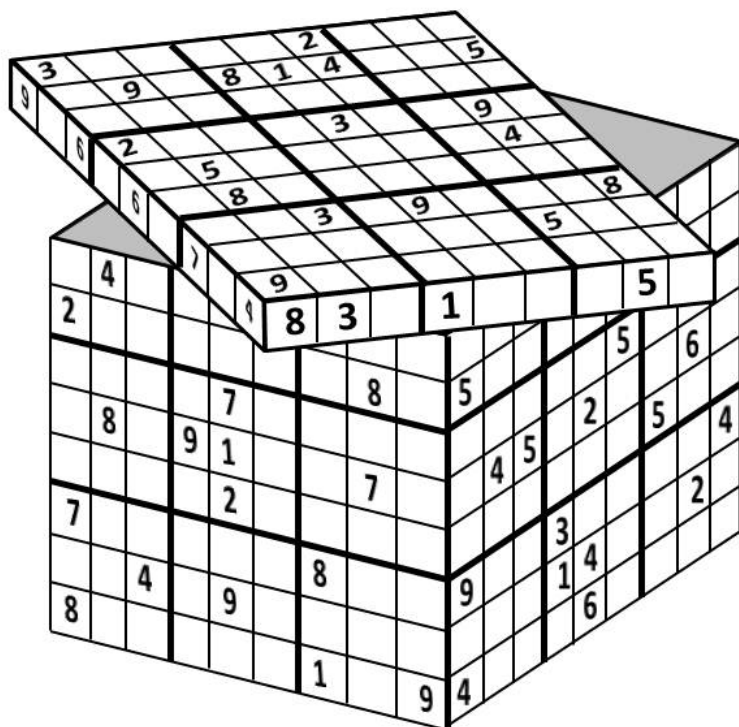


INTRODUZIONE ALLA MATEMATICA DISCRETA – PARTE I: INTERI, COMBINATORICA E GRAFI

Giuseppe Lancia



Contents

1	Preliminari matematici	1
1.1	Introduzione alla Matematica Discreta	1
1.2	Logica e algebra booleana	6
1.3	Insiemi	11
1.4	Relazioni	18
1.5	Funzioni	26
1.6	Il principio di induzione	30
1.6.1	Induzione multipla	35
1.7	Somme e loro manipolazioni	36
1.7.1	Somme multiple	39
1.8	Alcune somme importanti	41
1.8.1	Somma di numeri consecutivi	41
1.8.2	Somma di quadrati consecutivi	43
1.8.3	Somma di potenze consecutive	46
1.8.4	Il metodo di perturbazione	47
1.9	Calcolo delle probabilità	49
1.9.1	Variabili casuali e valor medio	52
2	La matematica degli interi	55
2.1	Teoria dei numeri	55

2.1.1	MCD e mcm	55
2.1.2	Numeri primi e loro distribuzione	59
2.1.3	Fattorizzazione in primi	62
2.1.4	Il piccolo teorema di Fermat	64
2.1.5	Test di primalità	65
2.2	Pari e Dispari	66
2.2.1	Il segno delle permutazioni.	69
3	Piccioni e buche	73
3.1	Il principio della piccionaia, forma semplice	73
3.2	Il principio della piccionaia, forma forte	75
4	Contiamo!	79
4.1	Principii fondamentali: somma e prodotto	79
4.1.1	Il principio della somma	79
4.1.2	I numeri di Fibonacci	80
4.1.3	Il principio del prodotto	82
4.2	Combinazioni (sottoinsiemi)	85
4.2.1	Il triangolo di Pascal	89
4.3	Disposizioni (sottoinsiemi ordinati)	91
4.4	Ripetizioni e multi-insiemi	92
4.4.1	Combinazioni con ripetizioni	94
5	Il principio di inclusione-esclusione	97
5.1	Il principio base	97
5.2	Spiazzamenti	110
6	Procedure combinatoriche	113
6.1	Matrimoni stabili	113
6.2	Generazione di strutture random	117

6.2.1	Insiemi	117
6.2.2	Permutazioni e disposizioni	118
6.3	Enumerazione completa	119
6.3.1	Generare tutti i sottoinsiemi	120
6.3.2	Generare tutte le permutazioni	120
7	Teoria dei grafi	123
7.1	Grafi non orientati	123
7.2	Cammini e cicli	126
7.3	Grafi bipartiti, hamiltoniani e euleriani	127
7.4	Alberi	133
7.5	Grafi orientati	137
7.6	Grafi pesati	138
8	Problemi su grafi	141
8.1	Il minimo albero di supporto	142
8.2	Accoppiamenti e coperture	145
8.3	Clique e insieme indipendente	152
8.4	Colorazione di grafi	154
8.5	Il commesso viaggiatore	157
9	Tracce di soluzioni	161
9.1	Capitolo 1	161
9.2	Capitolo 2	164
9.3	Capitolo 3	165
9.4	Capitolo 4	166
9.5	Capitolo 5	168
9.6	Capitolo 7	169
9.7	Capitolo 8	171

Chapter 1

Preliminari matematici

1.1 Introduzione alla Matematica Discreta

Ad un party si presentano n persone, p delle quali sono uomini e q sono donne (immaginiamo, ad esempio, che sia $p = 15$ e $q = 10$, sicchè $n = 25$). Lo studio della matematica discreta ci insegnerà, tra le altre cose, a ragionare nel rispondere a domande quali le seguenti:

- Supponendo che ciascuno stringa la mano a tutti gli altri, quante strette di mano si hanno in totale? Quante se invece supponiamo che a stringersi la mano siano sempre e solo un uomo e una donna?
- Viene suonata una canzone e tutte le donne vogliono ballare. In quanti modi possono formarsi delle coppie per ballare?
- La cena è servita su una grande tavola rettangolare. In quanti modi i commensali si possono sedere a tavola? In quanti modi se il capotavola è una donna? In quanti modi se il capotavola è una donna e ogni donna è seduta in mezzo a due uomini?

A titolo d'esempio (la teoria relativa a come risolvere queste e simili questioni verrà sviluppata nei prossimi capitoli) proviamo a ragionare su questi punti.

Cominciamo dal primo punto. Assumendo che ognuno stringa la mano a tutti gli altri, ognuno stringerebbe $n - 1$ mani e quindi in totale si avrebbero $n(n - 1)$ strette, giusto? Sbagliato! In base a questo ragionamento le strette di mano in un gruppo di due persone sarebbero due, mentre ovviamente dovrebbe risultare una stretta sola. L'errore sta nel fatto che ogni stretta di mano è contata due volte, i.e., una volta per ciascuna delle due persone coinvolte nella stretta. Tenendo conto di ciò si conclude che le strette di mano sono in realtà $n(n - 1)/2$. Nel nostro esempio, quindi, le strette di mano sono in tutto 300. Se invece a stringersi la mano sono sempre un uomo e una donna, le strette di mano in totale sono $p \times q = 15 \times 10 = 150$. In questo caso, è bastato osservare che (i) ognuno dei p uomini stringe q mani; (ii) nessuna stretta è contata due volte perchè a stringersi le mani non sono mai due uomini; (iii) tutte le strette sono contate perchè due donne non si stringono mai la mano.

Passiamo al secondo punto. Consideriamo prima, per semplicità, il caso in cui alla festa ci sia numero uguale di uomini e donne. In questo caso, ognuna delle p donne potrebbe ballare con uno fra p uomini. Se la prima donna ballasse con x , la seconda potrebbe ballare con uno tra $p-1$ uomini (tutti tranne x). Sia questi y . La terza potrebbe ballare con $p-2$ compagni (tutti tranne x e y). Proseguendo in questo modo, si conclude che ci sono $p(p-1) \cdots 3 \cdot 2 \cdot 1$ modi di formare le coppie per un ballo. Il numero $p(p-1) \cdots 3 \cdot 2 \cdot 1$ è detto $p!$ (da leggersi *p fattoriale*). Alcuni valori del fattoriale ci danno un'idea di come questa funzione aumenti vertiginosamente all'aumentare di p : si ha $3! = 6$, $4! = 24$, $10! = 3,628,800$, $15! = 1,307,674,368,000$ e $20! = 2,432,902,008,176,640,000$. In generale, avendo p oggetti distinti, e volendo disporli (ordinarli) in un elenco, ogni ordinamento è detto una *permutazione* degli oggetti, e ci sono in tutto $p!$ permutazioni. È importante che gli elementi siano *distinti* (ad esempio, se tutti gli elementi fossero indistinguibili, ci sarebbe una sola permutazione e non $p!$)

Tornando al nostro esempio, e osservando che si ha $p > q$, ci sono $p-q$ uomini che non balleranno. La prima donna ha p scelte per il suo compagno. La seconda ne ha $p-1$, la terza $p-2$, ecc. In totale i modi di formare le coppie per il ballo sono

$$p(p-1)(p-2) \cdots (p-q+1) = \frac{p!}{(p-q)!}. \quad (1.1)$$

Nel caso specifico, essendoci 15 uomini e 10 donne, le combinazioni diverse in cui possono accoppiarsi per un ballo sono $15!/5! = 10,897,286,400$.

Supponiamo infine che tutti gli ospiti si vogliano sedere a tavola. Fissiamo il capotavola e l'ordine (ad esempio, il senso orario). Il capotavola può essere uno qualsiasi degli n invitati. Alla sua sinistra può sedersi uno dei restanti $n-1$ ospiti. Alla sinistra di questo, uno dei restanti $n-2$, ecc. In totale si hanno $n!$ modi di sedersi. Nel nostro esempio specifico, $n = 25$ e quindi ci sono $25!$ modi (più di 15 milioni di miliardi di miliardi) di fare sedere gli invitati a tavola.*

Se imponiamo che il capotavola sia una donna, questa può essere scelta in q modi. Per ciascuno di questi modi rimangono $n-1$ persone che possono essere sedute in qualsiasi ordine, e quindi il numero totale di disposizioni possibili è $q \times (n-1)!$ (circa 6 milioni di miliardi di miliardi). Se imponiamo inoltre che ogni donna debba essere seduta fra due uomini, molte delle permutazioni precedenti diventano non valide. Per calcolare il numero di permutazioni del tipo desiderato, si può ragionare così: a ogni donna assegniamo –in tutti i modi possibili, che coincidono con i modi di formare le coppie per ballare– un particolare uomo che starà alla sua sinistra (ossia, creiamo $q = 10$ coppie miste, immaginando di aver ammanettato il braccio sinistro della donna al destro dell'uomo, in modo che la coppia diventi un'unità). Infine, rimangono $p-q = 5$ uomini “liberi”. Facciamo quindi sedere i $p = 15$ elementi (le q coppie più i $p-q$ singoli) in tutti i modi possibili partendo dalla posizione del capotavola e procedendo in senso orario, con l'accortezza però che il primo elemento seduto sia di tipo coppia (in questo modo siamo sicuri che il capotavola sarà una donna). Si noti che ogni donna avrà alla sua sinistra un uomo (quello a cui è ammanettata), ma anche a destra un uomo, perchè se così non fosse, la donna alla sua destra non avrebbe un uomo a sinistra.

*Volendo essere pignoli, bisognerebbe discutere sul fatto che esistono dei modi simmetrici di fare sedere le persone, e decidere se questi modi vadano considerati come distinti o meno. Specificamente, essendo la tavola rettangolare, e supponendo che esistano due possibili posti di capotavola, diciamo “nord” e “sud”, per ogni ordine x in cui il capotavola nord è A, esiste un ordine y in cui il capotavola sud è A e in cui ogni commensale ha, a destra e sinistra, le stesse due persone che aveva in x . Se questi due modi di sedersi fossero considerati uguali, allora il numero totale di ordinamenti sarebbe $n!/2$. Se poi non esistesse neppure il capotavola –ad esempio, se la tavola fosse rotonda– e due modi di sedersi in cui ciascun commensale ha, sia a destra che a sinistra, le stesse persone fossero considerati uguali, allora il numero totale di ordinamenti sarebbe $(n-1)!$. Infatti, da ogni ordinamento se ne potrebbero ricavare n equivalenti semplicemente facendo ruotare tutte le persone contemporaneamente di una o più posizioni.

Facciamo un piccolo esempio per chiarire la strategia enumerativa appena descritta. Supponendo di avere cinque uomini, che indichiamo con $\{A, B, C, D, E\}$ e tre donne, che indichiamo con $\{a, b, c\}$, per prima cosa formiamo le coppie in tutti i modi possibili. Uno di questi modi è ad esempio, $\{(a, B), (b, C), (c, E)\}$. In corrispondenza di questo accoppiamento, restano liberi gli uomini A e D , e procediamo ad elencare i possibili ordinamenti dell'insieme $\{A, D, (a, B), (b, C), (c, E)\}$ che cominciano con una coppia. Uno di questi ordinamenti è

$$\pi = ((a, B), D, A, (c, E), (b, C))$$

In base ad esso, a capotavola abbiamo a , seguito in senso orario da B , D , A , ecc., fino a C che siede a destra di a . Un altro possibile ordinamento è

$$\pi = ((b, C), A, (c, E), D, (a, B))$$

in base al quale a capotavola abbiamo b , seguito in senso orario da C , poi A , c , ecc., fino a B che siede a destra di C .

Ricapitolando il ragionamento appena esposto, ci sono $p!/(p-q)!$ modi di formare le coppie, e, in corrispondenza di ciascuno di essi, $p!$ permutazioni degli elementi, di cui una frazione q/p comincia con una coppia. Quindi, esistono in tutto

$$\frac{q}{p} \times p! \times \frac{p!}{(p-q)!} = q \times (p-1)! \times \frac{p!}{(p-q)!}$$

modi di fare sedere le persone nei quali ogni donna è sempre in mezzo a due uomini. Nel nostro esempio specifico, abbiamo

$$\frac{10 \times 14! \times 15!}{5!} \simeq 9.5 \times 10^{21}$$

modi ammissibili, e quindi, rispetto a tutti i modi possibili, meno di una permutazione ogni 1600 circa risulta soddisfare la condizione richiesta.

Esempio. Un mazzo di carte da briscola viene mescolato e le carte vengono girate a faccia in su una alla volta. Quante sono le possibili sequenze diverse con cui le carte vengono ordinate da questa operazione? Il mazzo ha 40 carte, per cui gli ordinamenti sono $40!$. Questo numero è pari a circa 10^{48} . \diamond

ESERCIZIO 1.1. Elencare le 24 permutazioni di $\{A, B, C, D\}$. \diamond

ESERCIZIO 1.2. Si elenchino tutte le permutazioni di $\{1, 2, 3, 4, 5\}$ in cui ogni numero pari è immediatamente preceduto, e immediatamente seguito, da un numero dispari. \diamond

ESERCIZIO 1.3. Si elenchino tutte le permutazioni di $\{A, B, C, E\}$ in cui le due vocali sono consecutive. Si ricavi una formula per calcolare il numero di permutazioni di un insieme con n vocali e m consonanti in cui tutte le vocali sono consecutive \diamond

ESERCIZIO 1.4. Quanti sono gli anagrammi (anche senza senso compiuto) della parola LAMPIONE in cui ogni vocale è immediatamente preceduta da una consonante? \diamond

ESERCIZIO 1.5. Quanti sono i modi di fare sedere gli invitati a tavola mantenendo il vincolo che ogni donna sia seduta fra due uomini, ma senza l'obbligo che il capotavola sia una donna? \diamond

Sulla crescita delle funzioni

Come si è visto anche nell'esempio appena illustrato, nello studio dei problemi combinatorici ci capita sovente di avere a che fare con funzioni[†] la cui crescita è talmente rapida da risultare spesso sorprendente e difficile da stimare senza un po' di esperienza.

Consideriamo il seguente esempio. Prendiamo una scacchiera e mettiamo una moneta da 1 euro sulla prima casella, 2 sulla seconda, 4 sulla terza e così via. Quanto sarà alta la torre di monete sull'ultima casella?

