può applicare per tre volte di fila il lemma 25 o, meglio ancora, utilizzare l'idea della sua dimostrazione ed osservare che l'applicazione $x \in v \mapsto x \setminus b \in \mathcal{P}(a \setminus b)$ è biettiva (con inversa $x \in \mathcal{P}(a \setminus b) \mapsto x \cup b \in v$) per concludere: $|v| = |\mathcal{P}(a \setminus b)| = 2^{|a \setminus b|} = 2^{17}$.

In alternativa, si può ragionare sulle funzioni caratteristiche, cioè su come siano descritte le funzioni caratteristiche degli elementi di v . Questo perché, come conseguenza del teorema 23 e del lemma 3, $|v|$ è il numero delle funzioni caratteristiche degli elementi di v . Per ogni $x \subseteq a$, è ovvio che $x \in v$ se e solo se la funzione caratteristica $\chi_{x,a}$ manda gli elementi di b in 1, quindi $|v|$ è il numero delle applicazioni $a \rightarrow \{0, 1\}$ che mandano i tre elementi di b in 1. Ragionando come per la proposizione 19, vediamo che una tale applicazione è determinata dalla scelta delle immagini (in $\{0, 1\}$) dei 17 elementi di $a \setminus b$, dunque $|v| = 2^{17}$. O più formalmente: le applicazioni richieste sono determinate dalle loro restrizioni ad $a \setminus b$, quindi il loro numero è $|\text{Map}(a \setminus b, \{0, 1\})| = 2^{17}$.

- ii. Con le stesse notazioni di prima, quanti elementi ha $w := \{x \in \mathcal{P}(a) \mid b \cap x = \emptyset\}$? Anche in questo caso possiamo pensare ad almeno due approcci: quello più ovvio: $w = \mathcal{P}(a \setminus b)$, quindi $|w| = 2^{17}$. In alternativa: le funzioni caratteristiche degli elementi di w sono quelle che mandano i tre elementi di b in 0, dunque il loro numero è 2^{17} .
- iii. Ulteriori varianti: quanti elementi ha $z := \{x \in \mathcal{P}(a) \mid b \cap x = \{4, 17\}\}$? E quanti ne ha $s := \{x \in \mathcal{P}(a) \mid |b \cap x| = 2\}$? Due approcci per $|z|$: abbiamo $z = \{x \in \mathcal{P}(a \setminus \{9\}) \mid \{4, 17\} \subseteq x\}$, quindi possiamo ragionare come al punto precedente, dopo aver sostituito a con $a \setminus \{9\}$ per ottenere $|z| = 2^{19-2} = 2^{17}$. Oppure: le funzioni caratteristiche degli elementi di z sono quelle che mandano 4 e 17 in 1 e 9 in 0, quindi sono, come prima, determinate dalle loro restrizioni ad $a \setminus b$ e ce ne sono quindi esattamente 2^{17} .

Per quanto riguarda invece s , possiamo osservare che s è l'unione di tre insiemi a due a due disgiunti: $s_4 = \{x \in \mathcal{P}(a) \mid b \cap x = \{9, 17\}\}$, $s_9 = z$ ed $s_{17} = \{x \in \mathcal{P}(a) \mid b \cap x = \{4, 9\}\}$. Dobrebbe essere chiaro che questi sono tra loro equipotenti, quindi $|s| = 3|z| = 3 \cdot 2^{17}$.

- iv. Proviamo ora a contare il numero delle 8-parti degli insiemi definiti nei punti precedenti. Iniziamo con $v' := \{x \in \mathcal{P}_8(a) \mid b \subseteq x\}$. Imitando la dimostrazione del teorema 32, osserviamo che l'applicazione $x \in v' \mapsto x \setminus b \in \mathcal{P}_5(a \setminus b)$ è biettiva (è indotta da quella utilizzata per contare $|v|$, nel senso del lemma 3; naturalmente 5 appare qui in quanto $5 = 8 - |b|$), quindi $|v'| = \binom{17}{5}$. Poi, $w' := \{x \in \mathcal{P}_8(a) \mid b \cap x = \emptyset\} = \mathcal{P}_8(a \setminus b)$ ha ovviamente cardinalità $\binom{17}{8}$. La cardinalità di $z' := \{x \in \mathcal{P}_8(a) \mid b \cap x = \{4, 17\}\} = \{x \in \mathcal{P}_8(a \setminus \{9\}) \mid \{4, 17\} \subseteq x\}$ si può calcolare come nel caso di v' , ottenendo $|z'| = \binom{19-2}{8-2} = \binom{17}{6}$, mentre, se $s' = \{x \in \mathcal{P}_8(a) \mid |b \cap x| = 2\}$, allora $|s'| = 3|z'| = 3\binom{17}{6}$.

Esempio 35. Applichiamo queste stesse idee in altri contesti. Se a e b sono insiemi finiti, quante sono le corrispondenze da a a b ? Siccome l'applicazione $g \in \mathcal{P}(a \times b) \mapsto (a, b, g) \in \text{Corr}(a, b)$ è biettiva, $|\text{Corr}(a, b)| = |\mathcal{P}(a \times b)| = 2^{|a||b|}$. Ad esempio, se a ha cardinalità 5 esistono esattamente $2^{5 \cdot 5} = 2^{25}$ relazioni binarie in a (è un bel numero, oltre 33 milioni).