Si tratta di una pila di 2^{63} monete. 2^{63} è il prodotto

$$2 \cdot 2 \cdot 2 \cdots 2 \cdot 2$$

con 63 fattori. Il prodotto di n fattori tutti uguali fra loro, e di valore a ciascuno, è detto funzione *esponenziale*, ed è indicata con a^n . Nel nostro caso particolare, abbiamo $a = 2$ e $n = 63$. Per fare una stima grossolana del valore 2^{63} , rimpiazziamo ogni 10 fattori (2^{10}) con $10^3 = 1000$ (in realtà $2^{10} = 1024$, per cui stiamo sottostimando il valore). Ne consegue che $2^{63} > (10^3)^6 \cdot 2^3$, ossia

$$2^{63} > 8 \cdot 10^{18}.$$

Ora, assumendo che una pila di 8 euro abbia spessore di 1 cm (in realtà ne bastano di meno per fare 1 cm, per cui stiamo ancora sottostimando), abbiamo che la pila è alta almeno 10^{18} centimetri. Siccome $10^5 \text{ cm} = 1 \text{ Km}$, la pila è alta almeno 10^{13} Km. La distanza della Terra dalla Luna è di circa $4 \cdot 10^5$ Km, per cui questa pila va ben oltre la Luna! Quanto oltre? La distanza della Terra dal Sole è di circa $2 \cdot 10^7$ Km, per cui la nostra pila sarebbe (almeno) 500,000 volte più lunga che la distanza da qui al Sole!

Da questo esempio si evince che, per avere approssimazioni inferiori al valore di 2^n , si possono rimpiazzare i gruppi di dieci "2" con gruppi di tre "10". Oppure, siccome $2^4 = 16 > 10$, possiamo rimpiazzare ogni quattro "2" con un "10". Per avere approssimazioni superiori, siccome $2^3 = 8 < 10$, possiamo rimpiazzare ogni tre "2" con un "10". Per cui

$$8 \cdot 10^{18} < 2^{63} < 10^{21} \tag{1.2}$$

Per ottenere esattamente l'esponente y tale che $10^y = 2^x$ bisognerebbe dividere x per circa 3.32 (o meglio per il $\log_2 10$).

Veniamo ora ad un esempio combinatorico altrettanto sorprendente. Consideriamo una scacchiera vuota su cui si vogliono disporre a caso i pezzi degli scacchi nelle varie caselle. Ci chiediamo se il numero di disposizioni possibili dei pezzi sulla scacchiera sia maggiore o minore del numero di granelli di sabbia sulla spiaggia di Lignano.

Nel gioco degli scacchi esistono pezzi di due colori, bianco e nero. Per ogni colore ci sono 8 pedoni, 2 torri, 2 cavalli, 2 alfieri, un re e una regina. La scacchiera contiene $8 \times 8 = 64$ caselle e, convenzionalmente, l'angolo basso a sinistra è una casella nera. I pezzi dello stesso tipo (ad esempio, i pedoni) sono indistinguibili fra loro.

[†]La definizione formale di cos'è una funzione verrà data nella Sezione 1.5.

Ai fini della discussione, immaginiamo che un granello di sabbia sia un cubo di lato 0.5mm. In particolare, quindi, 1m^3 di sabbia contiene $2000^3 = 8 \times 10^9$ granelli di sabbia. Per semplicità, arrotondiamo questo numero a 10^{10} (dieci miliardi). Diciamo poi che la spiaggia si estenda per 10Km di lunghezza, 100m di larghezza e 10m di profondità (come si vede, questi sono stime già leggermente in eccesso rispetto ai valori reali). In totale, quindi, avremmo 10^7 metri cubi di sabbia, pari a un numero 10^{17} (cento milioni di miliardi) di granelli di sabbia.

Il numero di disposizioni possibili dei pezzi degli scacchi su una scacchiera è (discuteremo più avanti su come questo numero possa essere determinato)

$$\frac{64 \times 63 \times 62 \times \cdots \times 35 \times 34 \times 33}{(8 \times 7 \times 6 \times 5 \times 4 \times 3)^2 \times 2^8}$$

e questo numero è pari a circa 10^{43} (dieci milioni di miliardi di miliardi di miliardi di miliardi). Quanti sono i granelli di sabbia sulla costa adriatica? Immaginando che la costa si estenda per 1000Km di lunghezza, ci sarebbero 10^{19} granelli di sabbia, per cui questo numero sarebbe enormemente maggiore. E se prendessimo i granelli di sabbia di tutte le coste di tutte le nazioni del mondo? Anche immaginando di avere 100000Km di coste e che ogni spiaggia sia larga 1Km, avremmo 10^{22} granelli di sabbia, per cui il numero di modi di piazzare gli scacchi sulla scacchiera sarebbe miliardi di miliardi di volte maggiore. Se anche l'intero pianeta Terra fosse composto interamente di sabbia[‡], il numero di granelli sarebbe inferiore al numero di disposizioni degli scacchi!

Nell'esempio degli scacchi, il numero di disposizioni dipende dal prodotto di interi consecutivi, il che ci riporta, come nel caso dei commensali che dovevano sedersi a tavola, a considerare la funzione fattoriale, $n!$. Notiamo che il fattoriale cresce almeno come 2^n e al massimo come n^n . Questi sono limiti molto lontani l'uno dall'altro. Si può migliorare un po' il limite inferiore notando che in $n!$ tutti i fattori da 10 a n valgono almeno 10, per cui $n! > 10^{n-9}$. La miglior stima della crescita di $n!$ è la seguente, che diventa sempre più accurata all'aumentare di n :

$$n! \simeq \left(\frac{n}{e}\right)^n \sqrt{2\pi n} \quad (1.3)$$

dove $e \simeq 2.718$ è la costante di Nepero. In prima approssimazione, possiamo dire che $n!$ cresce (almeno) come $(n/3)^n$.

ESERCIZIO 1.6. Consideriamo un gruppo di n persone (sul come si sono trovati i valori che seguono verrà data spiegazione più avanti. Per ora li si prenda per buoni). Viene organizzato un torneo di tennis fra tutte le persone, e denotiamo con $A(n)$ il numero di partite che il vincitore dovrà avere giocato alla fine del torneo. $A(n)$ è (almeno) $\log_2 n$. Esattamente, $A(n)$ è il minimo intero non inferiore a $\log_2 n$ (ossia, l'arrotondamento, per eccesso, di $\log_2 n$ ad intero, indicato con $\lceil \log_2 n \rceil$). Si svolge poi una votazione per stabilire chi sia il giocatore più tecnico e chi il più simpatico. La stessa persona può essere nominata per entrambe le categorie. Detto $B(n)$ il numero di possibili coppie "(più tecnico, più simpatico)", si ha $B(n) = n^2$. Successivamente, viene tirata una moneta per n volte, e ogni persona per cui esce "testa" riceve un premio. Detto $C(n)$ il numero di modi in cui la suddetta premiazione può avere luogo, si ha $C(n) = 2^n$. Infine, le n persone abbandonano una alla volta il gruppo e tornano, in un certo ordine, alle rispettive abitazioni. Detto $D(n)$ il numero di ordini possibili in cui le persone se ne vanno, si ha $D(n) = n!$. Si completi (anche con valori

[‡]Il volume della Terra è pari a circa 1080 miliardi di chilometri cubi.

approssimati) la seguente tabella

n	$A(n)$	$B(n)$	$C(n)$	$D(n)$
1	0	1	2	1
2	1	4	4	2
3	2	9	8	6
4	2	16	16	24
8	3	64	256	40320
10	4	100	1024	3628800
16				
20				
30				
50				
64				
100				

◇

1.2 Logica e algebra booleana

La logica si occupa dello studio di proposizioni che possono risultare vere o false. Questi due valori sono indicati come **VERO** e **FALSO**, e le proposizioni di questo tipo sono comunemente chiamate *predicati*. Se P è un predicato e Q un altro predicato, possiamo creare nuovi predicati tramite tre operazioni fondamentali: **or** (\vee), **and** (\wedge) e **not** (\neg). Le regole sono

- $P \vee Q$ è **VERO** se *almeno una* tra P e Q vale **VERO**, altrimenti $P \vee Q$ è **FALSO**.
- $P \wedge Q$ è **VERO** se *entrambe* P e Q valgono **VERO**, altrimenti $P \wedge Q$ è **FALSO**.
- $\neg P$ è **VERO** se P è **FALSO** e $\neg P$ è **FALSO** se P è **VERO**.

Si hanno le seguenti *tabelle di verità*:

P	Q	$P \vee Q$	$P \wedge Q$	$\neg P$
FALSO	FALSO	FALSO	FALSO	VERO
FALSO	VERO	VERO	FALSO	VERO
VERO	FALSO	VERO	FALSO	FALSO
VERO	VERO	VERO	VERO	FALSO

L'introduzione delle operazioni logiche e delle rispettive tabelle di verità ci permette di trattare la logica come un tipo particolare di algebra, definita su un insieme di due elementi. Tale algebra è detta algebra di Boole, o *algebra booleana*. L'ordine di priorità delle tre operazioni è il seguente. La negazione \neg ha priorità massima, mentre l'operazione \wedge (detta anche *prodotto logico*) ha la priorità sull'operazione \vee (detta anche *somma logica*).

In base a queste regole, si ha che

$$(P \wedge Q) \vee R = P \wedge Q \vee R$$

e

$$(\neg P) \vee Q = \neg P \vee Q$$

mentre

$$\neg(P \vee Q) \neq \neg P \vee Q.$$

È importante saper calcolare la negazione di una proposizione in cui appare un quantificatore universale (i.e., “per ogni”, denotato con \forall) o esistenziale (i.e., “esiste”, denotato con \exists). Se la proposizione è del tipo “per ogni x vale $P(x)$ ”, la sua negazione è: “esiste almeno un x per cui non vale $P(x)$ ”. Se la proposizione è del tipo “esiste un x per cui vale $Q(x)$ ”, la sua negazione è: “per nessun x vale $Q(x)$ ” analogo a “per ogni x non vale $Q(x)$ ”.

Un’ulteriore operazione logica è l’implicazione, indicata con \implies , che va interpretata come

- $P \implies Q$ è **VERO** se, tutte le volte in cui P è **VERO**, anche Q è **VERO**. (Si noti che, quando P è **FALSO** Q può essere indifferentemente **VERO** o **FALSO**, mentre l’unica possibilità esclusa è che possa essere P **VERO** ma Q **FALSO**.)

La tabella della verità è perciò:

P	Q	$P \implies Q$
FALSO	FALSO	VERO
FALSO	VERO	VERO
VERO	FALSO	FALSO
VERO	VERO	VERO

Dall’analisi della tabella di verità dell’implicazione, si deduce che $P \implies Q$ è la stessa cosa che $\neg P \vee Q$. Inoltre, siccome $\neg\neg X = X$ sempre, abbiamo che $\neg P \vee Q = \neg P \vee \neg\neg Q$. Per cui invertendo il ruolo di P e di $\neg Q$ si ha che $P \implies Q$ è la stessa cosa che $\neg Q \implies \neg P$.

Si noti che se $P = \text{FALSO}$ allora $P \implies Q$ è sempre **VERO**! Questo fatto risulta controintuitivo a molti, ed è divertente cercare di fare degli esempi di (pseudo)dimostrazioni in cui da una ipotesi falsa riusciamo a dedurre, coerentemente, un fatto altresì falso. Proviamo a scegliere una frase Q qualsiasi e dimostrarlo che $1 = 0$ implica Q . Sia allora $Q = \text{“Le mucche sono verdi”}$; proviamo a dimostrarlo così. Ad ogni colore diamo un codice numerico, in modo che i vari possibili colori siano codificati come $1, 2, \dots, k$. Sia v il codice del colore verde. Presa una mucca qualsiasi, sia c il codice del suo colore. Allora $c = c \times 1 = c \times 0 = 0 = v \times 0 = v \times 1 = v$ sicchè il colore di quella mucca è proprio v : la mucca è verde!

Un esempio importante di utilizzo della logica riguarda un tipo di *sillogismo*, chiamato anche deduzione o *modus ponens*:

se P è vero, ed è vero che $P \implies Q$, allora si può concludere che anche Q è vero.

Per *dimostrazione* di un'affermazione P (in particolare, ad es. di un teorema) si intende, fondamentalmente, l'utilizzo di una catena di deduzioni vere $D_1 \implies D_2, D_2 \implies D_3, \dots, D_{k-1} \implies D_k$ e $D_k \implies P$, dove D_1 è un fatto “notoriamente” vero (un postulato, o il risultato di un'altra dimostrazione).

Bisogna fare attenzione a non confondere la conclusione con la premessa. Ad esempio, se sappiamo che *Tutti i friulani amano il vino* e che *Paolo ama il vino* non possiamo concludere che *Paolo è friulano*.

Dimostrazioni per assurdo. Supponiamo ora di sapere che *Franca odia il vino* e di voler dimostrare che *Franca non è friulana*. La conclusione si ottiene tramite la “dimostrazione per assurdo”. Infatti, supponendo che Franca fosse friulana saremmo costretti a dover negare una cosa vera (ossia che odia il vino, perchè, in quanto friulana, deve amare il vino).

In generale, una dimostrazione per assurdo consiste nel dimostrare una proposizione falsa (ad esempio, dimostrare che $1 + 1 = 1$) a partire da un'ipotesi X . In tal modo, ne consegue che anche X deve essere falsa. Si noti che, volendo dimostrare una certa proposizione P , potremmo prendere fra le premesse la negazione di P e farne conseguire un asserto falso (tipicamente, una contraddizione). Questo implica che la negazione di P deve essere falsa, e quindi P deve essere vera.

Esempio. Si consideri il seguente problemino. Ci sono 5 cappelli, di cui 3 bianchi e due neri. A tre persone, che chiameremo A, B e C, viene messo uno tra questi cappelli. Ogni persona può vedere il cappello che hanno in testa gli altri due, ma non il suo. Ad ogni persona viene poi chiesto di indovinare il colore del suo cappello. Se sbaglia, deve pagare un milione di euro. Se rifiuta di rispondere, non succede niente. Se indovina, vince un milione di euro. Il primo a parlare, rifiuta di rispondere. Il secondo pure. Il terzo, dopo aver visto che sia A che B hanno un cappello bianco, risponde “il mio cappello è bianco” e vince il premio. Il ragionamento diretto sarebbe complicatissimo, ma un ragionamento per assurdo porta subito alla risposta. Supponiamo, per assurdo, che il cappello di C sia nero. Giustamente, A ha rifiutato di rispondere, avendo visto un cappello bianco (quello di B) e uno nero. Ma allora B, vedendo il cappello nero di C, avrebbe dedotto che il suo cappello era bianco (o A avrebbe risposto “bianco”) e avrebbe potuto rispondere. Invece, siccome B non ha risposto, il cappello di C deve essere bianco. \diamond

Come ulteriore esempio di dimostrazione per assurdo, consideriamo l'enunciato P = “esistono infiniti numeri primi” e dimostriamo che $\neg P \implies P$, da cui P deve essere vero. Ossia dimostriamo che se i numeri primi fossero in numero finito, allora non potrebbero essere in numero finito.[§] La dimostrazione del teorema è dovuta ad Euclide. Supponiamo, per assurdo, che tutti i numeri primi siano p_1, \dots, p_n . Creiamo un nuovo numero $a = p_1 \times p_2 \times \dots \times p_n + 1$. Sia p un divisore primo di a (al limite, p è pari ad a stesso). Si ha $p \neq p_i$ per $i = 1, \dots, n$, perchè a non è divisibile per alcun p_i (a diviso per p_i da' quoziente $p_1 \times \dots \times p_{i-1} \times p_{i+1} \times \dots \times p_n$ e resto 1). Quindi p è un nuovo numero primo e p_1, \dots, p_n non erano *tutti* i numeri primi.

ESERCIZIO 1.7. Presa per vera l'affermazione “cane che abbaia non morde”, si dica quali tra le seguenti affermazioni sono con essa compatibili:

1. cane che morde non abbaia

[§]Diamo qui per scontato che il lettore conosca la definizione di numeri primi e le loro proprietà principali. La teoria relativa ai numeri primi verrà ripresa più approfonditamente nel capitolo 2

2. cane che non abbaia, morde
3. ci sono cani che abbaiano e non mordono
4. ci sono cani che non abbaiano e mordono
5. ci sono cani che abbaiano e mordono
6. ci sono cani che non abbaiano e non mordono.

◇

ESERCIZIO 1.8. Siano A= “chi ha più di 21 anni può guidare” e B= “Paolo ha 18 anni”, C= “Gianni ha 24 anni”, D= “chi guida conosce il codice stradale”. Quali tra queste deduzioni si possono fare?

- Gianni conosce il codice stradale
- Gianni guida
- Paolo non può guidare
- Gianni può guidare

Inoltre, qual è la negazione di A? E quella di D?

◇

ESERCIZIO 1.9. Consideriamo le seguenti verità, che ci provengono dalla zoologia:

- ogni cane abbaia
- non esistono cani verdi.
- le rane sono animali verdi che non abbaiano

Si dica quali tra le seguenti proposizioni sono vere, quali false e quali indecidibili in base alle premesse:

1. ogni cane verde abbaia
2. esistono cani verdi che non abbaiano
3. esistono cani verdi che abbaiano
4. ogni animale verde o è un cane oppure abbaia
5. esistono animali verdi che non sono cani e che abbaiano
6. nessun animale verde è un cane che non abbaia
7. ogni animale verde o non è un cane oppure non abbaia.

◇

ESERCIZIO 1.10. Si dimostri, per assurdo, che non possono esistere dei naturali positivi a e b tali che $a = b^2 - a^2$.

◇

Se e solo se. Tipicamente, nell'effettuare una dimostrazione, cerchiamo di ricavare una proposizione B a partire da una premessa A che sappiamo essere vera. Ciò che stiamo dimostrando, di fatto, è che $A \implies B$. Alcune volte, però, risultano vere sia l'implicazione $A \implies B$ che la sua opposta, $B \implies A$. In questo caso, diciamo che

A è vera *se e solo se* B è vera

o che

l'essere A vera è condizione *necessaria e sufficiente* perchè B sia vera.

Chiamiamo A la *premessa* e B la *conclusione*. Diciamo che la premessa è sufficiente se il suo verificarsi implica la conclusione (ossia, $A \implies B$), mentre essa è necessaria se, quando la conclusione è vera, anche la premessa deve esserlo (ossia, $B \implies A$). Ad esempio, essere dei buoni atleti, con ottimi riflessi, è una condizione necessaria, ma non sufficiente, per poter essere campioni a livello mondiale di tennis. Analogamente, vincere un grande jackpot alla lotteria è condizione sufficiente, ma non necessaria, a garantirsi un buon tenore di vita per il resto dei propri anni. Come esempio di condizione necessaria e sufficiente, consideriamo la partita di ritorno di un incontro di Champions League, diciamo Udinese-Barcellona. Supponendo che la partita di andata sia finita $1-1$, e che il punteggio attuale sia $2-2$, condizione necessaria e sufficiente perchè l'Udinese passi il turno è che segni almeno un goal in più del Barcellona (in caso di parità sia all'andata che al ritorno, i goals segnati fuori casa varrebbero doppio, e passerebbe il Barcellona).

La notazione matematica per indicare una condizione necessaria e sufficiente è

$$A \iff B$$

Ricordiamo ancora una volta che, quando è richiesto di dimostrare che $A \iff B$, di fatto vanno dimostrate *due cose*:

1. che $A \implies B$
2. che $B \implies A$ (o, alternativamente, che $\neg A \implies \neg B$.)

Esempio. Dimostriamo che, dati due numeri a, b

$$a > b \iff (\exists c > 0 \text{ tale che } a = b + c)$$

(\Rightarrow) Sia $a > b$. Detto $c := a - b$ si ha $c > 0$ e $a = b + (a - b) = b + c$.

(\Leftarrow) Sia $c > 0$ tale che $a = b + c$. Siccome $c > 0$, sommando b da entrambe le parti della disuguaglianza, si ha $b + c > b$, ossia $a > b$. \diamond

Esempio. Un numero naturale a si dice

- *pari* se esiste un numero naturale k tale che $a = 2k$
- *dispari* se esiste un numero naturale q tale che $a = 2q + 1$

(Si dimostri, per esercizio, che nessun numero può essere contemporaneamente pari e dispari e che ogni numero naturale o è pari o è dispari. Ci si accorgerà di come anche “teoremi” banali come questi possono risultare particolarmente fastidiosi da dimostrare in modo formale e rigoroso...)

Dimostriamo ora che

$$a \text{ è dispari} \iff a^2 \text{ è dispari.}$$

(\Rightarrow) Sia a dispari, con $a = 2k + 1$. Allora $a^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2k' + 1$, con $k' = (2k^2 + 2k)$, e quindi a^2 è dispari.

(\Leftarrow) Supponiamo che a sia pari, con $a = 2k$. Allora $a^2 = 4k^2 = 2(2k^2) = 2k'$, con $k' = 2k^2$, e quindi a^2 è pari. \diamond

ESERCIZIO 1.11. Definiamo “numero magico” un numero che è pari alla somma delle sue cifre. Dimostrare per assurdo che non esistono numeri magici di 2 o più cifre. \diamond

ESERCIZIO 1.12. Definiamo “numero strano” un numero che è pari al prodotto delle sue cifre. Dimostrare per assurdo che non esistono numeri strani di 2 o più cifre. \diamond

ESERCIZIO 1.13. Si dimostri che due naturali a e b sono entrambi dispari se e solo se il loro prodotto $a \times b$ è dispari. \diamond

1.3 Insiemi

L'*insieme* è un concetto primitivo, che non può essere definito se non con un sinonimo (e.g., collezione, gruppo, aggregato). Le entità che compongono un insieme sono dette i suoi *elementi*. In sostanza, l'insieme è un'astrazione che ci permette di considerare una pluralità (gli elementi) come un singolo (l'insieme stesso). Diciamo che gli elementi *appartengono* all'insieme, e che quest'ultimo *contiene* i suoi elementi.

Il concetto di insieme è assai comune nella lingua quotidiana, dove ha un significato molto più sfumato rispetto a quello che si richiede agli insiemi da un punto di vista matematico. In matematica, perchè A sia un insieme, deve esistere un predicato che risulta vero per ogni elemento dell'insieme e falso per ogni altro elemento possibile. Questo predicato definisce la proprietà che caratterizza l'insieme. Ad esempio

$$A = \text{l'insieme di tutte le ragazze belle}$$

non è un insieme nel senso matematico del termine, in quanto è difficile pensare che esista oggettivamente la proprietà di essere “una ragazza bella”. Sicuramente il concetto di bellezza è molto soggettivo (la bellezza è nell'occhio di chi guarda...). Inoltre, non è ben chiaro neppure cosa si debba intendere per “ragazza”. Fino

a che età una donna è una ragazza? 18 anni? 24? 22 anni 3 mesi e 7 giorni? Volendo poi essere pignoli all'estremo, anche stabilire se una persona è una femmina o un maschio può essere in alcuni casi difficile (si pensi al caso suscitato ai giochi olimpici di Pechino 2008 dalla campionessa degli 800 metri che è stata accusata dalle sue avversarie di essere in realtà un maschio....).

Si consideri, d'altro canto, il seguente insieme:

$$B = \text{l'insieme di tutti i numeri primi compresi tra } 2^{1000} \text{ e } 2^{2000}$$

Per quanto anche questo insieme presenti enormi insidie, da un punto di vista pratico, nello stabilire quali siano i suoi elementi (è molto complesso determinare se un numero “grande” è primo o composto) la proprietà che li caratterizza è precisa ed inequivocabile, e quindi B è un insieme perfettamente definito nel senso matematico del termine.

Nel resto del testo, daremo per scontata la familiarità del lettore con i seguenti insiemi notevoli:

- \mathbb{N} , l'insieme dei numeri *naturali*. L'insieme dei naturali positivi verrà indicato con \mathbb{N}^+ .
- \mathbb{Z} , l'insieme dei numeri *interi*.
- \mathbb{Q} , l'insieme dei numeri *razionali*.
- \mathbb{R} , l'insieme dei numeri *reali*.

Dato un insieme A , il numero dei suoi elementi è detto la sua *cardinalità*, ed è indicato con la notazione $|A|$. Diciamo che A è un *insieme finito* quando $|A|$ è un numero naturale, mentre in caso contrario diciamo che A è un *insieme infinito* (ad esempio, sono infiniti l'insieme dei numeri primi, l'insieme dei numeri pari, ecc.)

Se A è un insieme, scrivendo $a \in A$ (da leggersi a appartiene ad A), indichiamo che a è un elemento di A . Simmetricamente, lo stesso significato si ha usando la scrittura $A \ni a$, anche se in questo caso l'enfasi è posta sul fatto che A contiene a . Per quel che riguarda la non-appartenenza, scrivendo $b \notin A$, indichiamo il fatto che b non è un elemento di A .

Un insieme può essere descritto in vari modi:

- Se l'insieme ha bassa cardinalità, se ne possono elencare esplicitamente gli elementi, racchiusi fra parentesi graffe:

$$A_1 = \{1, 4, \sqrt{\pi}\}$$

$$A_2 = \{\text{rosso, giallo, blu, viola}\}$$

- se l'insieme è infinito, oppure è finito ma la sua cardinalità non è bassa, e quindi non siamo in grado di elencarne esplicitamente tutti gli elementi, possiamo utilizzare una descrizione “a parole” (o tramite formule matematiche, o un mix dei due), della regola che definisce l'appartenenza o meno di un elemento all'insieme. È importante che la descrizione risulti inequivocabile:

$$B_1 = \{x \mid x \text{ è un numero primo } < 100\}$$

$$B_2 = \{\text{tutti i punti } p \text{ a distanza minore di 0.5cm da un punto } p' \text{ assegnato}\}$$

$$B_3 = \{3x | x \in \mathbb{N}\}.$$

L'esempio B_1 utilizza una notazione molto generale, i.e.,

$$\{x | P(x)\} \quad (1.4)$$

dove $P(x)$ è un predicato dipendente da x . Il senso della scrittura di cui sopra è “*l'insieme di tutti gli x che soddisfano il predicato P* ” ossia “*tutti gli x tali che $P(x)$ è vero*”. In questa scrittura, la barra verticale $|$ ha il significato di *tali che* (alternativamente, lo stesso significato si può ottenere scrivendo due punti, come in $\{x : P(x)\}$). L'esempio B_3 è un caso “compresso” di notazione (1.4) (un leggero abuso di notazione che però, risultando di chiara comprensione, ci permette di esprimerci in modo più conciso). Volendo ricondurci alla forma più canonica, avremmo potuto scrivere

$$\{x | (\exists y \in \mathbb{N} | x = 3y)\}.$$

Chiaramente, si tratta dell'insieme dei multipli non-negativi di 3.

In alcuni casi, la proprietà che contraddistingue un insieme può risultare intuibile listandone solo alcuni elementi, in modo che viene lasciata al lettore la deduzione dei rimanenti. Ad esempio, $\mathbb{N} = \{0, 1, 2, \dots\}$, $\mathbb{Z} = \{0, 1, -1, 2, -2, \dots\}$, ecc. Utilizzando questo tipo di descrizione, l'insieme B_3 potrebbe venire indicato come

$$\{0, 3, 6, 9, 12, \dots\}$$

Ovviamente, nell'elencare gli elementi di un insieme si cercherà di farlo nel modo più opportuno. Ad esempio, l'insieme di tutti i multipli di 3 è deducibile elencandone i primi elementi nell'ordine crescente, mentre diventerebbe impossibile la sua deduzione se esso fosse stato descritto come

$$\{24, 303, 0, 6, 18, \dots\}$$

Si noti che un insieme rimane lo stesso indipendentemente sia dall'ordine con cui i suoi elementi vengono elencati, che dalle eventuali ripetizioni di ciascun elemento. Quindi, l'insieme $\{1, 2, 5\}$ è lo stesso che $\{5, 1, 2\}$ ed anche che $\{1, 2, 1, 5\}$ o $\{5, 5, 5, 5, 2, 1, 1\}$.

Insieme vuoto, universo e complementare. Un insieme molto speciale è quello che non contiene alcun elemento, detto *insieme vuoto*. L'insieme vuoto è indicato con il simbolo \emptyset ed ha chiaramente cardinalità 0.

Dati un insieme A e un insieme B , se avviene che ogni elemento di A è anche elemento di B , allora diciamo che A è un *sottoinsieme* di B (o che B è un *sovrainsieme* di A), e scriviamo

$$A \subseteq B$$

oppure

$$B \supseteq A.$$

Ovviamente, per ogni B si ha $\emptyset \subseteq B$, ed anche $B \subseteq B$. Qualche studente ha difficoltà ad accettare che $\emptyset \subseteq B$, in quanto la nostra definizione di sottoinsieme richiede che “ogni elemento del sottoinsieme sia

anche elemento del sovrainsieme”. Siccome, in questo caso, il sottoinsieme non ha elementi, come fa *ogni* suo elemento a soddisfare una certa proprietà? Se la cosa risulta più semplice, possiamo allora pensare ad una caratterizzazione equivalente, però posta nella forma negata. Dire che ogni elemento di un sottoinsieme è contenuto nel sovrainsieme è esattamente lo stesso che affermare *non esistono elementi del sottoinsieme che non sono contenuti nel sovrainsieme*. Questo è palesemente vero quando il sottoinsieme è vuoto, visto che per lui non esistono elementi punto. Se poi vogliamo una definizione terra-terra di sottoinsieme, che comunque convoglia tutto il significato importante del concetto, possiamo dire questo: “i sottoinsiemi di B sono tutti e soli gli insiemi che possono essere ottenuti rimuovendo qualche elemento -al limite nessuno- da B ”.

Si noti che la definizione di sottoinsieme non esclude che sia $A = B$. Se inoltre $A \subseteq B$ ma $A \neq B$, allora diciamo che A è un sottoinsieme *proprio* di B , e scriviamo

$$A \subset B$$

(Qualche autore, per porre maggior enfasi sul fatto che A e B sono insiemi diversi, preferisce utilizzare la notazione $A \subsetneq B$, e dà alla notazione $A \subset B$ lo stesso significato di $A \subseteq B$.)

Se avviene che $A \subseteq B$ e $B \subseteq A$, allora $A = B$. È fondamentale realizzare l'importanza della relazione appena descritta: per dimostrare che due insiemi A e B sono uguali, *bisogna dimostrare due cose*:

1. che ogni elemento di A è anche elemento di B (ossia che $A \subseteq B$)
2. che ogni elemento di B è anche elemento di A (ossia che $B \subseteq A$).

È importante distinguere la nozione di appartenenza da quella di sottoinsieme, anche se alle volte possono esserci delle situazioni in cui le due sembrano confondersi. Ad esempio, se $A = \{a, b, \{a\}, \{a, b\}\}$ si ha

$$\emptyset \subset A; a \in A; \{a\} \in A \text{ ma anche } \{a\} \subset A; \{\{a\}\} \subset A; \{a, b\} \in A \text{ ma anche } \{a, b\} \subset A; A \subseteq A.$$

Dato un insieme A , l'insieme dei suoi sottoinsiemi è detto *insieme delle parti* di A , indicato anche con $\mathcal{P}(A)$. Ad esempio, se $A = \{a, b, c\}$, si ha

$$\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

Molto spesso, nel parlare di insiemi in un determinato contesto, si fa l'ipotesi (a volte sottintesa) che gli elementi di questi insiemi siano presi sempre da un opportuno sovrainsieme detto *universo*. Ad esempio, parlando di insiemi di numeri (ad esempio numeri pari, o primi, ecc), si può supporre che l'universo sia l'insieme dei numeri naturali \mathbb{N} . Quando è stato fissato l'universo E , dato un insieme A resta definito il suo insieme *complementare* \bar{A} , ossia l'insieme di tutti gli elementi dell'universo che non appartengono ad A :

$$\bar{A} = \{x \mid x \in E \text{ ma } x \notin A\}$$

Ad esempio, il complementare dell'insieme dei numeri primi (rispetto ai numeri naturali) è l'insieme dei numeri composti. Si noti che, se non fosse definito un universo, $\bar{A} = \{x \mid x \notin A\}$ conterrebbe “tutto ciò che non appartiene ad A ” senza limiti: quindi, se A è l'insieme dei numeri primi, anche il mio gatto apparterebbe a \bar{A} .