Se assumiamo $a \neq \emptyset \neq b$ e fissiamo $x \in a$ e $y \in b$, quante sono le corrispondenze γ da a e b tali che y sia uno dei corrispondenti di x ? Siccome queste corrispondenze sono quelle il cui grafico abbia (x, y) tra i suoi elementi,

ragionando come negli esempi precedenti (o, direttamente, per il corollario 26) vediamo che loro numero è $2^{|a||b|-1}$. Più in generale, se c è una parte di b , quante sono le corrispondenze γ da a e b tali che ogni elemento di c sia un corrispondente di x ? Di nuovo, ci basta contare le parti di $a \times b$ che ne siano i grafici, cioè le parti di $a \times b$ contenenti $\{x\} \times c$, un insieme equipotente a c (come nella dimostrazione della proposizione 12). Già sappiamo come procedere: è la prima domanda che ci siamo posti negli esempi precedenti; l'insieme delle corrispondenze γ di cui stiamo parlando è equipotente a $\mathcal{P}((a \times b) \setminus (\{x\} \times c))$, quindi ha cardinalità $2^{|a||b|-|c|}$.

Una variante ulteriore consiste nel chiederci quanti elementi abbia l'insieme Γ di tutte le corrispondenze γ da a e b tali che c sia precisamente l'insieme dei corrispondenti di x , ovvero: $c = \{v \in b \mid x \gamma v\}$. Piuttosto che seguire la falsariga precedente, qui conviene cambiare punto di vista e fare un'altra osservazione. Per ogni $u \in a$ e $\gamma \in \text{Corr}(a, b)$, chiamiamo γ_u l'insieme degli elementi di b che, siano corrispondenti di u rispetto a γ . Allora sono ben definite le applicazioni $\theta_\gamma: u \in a \mapsto \gamma_u \in \mathcal{P}(b)$ e $\theta: \gamma \in \text{Corr}(a, b) \mapsto \theta_\gamma \in \text{Map}(a, \mathcal{P}(b))$. Si può verificare⁽¹⁷⁾ che θ è biettiva. Con queste notazioni $\vec{\theta}(\Gamma)$ è l'insieme delle applicazioni $f: a \rightarrow \mathcal{P}(b)$ tali che $f(x) = c$. Ragionando come nella sezione precedente (negli esempi 22 e in quanto precede), sappiamo come calcolare la cardinalità di questo insieme di applicazioni: esse sono descritte dall'assegnazione di un'immagine (in $\mathcal{P}(b)$) a ciascun elemento di $a \setminus \{x\}$, dunque $|\vec{\theta}(\Gamma)| = |\mathcal{P}(b)|^{|a \setminus \{x\}|}$ e quindi $|\Gamma| = |\vec{\theta}(\Gamma)| = 2^{|b|(|a|-1)}$.

Chiudiamo con due esercizi. Se $a = \{n \in \mathbb{N} \mid n < 100\}$, quante sono le relazioni binarie riflessive in a ? E quante quelle simmetriche? Ricordiamo che se γ è una relazione binaria in a e g è il suo grafico, allora γ è riflessiva se e solo se g contiene $\Delta_a := \{(x, x) \mid x \in a\}$ ed è simmetrica se e solo se per ogni $i, j \in a$ si ha $(i, j) \in g$ se e solo se $(j, i) \in g$.

⁽¹⁷⁾e si invita a farlo, a titolo di esercizio; θ^{-1} è l'applicazione che ad ogni $f \in \text{Map}(a, \mathcal{P}(b))$ associa $\gamma \in \text{Corr}(a, b)$ definita da: $\forall (u, v) \in a \times b \ (u \gamma v \iff u \in f(v))$.

7. APPENDICE

7.1. Dimostrazioni per controesempio minimo e per induzione. Iniziamo da una definizione: chiamiamo *intero positivo primo* un numero intero p se e solo se $p > 1$ e i soli divisori di p in $(\mathbb{N}, \cdot)$ sono 1 e p .⁽¹⁸⁾ Indichiamo col simbolo $\mathbb{P}$ l'insieme dei numeri interi positivi primi.

Per quanto ingannevolmente banale, diamo una seconda definizione. Informalmente: se X è un insieme di numeri naturali si usa chiamare prodotto di elementi di X ogni numero che si ottenga moltiplicando tra loro elementi di X . Per evitare ambiguità esprimiamoci in termini più precisi (è questa la definizione): diciamo che un numero naturale n è un prodotto di elementi di X se e solo se esistono un intero positivo λ ed elementi $x_1, x_2, \dots, x_\lambda$ di X tali che $n = \prod_{i=1}^{\lambda} x_i$ (vale a dire: $n = x_1 x_2 \cdots x_\lambda$). Notiamo che questa condizione include il caso in cui $\lambda = 1$ (e quindi $n = x_1 \in X$), quindi ogni elemento di X è un prodotto di elementi di X . Usando il linguaggio dell'algebra, come chi legge può facilmente osservare stiamo dicendo che i prodotti di elementi di X sono tutti e soli gli elementi della parte chiusa generata da X in $(\mathbb{N}, \cdot)$.

Fatte queste premesse, dimostriamo che ogni numero intero maggiore di 1 è prodotto di interi positivi primi.

Proposizione 36. *Ogni numero intero maggiore di 1 è prodotto di elementi di $\mathbb{P}$.*

Dimostrazione. Ragioniamo per controesempio minimo. Forniamo l'argomentazione in due versioni: a sinistra la scriviamo in modo più agile e (forse) più facile da seguire, a destra in termini più formali, come fatto nella sottosezione 2.1 ed in accordo con le notazioni usate lì, e più facile da non fraintendere.

Supponiamo l'asserto falso; ciò significa che esistono interi maggiori di 1 che non sono prodotti di interi positivi primi e quindi, per il principio di buon ordinamento dei naturali, esiste il minimo m tra essi.

Supponiamo l'asserto falso. Chiamiamo $\varphi(n)$ il predicato unario che esprime “ n è prodotto di elementi di $\mathbb{P}$ ”; siano N l'insieme dei numeri interi maggiori di 1 (dunque $N = \mathbb{N}^* \setminus \{1\}$) e $C = \{n \in N \mid \neg \varphi(n)\}$. Allora C è l'insieme degli interi maggiori di 1 che non sono prodotti di elementi di $\mathbb{P}$, vale a dire: l'insieme dei controesempi all'enunciato. Aver assunto l'enunciato falso significa aver assunto $C \neq \emptyset$; per il principio di buon ordinamento dei naturali, esiste allora $m = \min C$.

Detto questo, la dimostrazione si conclude molto rapidamente: siccome m non è prodotto di elementi di $\mathbb{P}$, certamente $m \notin \mathbb{P}$. Allora m ha un divisore a diverso da 1 e da m ; fissato tale a abbiamo $1 < a < m$; inoltre esiste $b \in \mathbb{N}$ tale che $m = ab$. Da $1 < a < m$ segue $1 < b < m$.

Allora a e b sono interi maggiori di 1. Poiché essi sono entrambi minori di m la scelta di m (come controesempio minimo) comporta che ...

Allora $a, b < m = \min C$, quindi $a, b \notin C$. Ma $a, b \in N$, dunque, per definizione di C , si ha $\varphi(a)$ e $\varphi(b)$, vale a dire: ...

... a e b sono, entrambi, prodotti di interi positivi primi. Da ciò segue subito che $m = ab$ è un prodotto di interi positivi primi, in contraddizione con la scelta di m . Questa contraddizione conclude la dimostrazione. $\square$

Vediamo ora un classico esempio di dimostrazione per induzione, quello di una formula il calcolo della somma degli interi positivi minori di un intero positivo prefissato.

Proposizione 37. *Per ogni $n \in \mathbb{N}^*$ si ha $\sum_{i=1}^n i = \frac{n(n+1)}{2}$.*⁽¹⁹⁾

Dimostrazione. Ragioniamo per induzione, usando notazioni in accordo con quelle del teorema 1. Chiamiamo φ la formula $\sum_{i=1}^n i = \frac{n(n+1)}{2}$; ovviamente questa è un predicato unario nella variabile n . Iniziamo dalla base di induzione. Poniamo $b = 1$, perché ci interessa provare la formula per tutti gli interi positivi e, ovviamente, $\mathbb{N}^* = N_1$. La formula $\varphi(1)$ è

$$\sum_{i=1}^1 i = \frac{1(1+1)}{2}. \quad (\varphi(1))$$

Evidentemente $\sum_{i=1}^1 i = 1 = 1(1+1)/2$, quindi $\varphi(1)$ è vera; abbiamo verificato la base d'induzione. Occupiamoci ora del passo induttivo. Per ogni $n \in \mathbb{N}^*$ dobbiamo provare l'implicazione $\varphi(n) \Rightarrow \varphi(n+1)$, cioè

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

Evidentemente, per ogni $n \in \mathbb{N}$ vale $\sum_{i=1}^{n+1} i = (\sum_{i=1}^n i) + (n+1)$. Di conseguenza, se $\sum_{i=1}^n i = n(n+1)/2$ allora

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

ed otteniamo l'uguaglianza desiderata. Avendo così verificato l'implicazione $\varphi(n) \Rightarrow \varphi(n+1)$ per ogni $n \in \mathbb{N}^*$, abbiamo completato la dimostrazione. $\square$

⁽¹⁸⁾a scanso di fraintendimenti: questa NON È la definizione di numero intero primo, che è un po' più articolata.

⁽¹⁹⁾il simbolo usato dovrebbe essere chiaro: $\sum_{i=1}^n i$, scritto anche $\sum_{i=1}^n i$, indica la somma $1 + 2 + \dots + n$ dei primi n numeri interi positivi.