Unione e intersezione. Le principali operazioni definite sugli insiemi sono l'unione

$$A \cup B = \{x \mid (x \in A) \vee (x \in B)\} \quad (1.5)$$

e l'intersezione

$$A \cap B = \{x \mid (x \in A) \wedge (x \in B)\}. \quad (1.6)$$

Unione e intersezione sono operazioni simmetriche

$$A \cup B = B \cup A; \quad A \cap B = B \cap A.$$

Inoltre, per esse vale la proprietà *associativa*, che permette di rimuovere le parentesi in una sequenza di unioni o intersezioni:

$$(A \cup B) \cup C = A \cup (B \cup C) = A \cup B \cup C$$

$$(A \cap B) \cap C = A \cap (B \cap C) = A \cap B \cap C.$$

Sia E l'insieme universo. Allora

$$A \cup \emptyset = A; \quad A \cup E = E; \quad A \cup A = A$$

mentre

$$A \cap \emptyset = \emptyset; \quad A \cap E = A; \quad A \cap A = A.$$

Da $X \supseteq A$, $X \supseteq B$, segue $X \supseteq A \cup B$. Questa proprietà può essere anche parafrasata dicendo che $A \cup B$ è il “minimo” dei sovrainsiemi comuni ad A e B . Analogamente, da $X \subseteq A$ e $X \subseteq B$ segue $X \subseteq A \cap B$. Questa proprietà può essere anche parafrasata dicendo che $A \cap B$ è il “massimo” dei sottoinsiemi comuni ad A e B .

Dati due insiemi A e B , definiamo la differenza

$$A - B = \{x \mid x \in A \wedge x \notin B\} \quad (1.7)$$

e la differenza simmetrica

$$A \Delta B = (A - B) \cup (B - A). \quad (1.8)$$

La differenza $A - B$ non è un'operazione simmetrica, ed anzi, si ha sempre $A - B \neq B - A$ tranne quando $A = B$. L'insieme $A - B$ consiste di tutti gli elementi di A che non appartengono a B . In particolare, $(A - B) \cup (A \cap B) = A$.

Due insiemi A e B si dicono *disgiunti* se $A \cap B = \emptyset$. Dato un insieme E e una famiglia A_1, A_2, \dots, A_k di sottoinsiemi non vuoti di E , diciamo che gli A_i sono una *partizione* di E se

1. $A_1 \cup A_2 \cup \dots \cup A_k = E$
2. $A_i \cap A_j = \emptyset$ per ogni $i, j \in \{1, \dots, k\}$, con $i \neq j$.

Quando si prende l'unione (o l'intersezione) di una famiglia di insiemi del tipo dell'esempio precedente, possiamo utilizzare le seguenti notazioni compatte:

$$\bigcup_{i=1,\dots,k} A_i \quad \bigcap_{i=1,\dots,k} A_i.$$

Se B è un sottoinsieme di un insieme S , il complementare di B rispetto ad S (indicato con \bar{B} , quando il sovrainsieme S è implicito) risulta essere $\bar{B} = S - B$.

Le **leggi di De Morgan** mettono in relazione le operazioni di unione e intersezione con il complementare:

$$\overline{A \cup B} = \bar{A} \cap \bar{B} \quad (1.9)$$

$$\overline{A \cap B} = \bar{A} \cup \bar{B}. \quad (1.10)$$

(le si dimostrino per esercizio.)

Per la cardinalità si hanno le seguenti relazioni (lo si dimostri per esercizio):

$$0 \leq |A \cap B| \leq \max\{|A|, |B|\} \leq |A \cup B| \leq |A| + |B| \quad (1.11)$$

$$|A \cup B| = |A| + |B| - |A \cap B|. \quad (1.12)$$

Prodotto di insiemi. Dati due insiemi A e B , resta definito il loro *insieme prodotto*

$$C := A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

Ogni elemento di C viene detto una *coppia*. Le coppie sono ottenute scegliendo in tutti i modi possibili due elementi, uno di A , detto il primo elemento della coppia, ed uno di B , detto il secondo elemento. Si noti che l'ordine degli elementi nella coppia è importante, sicchè $(a, b) \neq \{a, b\}$. Inoltre, se $(a, b) \in C$ non è detto che anche $(b, a) \in C$ (basti pensare al caso $A \neq B$).

Quando $A = B$, si ha il prodotto di un insieme con se stesso, che viene anche indicato con la notazione A^2

$$A^2 = \{(a, b) \mid a, b \in A\}.$$

Ad esempio,

$$\{1, 2, 3\}^2 = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}.$$

Un caso familiare di prodotto di un insieme con se stesso è quello dei punti del piano. È noto che ogni punto del piano può essere individuato da una coppia di coordinate (dette coordinate cartesiane) (x, y) , dove x e y sono dei numeri reali, e quindi il piano stesso Π può essere interpretato come il prodotto $\Pi = \mathbb{R} \times \mathbb{R} = \mathbb{R}^2$.

Il prodotto di insiemi può essere esteso a tre o più insiemi. Ad esempio,

$$A \times B \times C = \{(a, b, c) \mid a \in A, b \in B, c \in C\}.$$

Ogni elemento di $A \times B \times C$ è detto una *trippla*. Un caso familiare di prodotto di insiemi è quello dello spazio tridimensionale, corrispondente al prodotto $\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$. In modo perfettamente analogo, il prodotto di insiemi può essere esteso al caso di n insiemi A_1, A_2, \dots, A_n ,

$$A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n) \mid a_i \in A_i \text{ per } i = 1, \dots, n\}.$$

Una scrittura alternativa per indicare il prodotto di n insiemi A_i è la seguente:

$$\prod_{i=1, \dots, n} A_i.$$

Ogni elemento (a_1, \dots, a_n) dell'insieme prodotto è detto una *n-pla*. Il prodotto di un insieme con se stesso per n volte è anche chiamato la *potenza n-ma* dell'insieme, $A^n = A \times A \times \dots \times A$.

Esercizi.

ESERCIZIO 1.14. Può un insieme di mele essere uguale ad un insieme di pere? ◇

ESERCIZIO 1.15. Sia $E = \{9k \mid k = 0, 1, 2, 3, \dots\}$. Si discuta per quali valori di n, m (numeri naturali positivi) i seguenti numeri appartengono o meno E :

$6^n, 9n + 1, (3n + 1)(3n + 5) + 3, 3m + 6n$, il massimo numero che può uscire alla roulette per n volte di fila. ◇

ESERCIZIO 1.16. Fra ogni coppia dei quattro insiemi seguenti di numeri naturali vale una relazione di inclusione:

1. $\{3n \mid 1 \leq n \leq 30, n \in \mathbb{N}\}$
2. $\{3^n \mid n = 1, 2, 3, 4\}$
3. $\{n^2 \mid n = 3, 9\}$
4. $\{1, 2, 3, \dots, 100\}$

Disporre i quattro insiemi in ordine crescente per inclusione. ◇

ESERCIZIO 1.17. Si dimostri che se $A_1 \subseteq A_2 \subseteq \dots \subseteq A_n \subseteq A_1$, allora $A_1 = A_2 = \dots = A_n$. ◇

ESERCIZIO 1.18. Sia $E = \{1, 2, 3, 4, 5, 6\}$. Si determinino i sottoinsiemi di E che soddisfano alle seguenti condizioni:

1. $X \cup \{1, 2\} = \{1, 2, 6\} \quad \wedge \quad X \cap \{1, 2\} = \{1\}$
2. $X \cap \{1, 2, 3, 4\} = \{3, 4\} \quad \wedge \quad X \cap \{2, 4, 5, 6\} = \{2, 6\}$
3. $(X \cap \{1, 2, 3\} \subseteq \{1, 2, 4\}) \wedge (X \cap \{2, 5, 6\} \subseteq \{2, 6\}) \wedge (X \cap \{2, 4, 6\} \subseteq \{1, 3, 5\})$
4. $X \cap \{3, 4, 5\} \subseteq \{4, 5\} \quad \wedge \quad X \cap \{1, 2, 6\} \subseteq \{2, 6\}$
5. $X \cap \{3, 4, 5\} \supseteq \{4, 5\} \quad \wedge \quad X \cap \{1, 2, 6\} \supseteq \{2, 6\}$

◇

ESERCIZIO 1.19. Sapendo che $|A| = 4$ e $|B| = 8$, quali tra i seguenti valori possono essere $|A \cup B|$: 3, 4, 7, 10, 13? Quali tra i precedenti valori possono essere $|A \cap B|$? ◇

ESERCIZIO 1.20. Le leggi di De Morgan trovano applicazione anche nell'algebra booleana. Si verifichi, tramite le tabelle di verità, che per ogni $A, B \in \{\text{VERO}, \text{FALSO}\}$ si ha

- $\neg(A \vee B) = \neg A \wedge \neg B$
- $\neg(A \wedge B) = \neg A \vee \neg B$

◇

ESERCIZIO 1.21. Sia E un insieme di 20 elementi. Se A e B sono due suoi sottoinsiemi, rispettivamente di 14 e di 10 elementi, quanti possono essere (come minimo e come massimo) gli elementi di

$$A \cup B, A \cap B, A \cup \bar{B}, A \cap \bar{B}, \bar{A} \cup B, \bar{A} \cap B, \bar{A} \cup \bar{B}, \bar{A} \cap \bar{B}.$$

◇

1.4 Relazioni

Sia A un insieme e consideriamo le possibili relazioni fra coppie di elementi di A . Ogni relazione che coinvolge due argomenti x e y si dice *binaria*. Ad esempio:

- Su un insieme di persone:
 - x è padre di y
 - x è amico di y
 - x e y abitano nella stessa via
 - ...
- Su un insieme di numeri:
 - $x < y$
 - x è un divisore di y

- x e y hanno un divisore in comune
- ...
- Su un insieme di insiemi:
 - x è sottoinsieme di y
 - $x \cap y = \emptyset$
 - $|x \cup y| > 10$
 - ...

In generale, una relazione binaria è definita da un predicato P in due variabili. A ogni relazione corrisponde un sottoinsieme R di $A \times A$, dove R è l'insieme delle coppie per cui il predicato risulta vero. Anche la direzione inversa è possibile, ossia per ogni $R \subseteq A \times A$ esiste un predicato (una relazione binaria) tale che R è l'insieme delle coppie che soddisfano il predicato. In particolare la relazione è “la coppia (x, y) appartiene ad R .” Alla luce di ciò, possiamo dire che, sostanzialmente, una relazione binaria è un sottoinsieme di $A \times A$.

Ad esempio, se $A = \{1, 2, 3, 4\}$ e

$$R = \{(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)\},$$

la relazione rappresentata da R è quella di “essere minore di”. Similmente, la relazione “ x è un multiplo di y ” corrisponde all'insieme

$$\{(1, 1), (2, 1), (3, 1), (4, 1), (2, 2), (4, 2), (3, 3), (4, 4)\}.$$

Per denotare che x è in relazione con y , usiamo un simbolo che rappresenta la relazione e che viene scritto fra x e y . Ad esempio,

$$x \smile y, \quad x \leq y, \quad x \ominus y, \quad x \simeq y, \quad x \prec y, \quad x \vdash y, \dots$$

Quindi, scrivere $x \smile y$ è la medesima cosa che scrivere $(x, y) \in R$ dove R è l'insieme di coppie nella relazione “ \smile ”.

Una relazione può godere o meno di alcune importanti proprietà. In particolare, diciamo che una relazione è:

- **Riflessiva:** se $x \smile x$ per ogni $x \in A$. (ad esempio, la relazione “essere alto come” oppure “abitare nella stessa via” in un insieme di persone; un altro esempio è la relazione “essere divisibile per” in un insieme di numeri interi).
- **Irriflessiva:** se $\neg(x \smile x)$ per ogni $x \in A$. (ad esempio, la relazione “essere più vecchio di” oppure “abitare nella casa di fronte a” in un insieme di persone; un altro esempio è la relazione “essere coprimo con”, oppure “essere minore di”, nell'insieme dei numeri naturali maggiori di 1).
- **Simmetrica:** se $x \smile y$ implica $y \smile x$ per ogni $x, y \in A$. (ad esempio, la relazione “essere fratello di” in un insieme di persone di sesso maschile, oppure “essere collega di lavoro”; un altro esempio è la relazione “il prodotto di x e y vale 100” in un insieme di numeri interi).

- **Antisimmetrica:** se $x \sim y \implies \neg(y \sim x)$, per ogni $x, y \in A$ con $x \neq y$. (ad esempio, la relazione “essere padre di” in un insieme di persone di sesso maschile, oppure la relazione “ $x > y$ ” in un insieme di numeri).
- **Transitiva:** se $(x \sim y) \wedge (y \sim z) \implies (x \sim z)$, per ogni $x, y, z \in A$. (ad esempio, la relazione “essere collega di lavoro”, o “avere lo stesso nome proprio” in un insieme di persone, oppure la relazione “ $x > y$ ” o “essere divisibile per” in un insieme di numeri).

Le relazioni d'ordine.

Una relazione che sia (i) irreflessiva, (ii) antisimmetrica, e (iii) transitiva, viene detta una *relazione d'ordine* sull'insieme A .[¶] Tipicamente, riserviamo il simbolo “ \prec ” per rappresentare una relazione d'ordine, e per ogni coppia (a, b) tale che $a \prec b$ diciamo che “ a precede b ”. Data una relazione d'ordine, si possono verificare due possibilità:

- Per ogni coppia di elementi distinti $a, b \in A$ si ha che a precede b o b precede a .
- Esistono coppie di elementi distinti tali che nè $a \prec b$ nè $b \prec a$. Elementi siffatti vengono detti *inconfrontabili*.

Se rispetto a una relazione d'ordine non esistono elementi inconfrontabili, allora si parla di un *ordine totale*. Non è difficile dimostrare (ad esempio ragionando per assurdo) che se A è un insieme finito e \prec è un ordine totale, esistono un primo elemento di A (i.e., un elemento che precede tutti gli altri), e un ultimo elemento di A (i.e., un elemento che non ne precede alcun altro). Inoltre, ogni elemento tranne il primo è preceduto da esattamente un elemento di A , ed ogni elemento tranne l'ultimo precede esattamente un elemento di A .

Vediamo alcuni esempi:

- Su $A = \mathcal{P}(\{1, \dots, n\})$ consideriamo la relazione di inclusione stretta \subset . È facile verificare che si tratta di una relazione d'ordine. In particolare, l'ordine non è totale in quanto possono esistere elementi inconfrontabili, quali, ad esempio, $\{1, 2\}$ e $\{1, 3\}$.
- La relazione $<$ è un ordine totale sull'insieme dei numeri reali, come è facile verificare.
- Su un insieme A di persone, definiamo la relazione “è discendente di” al seguente modo: x è discendente di y se esiste una sequenza (x_1, \dots, x_k) di $k \geq 2$ persone tale che $x_1 = x$, $x_k = y$ e x_i è figlio di x_{i+1} per ogni $i = 1, \dots, k-1$. Dimostriamo che si tratta di una relazione d'ordine. Partiamo con l'osservare come il fatto che x sia un discendente di y implica che x sia più giovane di y , e quindi la relazione è necessariamente irreflessiva e antisimmetrica. Per quel che riguarda la transitività, supponiamo che x sia un discendente di y e y sia un discendente di z . Esistono allora sequenze $(x = x_1, \dots, x_h = y)$ e $(y = y_1, \dots, y_t = z)$ tali che x_i è figlio di x_{i+1} per ogni $i = 1, \dots, h-1$ e y_i è figlio di y_{i+1} per ogni

[¶]Alcuni autori preferiscono definire le relazioni d'ordine come relazioni riflessive. Questo può portare a delle situazioni poco naturali, come ad esempio il fatto che ogni elemento preceda se stesso nell'ordine. Formalmente, la relazione \leq fra i numeri reali, essendo riflessiva, non sarebbe una relazione d'ordine in base alla nostra definizione, ma, allo stesso modo, la relazione $<$, essendo irreflessiva, non sarebbe una relazione d'ordine per tali autori. Nella sostanza, le proprietà importanti nel definire una relazione d'ordine sono la transitività e l'antisimmetria, per cui tipicamente si finisce col chiamare *relazioni d'ordine irreflessive* (o *strette*) le relazioni come le abbiamo definite noi, e *relazioni d'ordine riflessive* (o *larghe*) le altre.

$i = 1, \dots, t-1$. È immediato verificare che la sequenza $(x = x_1, \dots, x_k, y_2, \dots, y_t = z)$ soddisfa le condizioni per concludere che x è un discendente di z . Notiamo infine come la relazione in questione non sia un ordine totale.

- **L'ordine lessicografico:** Sia \prec un ordine totale su un insieme A . Partendo da \prec , si può definire un nuovo ordinamento totale, detto *ordine lessicografico* e denotato anch'esso con \prec , sull'insieme di tutti i vettori a componenti in A . Siano $a = (a_1, \dots, a_n)$ e $b = (b_1, \dots, b_m)$ due vettori distinti (non necessariamente della stessa dimensione), a componenti in A . Senza perdita di generalità assumiamo $n \leq m$. Il vettore a precede b nell'ordine lessicografico se (i) $a_i = b_i$ per $i = 1, \dots, n$, (nel qual caso è $n < m$), oppure (ii) esiste k , con $1 \leq k \leq n$, tale che $a_i = b_i$ per $i = 1, \dots, k-1$ e $a_k \prec b_k$. In base al caso (i), si ha $(3, 2, 5) \prec (3, 2, 5, 1, 4)$, e (C, A, N, E) precede (C, A, N, E, S, T, R, O) . In base al caso (ii) si ha che $(3, 2, 3, 6) \prec (3, 2, 5, 1, 4)$ e che $(C, A, N, E, S, T, R, O) \prec (C, A, N, I, L, E)$. Quando A è un alfabeto, l'ordine lessicografico indotto dall'ordine delle lettere si identifica con l'ordine alfabetico di tutte le parole su A .
- Consideriamo il popolare gioco sasso/carta/forbice e un insieme di strategie per lo stesso. Ogni strategia è una tripla di numeri non-negativi (s, c, f) , tali che $s + c + f = 1$, rappresentanti le probabilità con cui lanciare, rispettivamente, sasso, carta o forbice ad ogni turno di gioco. Ad esempio, la strategia $(\frac{1}{3}, \frac{1}{3}, \frac{1}{3})$ consiste nello scegliere in maniera causale uniforme la mossa da effettuare. Sull'insieme delle strategie, definiamo la relazione “essere migliore di” al seguente modo: la strategia x è migliore della strategia y se, ad ogni turno di gioco, la probabilità di vincere adottando x contro un avversario che adotta y è maggiore che non adottando y contro un avversario che adotta x . Ad esempio, la strategia $x = (\frac{2}{3}, \frac{1}{3}, 0)$ è migliore di $y = (\frac{1}{2}, 0, \frac{1}{2})$ in quanto è possibile dimostrare^{||} che x vince con probabilità $1/2$ e y vince con probabilità $1/6$.

La relazione “essere migliore di” *non* è una relazione d'ordine. Infatti, pur essendo irreflessiva e anti-simmetrica, per essa non vale la proprietà transitiva. Un semplice esempio è dato dalle tre strategie $a = (1, 0, 0)$, $b = (0, 1, 0)$ e $c = (0, 0, 1)$. Abbiamo che c è migliore di b , b è migliore di a , ma a è migliore di c . Questo fenomeno vale per molti giochi dove è difficile stabilire una relazione d'ordine basata sul concetto di “più forte” tra giocatori. Ad esempio, nel tennis è assai frequente il caso di tre giocatori ognuno dei quali vince regolarmente con uno degli altri due ma perde con il secondo.

Le equivalenze.

Quando una relazione è (i) riflessiva, (ii) simmetrica, e (iii) transitiva, essa viene detta un'*equivalenza*. Tipicamente, riserviamo il simbolo “ \sim ” per rappresentare una relazione di equivalenza. Vediamo alcuni esempi:

- La relazione $x = y$ è banalmente un'equivalenza. Lasciamo al lettore la facile dimostrazione.
- Consideriamo la relazione su \mathbb{N} definita da “l'insieme dei divisori primi di x è lo stesso che quello dei divisori primi di y ”. Ad esempio $x = 30 = 5 \times 3 \times 2$ è in relazione con $y = 90 = 5 \times 3^2 \times 2$ perchè l'insieme dei fattori primi $\{2, 3, 5\}$ è lo stesso. Dimostriamo che si tratta di un'equivalenza:

(R:) $x \sim x$ sempre. Questo è ovvio.

(S:) se $x \sim y$, allora i divisori primi di y sono gli stessi che quelli di x e quindi $y \sim x$.

^{||}Si veda la sezione 1.9 sul calcolo delle probabilità.

(T:) se i divisori primi di x sono gli stessi che quelli di y , e quelli di y gli stessi che quelli di z , allora anche i divisori di x e di z sono gli stessi e quindi vale $x \sim z$.

- Sia A l'insieme delle rette nel piano. Per ogni coppia di rette x e y , diciamo che $x \sim y$ se x e y sono rette parallele (ossia, l'intersezione di x e y non consiste di un unico punto). Verifichiamo che si tratta di un'equivalenza. Dalla geometria sappiamo che:

(R:) ogni retta è parallela a se stessa.

(S:) se x è parallela a y , allora y è parallela a x .

(T:) se x è parallela a y , e y è parallela a z , anche x e z sono parallele.

- Sia A l'insieme $\{(p, q) \mid p \in \mathbb{Z}, q \in \mathbb{Z} - \{0\}\}$. Diciamo che $(p, q) \sim (p', q')$ se $pq' = p'q$. Ad esempio $(4, 3) \sim (12, 9)$, e $(3, -2) \sim (-6, 4)$. Dimostriamo che si tratta di un'equivalenza:

(R:) Siccome $pq = pq$, si ha $(p, q) \sim (p, q)$

(S:) Siccome $pq' = p'q$ implica $p'q = pq'$, allora $(p, q) \sim (p', q')$ implica $(p', q') \sim (p, q)$.

(T:) Dati $(p, q), (p', q'), (p'', q'') \in A$, supponiamo $pq' = p'q$ e $p'q'' = p''q'$. In particolare, $p/q = p'/q'$ e $p'/q' = p''/q''$, da cui $pq'' = p''q$. Quindi $(p, q) \sim (p', q')$ e $(p', q') \sim (p'', q'')$ implicano $(p, q) \sim (p'', q'')$.

ESERCIZIO 1.22. Date le seguenti relazioni, definite su un insieme di persone A , si determini per ciascuna di esse quali proprietà sono soddisfatte e quali no. Si dica quali tra queste relazioni sono delle equivalenze.

1. x abita nella stessa città di y
2. x è cugino/a di y
3. x e y hanno frequentato, almeno per un anno, la stessa scuola durante i loro studi
4. x è padre di y
5. x è nato nello stesso anno di y
6. x è più giovane di y
7. x è fratello (o sorella) di y (nel senso che x e y hanno entrambi i genitori in comune)
8. x è fratellastro (o sorellastra) di y (nel senso che x e y hanno esattamente un genitore in comune).

◇

Ogni relazione di equivalenza su A ripartisce l'insieme A nelle cosiddette *classi* dell'equivalenza. Per ogni elemento $a \in A$, la classe di a viene indicata con $[a]$ ed è definita come

$$[a] = \{x \in A \mid x \sim a\}.$$

L'insieme $\{[a] \mid a \in A\}$ delle classi dell'equivalenza viene chiamato *insieme quoziente* di A rispetto a \sim , ed è indicato con (A/\sim) . Verifichiamo ora che $\{[a] \mid a \in A\}$ definisce effettivamente una partizione di A .

1. Ogni classe è non vuota: Infatti, per definizione, per ogni $a \in A$, $[a]$ ha almeno l'elemento a .
2. L'unione delle classi è A : Infatti, ogni elemento $a \in A$ è in una delle classi.
3. Le classi distinte sono disgiunte: Consideriamo $[a]$ e $[b]$, con $a, b \in A$. Se esistesse $x \in [a] \cap [b]$, si avrebbe $x \sim a$ e $x \sim b$. Dalle proprietà simmetrica e transitiva dell'equivalenza, seguirebbe $a \sim b$. Quindi, per ogni $x \in [a]$ si avrebbe $x \sim a \sim b$ e quindi $x \in [b]$, ossia $[a] \subseteq [b]$. Allo stesso modo $(x \in [b]) \implies (x \in [a])$ e quindi $[b] \subseteq [a]$. Si conclude che $[a] = [b]$.

Riconsideriamo due delle equivalenze degli esempi precedenti:

1. Sull'insieme A delle rette nel piano, abbiamo $x \sim y$ se x e y sono rette parallele. Se da ogni classe dell'equivalenza cerchiamo di astrarre la proprietà comune a tutti gli elementi di quella classe, otteniamo il concetto di *direzione*.
2. Sull'insieme A di coppie $\{(p, q) \mid p \in \mathbb{Z}, q \in \mathbb{Z} - \{0\}\}$, abbiamo $(p, q) \sim (p', q')$ se $pq' = p'q$. Se da ogni classe dell'equivalenza cerchiamo di astrarre la proprietà comune a tutti gli elementi di quella classe, otteniamo il concetto di *numero razionale*. Infatti, ogni coppia della classe $[(p, q)]$ corrisponde al medesimo numero razionale, i.e., $\frac{p}{q}$.

ESERCIZIO 1.23. Si consideri la relazione \sim sull'insieme $A = \{1, 2, \dots, 1000\}$ definita da

$$a \sim b \iff (a = b) \vee (\text{MCD}(a, b) \text{ è pari}).$$

Si determini se \sim è un'equivalenza. Se non lo è, si dica quali delle proprietà di un'equivalenza non sono soddisfatte. Se lo è, si dica quante sono le classi dell'equivalenza. \diamond

Congruenza modulo n . Dato un numero naturale $n > 0$, ogni numero intero a può essere espresso, in un unico modo, come

$$a = q \times n + r \tag{1.13}$$

con $q, r \in \mathbb{Z}$ e $0 \leq r < n$. In questa operazione, a è detto il *dividendo*, n è il *divisore*, q è il *quoziente*, mentre r è il *resto* di a nella divisione per n . Il quoziente nella divisione intera viene anche denotato con $a \text{ div } n$, mentre il resto con $a \bmod n$. Se $a \bmod n = 0$, allora diciamo che a è un *multiplo* di n o, equivalentemente, che n *divide* a .

Lasciamo allo studente la verifica dell'esistenza di almeno una coppia (q, r) che soddisfa (1.13) e dimostriamo l'unicità di tale coppia. Consideriamo due coppie (q_1, r_1) e (q_2, r_2) tali che $a = q_1 n + r_1 = q_2 n + r_2$ con $0 \leq r_1 < n$ e $0 \leq r_2 < n$. Supponiamo, che sia $r_2 > r_1$. Si ha allora

$$0 < r_2 - r_1 < n$$

e quindi $(q_1 - q_2)n = r_2 - r_1$ sarebbe un multiplo positivo di n strettamente inferiore ad n . Questo è ovviamente assurdo, e perciò non può essere $r_2 > r_1$. Analogamente si dimostra che non può essere $r_1 > r_2$. Quindi, si ha $r_1 = r_2$, da cui $(q_1 - q_2)n = 0$, e quindi $q_1 = q_2$.

Fissato $n \in \{1, 2, 3, \dots\}$, consideriamo ora la relazione su \mathbb{Z} definita da $x \sim y$ se e solo se il resto di x nella divisione per n è lo stesso del resto di y nella divisione per n . Tale relazione si chiama *congruenza modulo n* e si tratta (come può essere banalmente verificato) di una relazione di equivalenza.

La relazione di congruenza modulo n viene spesso denotata con

$$x \equiv_n y$$

oppure con

$$x \equiv y \pmod{n}$$

Abbiamo quindi $12 \equiv_{10} 2$ ed anche $-8 \equiv_{10} 2$. Inoltre $20 \equiv_5 5 \equiv_5 15 \equiv_5 0$. Si ha $2 \equiv_8 -6$ eccetera. Se $n = 5$, le classi dell'equivalenza risultano

$$[0] = \{\dots, -15, -10, -5, 0, 5, 10, 15, 20, \dots\}$$

$$[1] = \{\dots, -14, -9, -4, 1, 6, 11, 16, \dots\}$$

$$[2] = \{\dots, -13, -8, -3, 2, 7, 12, 17, \dots\}$$

$$[3] = \{\dots, -12, -7, -2, 3, 8, 13, 18, \dots\}$$

$$[4] = \{\dots, -11, -6, -1, 4, 9, 14, 19, \dots\}$$

Vediamo ora una caratterizzazione alternativa della congruenza modulo n , data dal seguente lemma:

Lemma 1: Siano $x, y \in \mathbb{Z}$. Si ha $x \equiv_n y$ se e solo se $x - y$ è un multiplo di n .

Dim: (Se:) Supponiamo $x \equiv_n y$, e, in particolare, siano $q_1, q_2 \in \mathbb{Z}$ e $0 \leq r < n$ tali che $x = q_1n + r$ e $y = q_2n + r$. Allora $x - y = (q_1 - q_2)n$. (Solo se:) Sia $q \in \mathbb{Z}$ tale che $x - y = qn$. Siano q_1, q_2 e r_1, r_2 quozienti e resti per i quali si ha $x = q_1n + r_1$, $y = q_2n + r_2$. Abbiamo

$$x - y = (q_1 - q_2)n + (r_1 - r_2) = qn$$

e quindi

$$r_1 - r_2 = (q - q_1 + q_2)n$$

Essendo $0 \leq r_1, r_2 < n$, l'unico multiplo di n possibile per $r_1 - r_2$ è $0n = 0$. Quindi $r_1 = r_2$ da cui $x \equiv_n y$.

Nella vita di tutti i giorni abbiamo spesso a che fare con equivalenze modulari:

- I giorni sono ripartiti in 7 classi di equivalenza (i giorni della settimana). Sappiamo che se oggi è lunedì tra 14 giorni sarà ancora lunedì, perchè la differenza di date è un multiplo di 7.
- In modo simile, i mesi sono ripartiti in 12 classi di equivalenza: ogni 12 mesi si ripete lo stesso mese.
- Le ore di tutti i giorni sono ripartite in 24 classi di equivalenza.
- Gli angoli (interi) possono essere ripartiti in 360 classi di equivalenza. Un angolo di 370 gradi è equivalente a uno di 10 gradi.

L'aritmetica modulare. In modo simile a quanto avviene per le equazioni comuni, anche le equazioni modulo n possono essere manipolate aggiungendo la stessa quantità, o moltiplicando per lo stesso valore a destra e sinistra:

Lemma 2: Siano $x, y \in \mathbb{Z}$ tali che $x \equiv_n y$. Allora, per ogni $z \in \mathbb{Z}$ si ha

1. $x + z \equiv_n y + z$
2. $xz \equiv_n yz$

Dim: Sia $q \in \mathbb{Z}$ tale che $x - y = qn$. (1) Abbiamo $(x + z) - (y + z) = x - y = qn$ e quindi $x + z \equiv_n y + z$; (2) $xz - yz = (x - y)z = (qn)z$ e quindi $xz \equiv_n yz$.

In realtà, perchè un'equazione rimanga valida nell'aritmetica modulare non è necessario sommare la stessa quantità a destra e sinistra, ma la quantità deve essere la medesima modulo n . Allo stesso modo, si può moltiplicare a destra e sinistra per quantità diverse, a patto che siano equivalenti modulo n :

Lemma 3: Siano $x, y \in \mathbb{Z}$ tali che $x \equiv_n y$. Allora, per ogni $z_1, z_2 \in \mathbb{Z}$ tali che $z_1 \equiv_n z_2$ si ha

1. $x + z_1 \equiv_n y + z_2$
2. $xz_1 \equiv_n yz_2$

Dim: Sia $q \in \mathbb{Z}$ tale che $x - y = qn$. Sia inoltre $p \in \mathbb{Z}$ tale che $z_1 - z_2 = pn$. (1) Abbiamo $(x + z_1) - (y + z_2) = (x - y) + (z_1 - z_2) = (q + p)n$ e quindi $x + z_1 \equiv_n y + z_2$; (2) $xz_1 - yz_2 = (qn + y)z_1 - y(z_1 - pn) = (qz_1 + py)n$ e quindi $xz_1 \equiv_n yz_2$.

Vediamo alcuni esempi di aritmetica modulare.

- Assumendo un anno non bisestile, se il 1o Gennaio è un Mercoledì, che giorno sarà il Capodanno? Il Capodanno è il 365-mo giorno, ossia $(1 + 364)$ -mo. Abbiamo $364 \equiv_7 0$ per cui sommare 364 giorni è come sommarne 0, e il Capodanno cadrà di Mercoledì.
- Se una donna rimane incinta in Novembre, in che mese nascerà il bambino? Agosto è l'ottavo mese. La gestazione dura 9 mesi, per cui il bambino nascerà al mese 5 (Maggio) in quanto $5 \equiv_{12} 8 + 9$. Alternativamente, si noti che $9 \equiv_{12} -3$ e quindi, relativamente al mese, sommare 9 mesi a una data è come sottrarne 3.
- In aritmetica modulo 15, quanto vale 2^{100} ? Abbiamo $2^{100} = (2^4)^{25}$. Ma $2^4 \equiv_{15} 1$ per cui $2^{100} \equiv_{15} 1$.
- Quanto vale (12530×114211) modulo 3? Sappiamo dalle scuole elementari che un numero intero è divisibile per 3 se e solo se la somma delle sue cifre è multipla di 3. La somma delle cifre di 12530 è 11, per cui $12530 \equiv_3 2$. La somma delle cifre di 114211 è 10, per cui $114211 \equiv_3 1$. Abbiamo $12530 \times 114211 \equiv_3 2 \times 1 = 2$.

ESERCIZIO 1.24. Sia $A = \{1, 2, \dots, 10\}$. Si determinino delle equivalenze tali che:

1. $|(A/\sim)| = |A|$
2. $|(A/\sim)| = 1$
3. $|(A/\sim)| = |A|/2$
4. $|(A/\sim)| = |A| - 1$

◇

1.5 Funzioni

Dati un insieme A ed un insieme B , una legge f che associa ad ogni elemento di A uno ed un solo elemento di B è detta una *funzione* (o *applicazione* o *mappa*) di A in B . L'insieme A è detto il *dominio* della funzione, mentre B è il suo *codominio*. Si dice che la funzione è *definita su* A ed *assume valori in* B .

Dato $x \in A$, l'elemento $f(x) \in B$ che f associa ad x è detto *l'immagine* di x (o il suo *corrispondente*). Per indicare che f è una funzione di A in B si usa la notazione

$$f : A \mapsto B.$$

Nel definire il concetto di funzione, abbiamo fatto ricorso a delle idee che supponiamo primitive e intuitive, quali “legge” (o “regola”) e “associare”. In modo più formale, avremmo potuto definire una funzione come (equivalente a) un sottoinsieme C_f del prodotto $A \times B$, dove A è il dominio e B il codominio, che soddisfi a questo requisito:

“Per ogni $a \in A$ esiste, ed è unica, una coppia $(a, b) \in C_f$.”

In particolare, la coppia (a, b) specifica l'immagine di a , ossia $f(a) = b$.

Un esempio di funzione è quella definita su tutti i numeri naturali che, ad ogni numero, associa il suo doppio:

$$f(x) = 2x \quad \forall x \in \mathbb{N}.$$

Un altro esempio è la funzione che ha per dominio l'insieme dei residenti del comune di Milano, e per codominio l'insieme di tutti gli esseri umani, e che associa ad ogni persona il suo padre. Non è una funzione, invece, la regola che associa ad ogni residente il suo primogenito, o un soprannome con cui è noto fra i suoi amici (si ragioni su quali sono le condizioni non soddisfatte da queste regole per poterle considerare funzioni).

Per ogni sottoinsieme C di A , resta definito un sottoinsieme di B , ossia

$$f(C) = \{f(x) \mid x \in C\}$$

detto *l'insieme-immagine* di C . L'insieme $f(A)$ è anche detto, brevemente, *l'immagine* di f . Se $|f(A)| = 1$, allora la f viene detta una funzione *costante*.

Quando avviene che $f(A) = B$, allora la funzione è detta *suriettiva*. Quindi, se f è una funzione suriettiva, per ogni elemento y del codominio esiste un elemento x del dominio tale che $y = f(x)$.

Se una funzione porta elementi distinti del dominio in elementi distinti del codominio, allora questa funzione è detta *iniettiva*. Quindi, per una funzione iniettiva, $x_1 \neq x_2$ implica $f(x_1) \neq f(x_2)$.

La funzione che nell'esempio precedente associava ad ogni persona suo padre non è iniettiva (si pensi ai fratelli) nè suriettiva (ci sono persone senza figli).

Quando una funzione è sia iniettiva che suriettiva, essa viene detta *biiettiva* (o una *corrispondenza biunivoca*). In questo caso, per ogni elemento y del codominio, esiste uno ed un solo x del dominio tale che $y = f(x)$. Una corrispondenza biunivoca tra A e B è tutto ciò che serve per affermare che A e B hanno la stessa cardinalità. Questo vale sia per insiemi finiti che per insiemi infiniti.

Un caso speciale di funzione è la *funzione identica* o *identità* i_A , definita su un insieme A . Per essa, il codominio è uguale al dominio, e si ha $i_A(a) = a$ per ogni $a \in A$. Ovviamente, l'identità è sempre una funzione biiettiva.

Esempio. Nella matematica discreta rivestono particolare importanza due funzioni di \mathbb{R} in \mathbb{Z} dette il *pavimento* (floor) e il *soffitto* (ceiling) di un numero. Il pavimento di x , denotato con $\lfloor x \rfloor$, è il massimo intero non maggiore di x , mentre il suo soffitto, denotato con $\lceil x \rceil$, è il minimo intero non inferiore a x . In formule:

$$\lfloor x \rfloor = \max\{v \in \mathbb{Z} \mid v \leq x\}$$

$$\lceil x \rceil = \min\{v \in \mathbb{Z} \mid v \geq x\}.$$

Ad esempio, $\lfloor 1.3 \rfloor = 1$, ma $\lfloor -1.3 \rfloor = -2$; $\lfloor -4 \rfloor = \lceil -4 \rceil = -4$; $\lceil -1.3 \rceil = -1$. ◇

Date due funzioni, $f : A \mapsto B$ e $g : B \mapsto C$, tali che il codominio della prima coincide col dominio della seconda, resta definita una terza funzione,

$$h : A \mapsto C$$

detta *composizione* (o *funzione composta*) di f e g . La funzione composta è definita, per ogni $x \in A$, dalla regola

$$h(x) = g(f(x)).$$

La funzione composta viene anche indicata con gf o con $g \circ f$. La composizione di funzioni è un'operazione associativa, ossia, date tre applicazioni

$$f : A \mapsto B, \quad g : B \mapsto C, \quad h : C \mapsto D$$

risulta

$$h(gf) = (hg)f$$

in quanto, per ogni $x \in A$, si ha $h(gf)(x) = h(gf(x)) = h(g(f(x)))$ ed anche $(hg)f(x) = hg(f(x)) = h(g(f(x)))$.

Ogni applicazione di A in sè è componibile con se stessa. La funzione composta ff è indicata anche con f^2 . In modo analogo, per $n > 2$, definiamo f^n come la composizione di f con se stessa per n volte.

Nell'esempio della funzione f che ad ogni persona associa suo padre, la funzione f^2 ad ogni persona associa il suo nonno paterno. Una funzione f per la quale risulta $f = f^2$ viene detta *idempotente*. Esempi di funzioni idempotenti sono le funzioni costanti, l'identità, il valore assoluto $|x|$, le funzioni pavimento $\lfloor x \rfloor$ e soffitto $\lceil x \rceil$.

Funzione inversa e controimmagini. Quando una funzione $f : A \mapsto B$ è biiettiva, per ogni $y \in B$ esiste, ed è unico, un $x \in A$ tale che $y = f(x)$. La f quindi individua non solo una mappa da A a B , ma anche una mappa da B ad A , ossia la mappa che fa corrispondere ad ogni punto di B il punto di A “da cui proviene”. Questa mappa si chiama la funzione *inversa* di f , ed è indicata con f^{-1} . Quindi:

$$f^{-1}(y) = x \text{ se e solo se } f(x) = y.$$

Dalla definizione stessa di inversa, si ha che $f^{-1}(f(x)) = x$ per ogni $x \in A$, ed anche $f(f^{-1}(y)) = y$ per ogni $y \in B$, e quindi

$$f^{-1}f = i_A, \quad ff^{-1} = i_B. \quad (1.14)$$

Si può dimostrare (lo studente ci provi come esercizio) che la condizione di essere biiettiva è, oltre che sufficiente, anche necessaria perchè la f possieda un'inversa, ossia perchè esista una funzione f^{-1} che soddisfi le condizioni (1.14).

Qualunque sia l'applicazione $f : A \mapsto B$ (e quindi anche se f non fosse invertibile), per ogni sottoinsieme $B' \subseteq B$ esiste un sottoinsieme A' di A (al limite l'insieme vuoto) dato da tutti gli elementi la cui immagine è contenuta in B' . Con un leggero abuso di notazione, si utilizza la scrittura f^{-1} anche per indicare tale sottoinsieme:

$$f^{-1}(B') = \{x \in A \mid f(x) \in B'\}.$$

$A' = f^{-1}(B')$ è detto la *controimmagine*, *tramite la f di B'* . Si noti che in questa accezione, la scrittura f^{-1} di fatto definisce una funzione tra $\mathcal{P}(B)$ e $\mathcal{P}(A)$.

Chiaramente, $f^{-1}(\{y\}) = \emptyset$ se e solo se $y \notin f(A)$, ed $f^{-1}(B') = \emptyset$ se e solo se $B' \cap f(A) = \emptyset$. Inoltre, si ha sempre

$$f^{-1}(B) = f^{-1}(f(A)) = A.$$

Esempio. Dimostriamo che l'applicazione $f : \mathbb{R} \mapsto \mathbb{R}$ definita da $f(x) = ax + b$, con $a \neq 0$, è invertibile, e determiniamone l'inversa.

Innanzitutto, la funzione è iniettiva. Infatti, sia $f(x_1) = f(x_2)$. Allora $ax_1 + b = ax_2 + b$, da cui $ax_1 = ax_2$ e, essendo $a \neq 0$, $x_1 = x_2$. Inoltre, la funzione è suriettiva. Infatti, sia $y \in \mathbb{R}$. Detto $x = (y - b)/a$ si ha $y = a(y - b)/a + b = f(x)$.

Supponiamo ora di cambiare dominio e codominio da \mathbb{R} a \mathbb{Z} . La nuova funzione f è ancora invertibile? La risposta è no. Infatti, per quanto la funzione sia ancora iniettiva, non è più suriettiva. Ad esempio, per $a = 2$ e $b = 1$, il numero $y = 2$ non è immagine di alcun numero, in quanto $1/2 \notin \mathbb{Z}$. \diamond

Esempio. Consideriamo la funzione $f : \mathbb{Z} \times \mathbb{Z} \mapsto \mathbb{Z} \times \mathbb{Z}$ definita da $f(x, y) = (x - 2, 2x - y)$. Dopo aver dimostrato che f è invertibile, determiniamone l'inversa.

Per dimostrare che f è invertibile dobbiamo verificare che è sia iniettiva che suriettiva. Siano allora (x, y) e (x', y') due elementi di \mathbb{Z}^2 . Abbiamo $f(x, y) = f(x', y') \iff (x - 2, 2x - y) = (x' - 2, 2x' - y') \iff (x - 2 = x' - 2) \wedge (2x - y = 2x' - y')$. Dalla prima equazione otteniamo $x = x'$, che, sostituito nella seconda, implica $y = y'$. In conclusione, f è una funzione iniettiva. Per quel che riguarda la suriettività, dato $(x, y) \in \mathbb{Z}^2$, cerchiamo, se esiste, $(a, b) \in \mathbb{Z}^2$ tale che $f(a, b) = (x, y)$. Risolvendo $(a - 2 = x) \wedge (2a - b = y)$, otteniamo che $a = x + 2$ e $b = 2(x + 2) - y$, da cui $(x, y) = f(x + 2, 2x + 4 - y)$ e quindi f è suriettiva.

In particolare, la funzione $g(x, y) = (x + 2, 2x + 4 - y)$ è l'inversa di f . Infatti $gf(x, y) = g(x - 2, 2x - y) = ((x - 2) + 2, 2(x - 2) + 4 - (2x - y)) = (x, y)$. Inoltre, abbiamo già visto che $fg(x, y) = f(x + 2, 2x + 4 - y) = (x, y)$ e quindi $g = f^{-1}$. \diamond

ESERCIZIO 1.25. Sia f una funzione di A in B e sia $C \subseteq B$ tale che per ogni $c \in C$ esiste almeno un $x \in A$ con $c = f(x)$. Che relazione c'è fra $|C|$ e $|A|$? \diamond

ESERCIZIO 1.26. Si consideri l'applicazione $f : \mathbb{N} \mapsto \mathbb{N}$ definita da $f(n) = n + 1$. Si dica se f è iniettiva e se è suriettiva. Si risponda alla stessa domanda per l'applicazione $g : \mathbb{N} \mapsto \mathbb{N}$ definita da $g(0) = 0$ e, per $n > 0$, $g(n) = n - 1$. Si supponga poi di sostituire \mathbb{Z} a \mathbb{N} e si risponda nuovamente. \diamond

ESERCIZIO 1.27. Si dimostri che per nessun insieme S , l'applicazione $f : S \mapsto \mathcal{P}(S)$ definita da $f(x) = \{x\}$ per ogni $x \in S$ può essere suriettiva. Cosa succede cambiando il codominio in $\mathcal{P}(S) - \{\emptyset\}$? \diamond

ESERCIZIO 1.28. Si definisca una funzione $f : \mathbb{Z} \mapsto \mathbb{Z}$ suriettiva ma non biiettiva. \diamond

ESERCIZIO 1.29. Si calcolino le funzioni composte gf e fg per ciascuna delle seguenti coppie di funzioni da \mathbb{R} in \mathbb{R} :

1. $f(x) = 3x + 2 \quad g(x) = 4x + 3$
2. $f(x) = x + c \quad g(x) = x - c$
3. $f(x) = x^2 + 1 \quad g(x) = \frac{1}{x^2 + 1}$
4. $f(x) = 1 - 3x \quad g(x) = x - 2$.

\diamond

ESERCIZIO 1.30. Si definiscano due applicazioni f e g , tali che nessuna delle due sia costante, esista gf e gf sia una funzione costante. \diamond

ESERCIZIO 1.31. Si dimostri che, date due applicazioni lineari di \mathbb{R} in \mathbb{R} , $f(x) = ax + b$ e $g(x) = cx + d$, la loro composta gf è una funzione costante se e solo se è costante almeno una di esse. \diamond

ESERCIZIO 1.32. Sia f l'applicazione di dominio $E = \mathbb{N} - \{0, 1\}$ che ad ogni numero associa il suo massimo fattore primo. Si determinino gli insiemi $f(E)$, $f^{-1}(2)$, $f^{-1}(3)$, $f^{-1}(4)$. \diamond

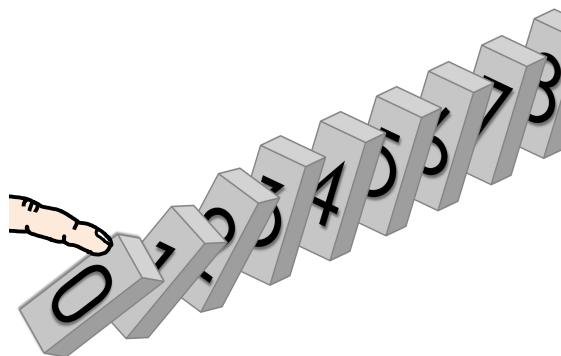


Figure 1.1: Il principio di induzione. $P(n)$ = l' n -mo tassello del domino cade.

ESERCIZIO 1.33. Siano E ed E' due insiemi di cardinalità 3. Si dica (i) quante applicazioni esistono di E in E' ; (ii) quante sono costanti; (iii) quante iniettive; (iv) quante suriettive. \diamond

ESERCIZIO 1.34. Sia $f : A \mapsto B$, siano $A', A'' \subseteq A$ e $B', B'' \subseteq B$. Dimostrare che

1. $A' \subseteq A''$ implica $f(A') \subseteq f(A'')$
2. $B' \subseteq B''$ implica $f^{-1}(B') \subseteq f^{-1}(B'')$
3. $f^{-1}(B') \subseteq f^{-1}(B'')$ implica $B' \cap f(A) \subseteq B'' \cap f(A)$
4. $f(A' \cap A'') \subseteq f(A') \cap f(A'')$
5. $f(A') \cap f(A'') = \emptyset$ implica $A' \cap A'' = \emptyset$. (si noti che, invece, $A' \cap A'' = \emptyset$ non implica, in generale, che sia vuoto l'insieme $f(A') \cap f(A'')$)
6. $f^{-1}(\bar{B}') = \bar{f^{-1}(B')}$

\diamond

1.6 Il principio di induzione

Supponiamo di avere un numero enorme di tasselli del domino (enorme è dire poco: supponiamo di averne infiniti) e di voler disporli in modo da poi riuscire a farli cadere tutti. Perchè tutti cadano, basterà garantire due proprietà:

- (a) Il primo tassello cade (cosa che possiamo forzare “esplicitamente”, spingendolo con il dito).
- (b) I tasselli sono posizionati in modo che la caduta di ogni tassello provochi la caduta del tassello successivo.

Queste due proprietà sono alla base del cosiddetto *principio di induzione*, grazie al quale è possibile dimostrare che una certa proprietà P vale per tutti i numeri naturali dimostrando che

- (i) P è vera per il numero 0
- (ii) Per ogni $k \geq 1$, se P è vera per il numero $k - 1$, allora è vera anche per il numero k .

Se evidenziamo la dipendenza di P dal numero n scrivendo $P(n)$, il principio di induzione afferma che $P(n) = \text{VERO}$ per ogni n se

- (i) $P(0) = \text{VERO}$
- (ii) $(P(k - 1) = \text{VERO}) \implies (P(k) = \text{VERO})$ per ogni $k \geq 1$.

Il caso $P(0)$ si dice *caso base* dell'induzione, mentre il passaggio da $k - 1$ a k è detto *passo induttivo*. Per convincersi che il principio di induzione implica che effettivamente $P(n)$ vale per ogni $n \in \mathbb{N}$ possiamo utilizzare un ragionamento per assurdo. Supponiamo infatti che valgano (i) e (ii), ma che lo stesso esistano dei numeri naturali per cui P non vale. Sia allora \hat{n} il minimo numero per il quale $P(n)$ è falso. Siccome vale (i), deve essere $\hat{n} > 0$. Inoltre, deve anche essere $P(\hat{n} - 1) = \text{FALSO}$ o, per (ii), si avrebbe $P(\hat{n}) = \text{VERO}$. Ma allora \hat{n} non era il *minimo* naturale per cui P non vale: assurdo.

Si noti che, se in (i) al posto del caso base $n = 0$ si considerasse il caso $n = n_0$, per $n_0 \in \mathbb{N}$, il principio di induzione porterebbe a concludere che la proprietà P vale per tutti gli $n \geq n_0$.

Esempio. Come esempio, dimostriamo che la somma dei primi n numeri dispari vale n^2 . Indichiamo tale somma con $S(n)$. Si noti che l' n -esimo numero dispari (per $n = 1, 2, \dots$) è $2n - 1$. Caso base:

$$S(0) = 0 = 0^2$$

Passo induttivo: Sia $k > 0$ e $S(k - 1) = (k - 1)^2$. Allora

$$S(k) = S(k - 1) + 2k - 1 = k^2 - 2k + 1 + 2k - 1 = k^2.$$

◇

Esempio. Dimostriamo che la somma dei primi n numeri naturali positivi è $\frac{n(n+1)}{2}$. Indichiamo tale somma con $S(n)$. Caso base:

$$S(0) = 0 = \frac{0 \cdot 1}{2}$$

Passo induttivo: Sia $k > 0$ e $S(k - 1) = \frac{(k-1)k}{2}$. Allora

$$\begin{aligned} S(k) &= S(k - 1) + k = \frac{(k - 1)k}{2} + 2\frac{k}{2} = \\ &= \frac{k}{2}(k - 1 + 2) = \frac{k(k + 1)}{2} \end{aligned}$$

◇

Esempio. Dimostriamo che $2^0 + 2^1 + \dots + 2^n = 2^{n+1} - 1$. Indichiamo la somma delle potenze di 2 fino a 2^n compreso con $S(n)$. Caso base:

$$S(0) = 2^0 = 1 = 2^1 - 1.$$

Passo induttivo: Sia $k > 0$ e $S(k-1) = 2^k - 1$. Allora

$$S(k) = S(k-1) + 2^k = 2^k - 1 + 2^k = 2^{k+1} - 1.$$

◇

Esempio. Dimostriamo che $3^{2n} - 1$ è un multiplo di 8 per ogni $n \geq 1$. Si noti che l'asserto può essere riformulato come: "Per ogni $n \geq 1$ si ha $3^{2n} \equiv_8 1$ ".

Caso base: per $n = 1$ si ha $3^{2 \times 1} = 9 \equiv_8 1$.

Passo induttivo: Sia $k \geq 2$ e sia vero l'asserto per $k-1$. In particolare, si ha

$$3^{2k} = 3^2 \times 3^{2(k-1)} \equiv_8 9 \times 1 \equiv_8 1$$

e quindi l'asserto vale per k .

◇

Esempio. Dimostriamo per induzione che per ogni naturale $n \geq 1$ si ha

$$\sum_{k=1}^n \frac{k}{2^k} = \frac{2^{n+1} - n - 2}{2^n}$$

Caso base: per $n = 1$ abbiamo

$$\frac{1}{2^1} = \frac{2^2 - 1 - 2}{2^1} = \frac{1}{2}$$

Passo induttivo: Sia $n > 1$ e supponiamo vero che $\sum_{k=1}^{n-1} (k/2^k) = (2^n - (n-1) - 2)/2^{n-1}$. Abbiamo

$$\begin{aligned} \sum_{k=1}^n \frac{k}{2^k} &= \sum_{k=1}^{n-1} \frac{k}{2^k} + \frac{n}{2^n} \\ &= \frac{2^n - (n-1) - 2}{2^{n-1}} + \frac{n}{2^n} \\ &= \frac{2(2^n - n - 1) + n}{2^n} \\ &= \frac{2^{n+1} - n - 2}{2^n} \end{aligned}$$

◇

Esempio. (La torre di Hanoi.) In base a un'antica leggenda, esiste un tempio indù in cui si trova una torre composta di 64 dischi d'oro, ciascuno di grandezza diversa, bucati al centro ed impernati su un piolo di diamante. La torre è disposta in modo che il disco più grande giaccia sul fondo e i dischi sopra ad esso siano via via di misura decrescente, fino al più piccolo che si trova in cima. Nel tempio si trovano anche due altri pioli di diamante, e alcuni monaci buddisti hanno il compito di spostare l'intera piramide su uno di tali pioli, muovendo un disco alla volta e facendo uso del terzo piolo per le mosse intermedie. Nello spostare i dischi va rispettata la seguente regola: *non si può mai porre un disco su uno di misura inferiore*. La leggenda vuole che quando i monaci avranno spostato l'intera piramide, il mondo finirà.

Il principio d'induzione ci permette di calcolare il numero di mosse che l'intera operazione richiede, e di tirare un sospiro di sollievo per quel che riguarda la sorte del mondo per i prossimi secoli dei secoli. Indichiamo infatti con $H(n)$ il minimo numero di mosse necessarie (e sufficienti) per spostare una piramide di n dischi da un piolo ad un altro, e dimostriamo che $H(n) = 2^n - 1$.

Per $n = 1$ è ovviamente $H(1) = 1 = 2^1 - 1$. Supponiamo ora che sia $n > 1$ e che valga $H(n-1) = 2^{n-1} - 1$. Dovendo spostare la torre di n dischi da un piolo P a un piolo P' , e detto P'' il terzo piolo, dobbiamo necessariamente procedere come segue:

1. Spostare $n - 1$ dischi da P a P'' facendo uso di P' come piolo intermedio. Al termine di questa fase, il disco più grande si è liberato e può essere portato su P' .
2. Muovere il disco di diametro massimo dal piolo P al piolo P' .
3. Spostare gli $n - 1$ dischi che si trovano sul piolo P'' al piolo P' , facendo uso di P come piolo intermedio.

La fase 1. e la fase 3. richiedono, per induzione, $H(n-1)$ mosse. La fase 2. ne richiede una, per cui otteniamo

$$H(n) = 2H(n-1) + 1 = 2(2^{n-1} - 1) + 1 = 2^n - 1$$

e il risultato è provato. Anche assumendo che i monaci lavorino al ritmo di spostamento di 1000 dischi al secondo, sarebbero necessari circa 585 milioni di anni perchè portino a termine il loro compito! ◇

ESERCIZIO 1.35. Si dimostri per induzione che la somma dei primi n cubi è uguale al quadrato della somma dei primi n naturali, i.e.,

$$1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2.$$

◇

ESERCIZIO 1.36. Dimostrare per induzione che

$$1 \times 2 + 2 \times 3 + 3 \times 4 + \cdots + n \times (n+1) = \frac{n(n+1)(n+2)}{3}.$$

◇

ESERCIZIO 1.37. Si dimostrino, per induzione, le seguenti uguaglianze:

1.

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}.$$

2.

$$\frac{1}{2} + \frac{2}{2^2} + \frac{3}{2^3} + \cdots + \frac{n}{2^n} = 2 - \frac{n+2}{2^n}.$$

3.

$$1 + 2q + 3q^2 + \cdots + nq^{n-1} = \frac{1 - (n+1)q^n + nq^{n+1}}{(1-q)^2}.$$

◇

ESERCIZIO 1.38. Sia $a \in \mathbb{R}$. Dimostrare per induzione che per ogni $n \in \mathbb{N}$ si ha $(1+a)^n \geq 1+an$.

◇

ESERCIZIO 1.39. Dimostrare per induzione che $15^n + 6$ è un multiplo di 7 per ogni naturale $n \geq 1$.

◇

Sebbene il passo induttivo sia di solito presentato come il modo di dimostrare $P(k)$ a partire da $P(k-1)$, sarebbe perfettamente analogo (e porterebbe ancora a concludere che $P(n)$ è vera per ogni n) un passo induttivo che dimostrasse che $P(k)$ consegue da $P(q)$ per un qualsiasi $q < k$ (non necessariamente $q = k-1$). Infatti, in tale modo si potrebbe dimostrare $P(1)$ da $P(0)$, dopodichè seguirebbe $P(2)$ da $P(0)$ o $P(1)$, e a quel punto seguirebbe $P(3)$ da $P(0)$ o $P(1)$ o $P(2)$, e così via...

I seguenti esempi mostrano come l'induzione possa essere usata in maniera errata e portare a “dimostrare” proposizioni false. Si trovino gli errori negli esempi seguenti.

Esempio. Sia x un qualsiasi numero. “Dimostreremo” che, per ogni insieme finito A tale che $x \in A$, allora $\max A = x$.

La dimostrazione è per induzione sulla cardinalità di A . Sia $n = |A|$. Se $n = 1$ l'asserto è chiaramente vero, in quanto in quel caso $A = \{x\}$. Supponiamo ora vero l'asserto per $|A| = 1, 2, \dots, n-1$ e sia $|A| = n > 1$. Sia $v = \min A$. Non può essere $v = x$, perchè rimuovendo un qualsiasi elemento diverso da x da A , x è, per induzione, il massimo tra gli elementi restanti e quindi ci sono elementi minori di x . Sia ora $A' = A - \{v\}$. Per induzione, $x = \max A'$. Ma allora, $x = \max A$, perchè v (l'unico elemento mancante tra A e A') non può essere il massimo di A .

◇

Di tenore simile al precedente, è l'esempio seguente:

Esempio. Si consideri la dimostrazione per induzione della proposizione $P(n)$: n linee, a due a due non parallele, si incontrano tutte in uno stesso punto.

$P(2)$ è chiaramente vera. Supponiamo ora di avere k linee e che $P(k-1)$ sia vero. Siano a, b, c, d, \dots le linee. Tolta la linea c , le rimanenti si incontrano (per induzione) in un punto, sia esso X . In particolare a e b passano per X . Ora, rimettiamo c e togliamo d . Sempre per induzione, le $k-1$ linee (comprese a, b e c) si incontrano in un punto, che deve essere X (questo siccome sappiamo già che a e b si incontrano in X). Si conclude che c passa per X , e quindi tutte le linee passano per X .

◇

Esempio. Si consideri la dimostrazione per induzione della proposizione $P(n)$: per ogni $n \geq 0$, si ha $n = 2n$.

$P(0)$ è vero siccome $0 = 2 \cdot 0$. Dato $k > 0$, si supponga vero $P(q)$ per $0 \leq q < k$. Scelto un $0 < q < k$, si spezzi k in $(k - q) + q$. Per ipotesi di induzione, $k - q = 2(k - q)$ e $q = 2q$. Ne consegue $k = (k - q) + q = 2(k - q) + 2q = 2k$. \diamond

ESERCIZIO 1.40. Si consideri l'affermazione: "Ogni sottoinsieme finito non vuoto di \mathbb{R} ha un minimo". La si dimostri: (a) per assurdo; (b) per induzione. \diamond

1.6.1 Induzione multipla

Consideriamo una proposizione $P(n_1, n_2, \dots, n_k)$ la cui verità dipende da k variabili in \mathbb{N} . Dovendo dimostrare la validità di tale proposizione per ogni possibile valore delle k variabili, vorremmo utilizzare il principio di induzione. Per analogia col caso $k = 1$, ci aspetteremmo di dover dimostrare che (i) vale $P(0, \dots, 0)$ e (ii) se $P()$ vale per una certa k -pla vale anche per la k -pla successiva. Questo tipo di approccio non può però funzionare, in quanto in \mathbb{N}^k non è definito il concetto di successore di una k -pla. Un modo per utilizzare l'induzione anche per questo tipo di dimostrazioni può allora essere il seguente: Si consideri una funzione $f : \mathbb{N}^k \mapsto \mathbb{N}$ e la proposizione $Q(n)$, di un'unica variabile in \mathbb{N} , definita da

$Q(n)$ è vero se, per ogni k -pla $(n_1, \dots, n_k) \in \mathbb{N}^k$ tale che $f(n_1, \dots, n_k) = n$, vale $P(n_1, \dots, n_k)$.

Abbiamo allora che $Q(n)$ vale per ogni $n \in \mathbb{N}$ se e solo se $P(n_1, n_2, \dots, n_k)$ vale per ogni $n_1, \dots, n_k \in \mathbb{N}$. Infatti, supponiamo che $Q(n)$ valga per ogni n e siano $\hat{n}_1, \dots, \hat{n}_k \in \mathbb{N}$. Allora, detto $\hat{n} = f(\hat{n}_1, \dots, \hat{n}_k)$, siccome vale $Q(\hat{n})$, vale anche $P(\hat{n}_1, \dots, \hat{n}_k)$. Viceversa, supponiamo P valga per ogni k -pla di naturali. In particolare, preso $n \in \mathbb{N}$, P vale per ogni (n_1, \dots, n_k) tale che $f(n_1, \dots, n_k) = n$, e quindi $Q(n)$ è vera.

Se utilizziamo una certa funzione f per la dimostrazione, diciamo che la dimostrazione procede per *induzione sul valore di f* . Alcuni esempi di funzioni più comunemente utilizzate nelle dimostrazioni per induzione multipla sono:

- $f(n_1, \dots, n_k) = \min\{n_1, \dots, n_k\}$
- $f(n_1, \dots, n_k) = \max\{n_1, \dots, n_k\}$
- $f(n_1, \dots, n_k) = n_1 + \dots + n_k$.

Non sono molti gli esempi di problemi risolvibili con l'induzione multipla, e difficilmente si tratta di induzione su più di due (induzione doppia) o tre (induzione tripla) variabili. A titolo puramente didattico, consideriamo il seguente problema (che potrebbe essere risolto anche senza fare ricorso all'induzione). Avendo una tavoletta di cioccolata, contenente m righe di n quadratini ciascuna, vogliamo separare i singoli quadratini spezzando ripetutamente la cioccolata lungo le linee che separano le righe o le colonne. In particolare, ad un'iterazione generica, la cioccolata è stata ridotta a un certo numero di "sotto-tavolette" rettangolari (dove con "rettangolari" comprendiamo anche il caso siano quadrate). A questo punto, prendiamo una delle sottotavolette che contengono più di un quadratino e la spezziamo in due. Il processo prosegue fino a che le sottotavolette coincidono con gli $m \times n$ quadratini della cioccolata originale. Vogliamo dimostrare che:

Per ogni coppia di naturali positivi m, n , per estrarre i singoli quadratini da una tavoletta di cioccolata rettangolare di dimensioni $m \times n$, sono necessarie $mn - 1$ iterazioni.

In questo caso l'esempio si presta facilmente ad un'induzione su mn . Si noti che in questo esempio sia m che n sono strettamente positivi, e quindi il caso base si ha per $mn = 1$. In questo caso, la cioccolata consiste di un unico quadratino e quindi sono necessari $0 = mn - 1$ tagli per separare i quadratini. Veniamo ora al passo induttivo. Supponiamo che l'asserto valga per tutte le coppie m, n tali che $1 \leq mn < p$ e consideriamo una tavoletta T di dimensioni $mn = p$. Il primo taglio su questa tavoletta, avverrà lungo una delle righe (spezzando T in due tavolette T_1 e T_2 di dimensioni $k \times n$ e $(m - k) \times n$) o lungo una delle colonne (spezzandola in due tavolette T'_1 e T'_2 di dimensioni $m \times k$ e $m \times (n - k)$). Consideriamo il primo dei due casi (l'altro caso si dimostra in modo perfettamente analogo). La tavoletta T_1 , per induzione, richiede $kn - 1$ iterazioni per essere ridotta ai singoli quadratini. Sempre per induzione, la tavoletta T_2 ne richiede $(m - k)n - 1$. Aggiungendo il taglio effettuato per separare T_1 da T_2 abbiamo che i tagli richiesti per ottenere i singoli quadratini di T sono

$$1 + kn - 1 + (m - k)n - 1 = mn - 1$$

e l'asserto risulta provato per T .

ESERCIZIO 1.41. Si dimostri nuovamente la proposizione riguardante la tavoletta di cioccolata, questa volta utilizzando (a scelta) l'induzione su $\min\{n, m\}$ o su $n + m$. \diamond

1.7 Somme e loro manipolazioni

La *sommatoria* (o, più semplicemente, *somma*) è un'espressione del tipo

$$\sum_{k=1}^n a_k$$

dove k è detto l'*indice* e a_k il *termine generico*. Il valore di tale somma è

$$a_1 + a_2 + a_3 + \cdots + a_{n-1} + a_n.$$

Questo secondo tipo di scrittura lascia un po' troppa libertà nello scegliere quanti elementi espliciti mettere a sinistra e a destra dei "...". Ad esempio, supponiamo di limitarci a scrivere i primi due termini e l'ultimo, lasciando gli altri in forma implicita (nel senso che dovrebbe essere chiara la loro definizione guardando ai tre termini esplicitamente elencati). La somma risulta quindi $a_1 + a_2 + \cdots + a_n$, ma è facile dare degli esempi in cui i termini impliciti non sono affatto facili da dedurre. Se, ad esempio, $a_i = 2^{i-1}$ si avrebbe la scrittura $1 + 2 + \cdots + 2^{n-1}$ che può essere confusa con $\sum_{i=1}^{2^{n-1}} i$. Sarebbe quindi stato meglio scriverla come $2^0 + 2^1 + \cdots + 2^{n-1}$. Con l'espressione \sum questo problema non si pone.

Gli indici di una somma sono numeri interi. La variabilità di un indice non deve necessariamente essere tra un limite inferiore e uno superiore, ma l'indice può essere preso su un qualsiasi insieme K di interi. In questo caso la scrittura migliore è quella che spiega la variabilità dell'indice sotto al simbolo di somma \sum :

$$\sum_{k \in K} a_k$$

Alcuni esempi:

$$\sum_{0 \leq k \leq n} a_k, \quad \sum_{k \text{ primo}, k < 20} a_k, \quad \sum_{1 \leq k \leq 100, k \text{ dispari}} a_k$$

Ad esempio, la somma dei quadrati dei numeri dispari tra 1 e 100 è preferibile scritta come

$$\sum_{\substack{1 \leq k \leq 100 \\ k \text{ dispari}}} k^2$$

che come

$$\sum_{k=1}^{50} (2k-1)^2$$

per quanto sia la stessa somma. Allo stesso modo “risparmiare” termini non serve e può rendere più difficile capire una somma. Ad esempio scrivere

$$\sum_{k=2}^{n-1} k(k-1)(n-k)$$

è peggio che scrivere

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

per quanto il valore sia lo stesso. Anche la somma sull'insieme vuoto è definita, e vale sempre 0:

$$\sum_{k \in \emptyset} a_k = 0.$$

Le seguenti regole permettono di manipolare le somme, per crearne di nuove, per aggregazione o disgregazione:

1. **Legge distributiva:** Da una somma si possono “portare fuori” le costanti, ossia le espressioni che non dipendono dall'indice:

$$\sum_{k \in K} c a_k = c \sum_{k \in K} a_k$$

2. **Legge associativa:** permette di spezzare una somma in due o di riunire due somme in una:

$$\sum_{k \in K} (a_k + b_k) = \sum_{k \in K} a_k + \sum_{k \in K} b_k$$

3. **Legge commutativa:** L'ordine con cui si sommano i termini può essere cambiato e la somma resta la stessa. Sia p una permutazione definita su tutti i numeri interi (ossia una funzione biettiva p di \mathbb{Z} in \mathbb{Z}). Allora

$$\sum_{k \in K} a_k = \sum_{p(k) \in K} a_{p(k)}$$

Un caso interessante (detto anche *cambio di indice*) è dato dalla *traslazione*, ossia una funzione che a ogni intero somma una certa costante: Se $c \in \mathbb{Z}$ è una costante, la funzione

$$p(i) = i + c$$

è una permutazione degli interi (per esercizio, lo si dimostri). Per cui

$$\sum_{k \in K} a_k = \sum_{(k+c) \in K} a_{k+c}.$$

Ad esempio, calcoliamo

$$S = \sum_{0 \leq k \leq n} (a + bk) \tag{1.15}$$

sfruttando solo le tre leggi elencate. Appliciamo la legge commutativa e rimpiazziamo k con $n-k$, ottenendo

$$S = \sum_{0 \leq n-k \leq n} (a + b(n-k)) = \sum_{0 \leq k \leq n} (a + bn - bk). \tag{1.16}$$

Dalla legge associativa sommiamo (1.15) e (1.16) e otteniamo

$$2S = \sum_{0 \leq k \leq n} ((a + bk) + (a + bn - bk)) = \sum_{0 \leq k \leq n} (2a + bn).$$

Per la legge distributiva (si noti che $(2a + bn)$ non dipende da k) si ha

$$2S = (2a + bn) \sum_{0 \leq k \leq n} 1 = (2a + bn)(n+1)$$

da cui, dividendo per 2

$$S = (a + \frac{1}{2}bn)(n+1).$$

Una formula generale che permette di fondere e spezzare le somme è la seguente:

$$\sum_{k \in K} a_k + \sum_{k \in K'} a_k = \sum_{k \in K \cap K'} a_k + \sum_{k \in K \cup K'} a_k. \tag{1.17}$$

Esempio.

- **fondere le somme:** sia $1 \leq m \leq n$. Allora

$$\sum_{k=1}^m a_k + \sum_{k=m}^n a_k = a_m + \sum_{k=1}^n a_k$$

- **spezzare le somme:** sia $1 \leq m \leq n$. Allora

$$\sum_{k=1}^n a_k = \sum_{k=1}^m a_k + \sum_{k=m+1}^n a_k$$

◇

1.7.1 Somme multiple

Qualora il termine generico di una somma sia a sua volta una somma, si parla di somma multipla. Il concetto può essere esteso a tre o più somme. Nel caso delle somme multiple, ogni somma avrà un indice diverso che ne definisce la variabilità. I vari indici possono poi risultare indipendenti l'uno dall'altro, come ad esempio nel caso

$$\sum_{1 \leq i \leq 5} \left(\sum_{0 \leq j \leq 4} \left(\sum_{0 \leq k \leq 3} (2^i + 3j/(i+k)) \right) \right)$$

o dipendenti fra loro, come ad esempio

$$\sum_{1 \leq i \leq 5} \left(\sum_{0 \leq j \leq 4, \text{ con } j \neq i} \left(\sum_{0 \leq k \leq j} (i+j-k) \right) \right).$$

In una somma multipla, le parentesi intorno alle somme interne si possono omettere, e la generica somma multipla (ad esempio, una somma tripla) risulta:

$$\sum_{i \in I} \sum_{j \in J} \sum_{k \in K} a(i, j, k)$$

dove $a(i, j, k)$ è il generico addendo, in cui si è evidenziata la dipendenza dai vari indici.

Consideriamo come esempio il prodotto delle componenti di due vettori. Un *vettore* di *dimensione* n è una sequenza di n numeri, detti le *componenti* del vettore. Ad esempio, i seguenti a , b e c sono vettori di dimensione 4:

$$a = (3, 2, 5, -1) \quad b = (6, \pi, -3, 0) \quad c = (0, 0, 0, 0).$$

Se a è un vettore, le sue componenti si indicano tramite indici, come in

$$a = (a_1, a_2, \dots, a_n).$$

Supponiamo, dati due vettori a e b di voler calcolare la somma dei prodotti fra ogni componente di a e di b . Per $n = 3$, scriviamo la somma cercata in un modo organizzato, mettendo tutti gli addendi in una tabella:

$$\begin{array}{ccccccc} a_1 b_1 & + & a_1 b_2 & + & a_1 b_3 & + & \\ a_2 b_1 & + & a_2 b_2 & + & a_2 b_3 & + & \\ a_3 b_1 & + & a_3 b_2 & + & a_3 b_3 & & \end{array} \quad (1.18)$$

Si dice anche che gli addendi sono stati messi in una *matrice* 3 per 3, ossia con 3 *righe* e 3 *colonne* (in generale, una matrice $m \times n$ ha mn numeri disposti su m righe e n colonne). La somma può essere calcolata facendo le somme di ogni riga e poi sommando tali valori. Si noti che la riga i ha termini in cui a_i è costante e varia solo b_j . Scriviamo

$$\sum_{1 \leq i \leq 3} \sum_{1 \leq j \leq 3} a_i b_j$$

Si sarebbe però potuto anche calcolare tale somma “per colonne”, ossia sommando il valore su ogni colonna (in cui b_j è costante) e facendo infine la somma dei totali. Questa somma si sarebbe dovuta scrivere

$$\sum_{1 \leq j \leq 3} \sum_{1 \leq i \leq 3} a_i b_j$$

C'è stato quindi uno scambio di indici. Vediamo ora formalmente perchè questo è giustificato:

$$\sum_{1 \leq i \leq 3} \sum_{1 \leq j \leq 3} a_i b_j = \sum_{1 \leq i \leq 3} (a_i \sum_{1 \leq j \leq 3} b_j) = \left(\sum_{1 \leq j \leq 3} b_j \right) \left(\sum_{1 \leq i \leq 3} a_i \right) \quad (1.19)$$

dove il primo passaggio è giustificato dal fatto che nell'espressione $\sum_{j=1}^3 a_i b_j$ il valore a_i è una costante (non dipende da j) e può quindi (legge distributiva) essere portato fuori dalla somma. Allo stesso modo, il secondo passaggio segue dal fatto che l'intera somma $\sum_{j=1}^3 b_j$ è una costante nell'espressione $\sum_{i=1}^3 (a_i \sum_{j=1}^3 b_j)$.

In modo perfettamente analogo, si può dimostrare che anche

$$\sum_{1 \leq j \leq 3} \sum_{1 \leq i \leq 3} a_i b_j = \left(\sum_{1 \leq i \leq 3} a_i \right) \left(\sum_{1 \leq j \leq 3} b_j \right). \quad (1.20)$$

In particolare, le formule (1.19) e (1.20) ci danno anche un modo immediato per calcolare il valore finale. Basta sommare tutte le componenti di a e moltiplicare il valore ottenuto con la somma di tutte le componenti di b .

Scambio di indici. La regola di scambio degli indici in una somma può essere riassunta così: quando in una somma doppia il primo indice i varia su un insieme I e il secondo indice j varia su un insieme J , in maniera *indipendente* dal valore di i (ossia, J è sempre lo stesso, per ogni valore di i), allora gli indici possono essere scambiati:

$$\sum_{i \in I} \sum_{j \in J} s_{ij} = \sum_{j \in J} \sum_{i \in I} s_{ij} \quad (1.21)$$

dove con s_{ij} abbiamo indicato il generico termine della somma (nell'esempio precedente, era $s_{ij} = a_i b_j$)

Se però la variabilità del secondo indice *dipende* dal valore del primo indice, allora bisogna fare attenzione. Si consideri il seguente esempio:

$$\sum_{i=0}^n \sum_{j=i}^n s_{ij}. \quad (1.22)$$

Questa somma *non* si può riscrivere come

$$\sum_{j=i}^n \sum_{i=0}^n s_{ij} \quad (1.23)$$

in quanto, leggendo da sinistra a destra, la variabilità del primo indice (j) non è definita chiaramente. Infatti si suppone che j parta da i , ma i è un simbolo “indefinito” (o, come si dice, *non quantificato*) la prima volta che lo si incontra.

La situazione di indici dipendenti si può descrivere in questo modo: il primo indice, i , varia su un insieme I , mentre il secondo j , varia su un insieme $J(i)$ che dipende, di volta in volta, dal valore corrente di i . In

questo caso, per poter scambiare gli indici, dobbiamo vedere, per ogni valore del secondo indice, j , quali sono i valori di i per i quali j apparteneva a $J(i)$. Sia J l'unione di tutti i $J(i)$ per $i \in I$ (ossia J è l'insieme di tutti i possibili valori del secondo indice). Definiamo, per ogni $j \in J$,

$$I(j) := \{i \in I \mid j \in J(i)\}.$$

Allora, possiamo effettuare lo scambio degli indici in questo modo:

$$\sum_{i \in I} \sum_{j \in J(i)} s_{ij} = \sum_{j \in J} \sum_{i \in I(j)} s_{ij}. \quad (1.24)$$

Nel caso dell'esempio (1.22) si ha $J = \{0, \dots, n\}$ e $I(j) = \{0, 1, \dots, j\}$ per ogni j . Pertanto, (1.22) può essere riscritta come

$$\sum_{j=0}^n \sum_{i=0}^j s_{ij}. \quad (1.25)$$

ESERCIZIO 1.42. Siano $a = (3, \frac{2}{3}, 5, \frac{1}{3}, -2, -6, 3, 9, -1)$ e $b = (-\frac{1}{3}, \frac{1}{4}, 2, 3, -1, \frac{1}{2}, \frac{1}{2})$. Si calcoli

$$\sum_{i=1}^9 \sum_{j=1}^7 \frac{a_i}{b_j}.$$

◇

1.8 Alcune somme importanti

1.8.1 Somma di numeri consecutivi

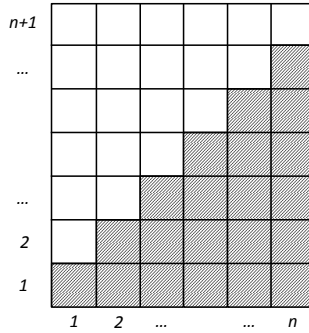
Approccio “geniale”

Il primo approccio è quello utilizzato da Gauss a 6 anni! Per sommare i primi 100 numeri, ha ragionato così. Il primo (1) più l'ultimo (100) danno 101. Il secondo (2) più il penultimo (99) danno ancora 101. E così via, $3 + 98 = 101, \dots, 50 + 51 = 101$. In totale si hanno 50 coppie di valore 101 e quindi $\sum_{i=1}^{100} i = 5050$.

Il ragionamento si può generalizzare così. Supponendo n pari, si hanno $n/2$ coppie di valore $n + 1$ e quindi

$$\sum_{i=1}^n i = \frac{n(n+1)}{2} \quad (1.26)$$

Se n è dispari, si può aggiungere 0 alla somma, come primo termine. In questo modo si ottengono $n + 1$ termini e $(n+1)/2$ coppie. Ogni coppia somma n ($0 + n, 1 + (n-1), \dots$), per cui la somma è ancora $n(n+1)/2$.

Figure 1.2: Area ombreggiata = $\sum_{i=1}^n i$.**Approccio “geometrico”**

Siano B la base e H l'altezza del rettangolo in Figura 1.2. Vogliamo calcolare l'area ombreggiata. Si ha

$$B = n \quad \text{e} \quad H = n + 1.$$

L'area totale è $H \cdot B = n(n + 1)$. L'area ombreggiata è pari a $\sum_{i=1}^n i$ ed è anche uguale all'area chiara. Siccome area chiara + area scura = area totale, si ha

$$2 \cdot \sum_{i=1}^n i = n(n + 1) \quad (1.27)$$

per cui

$$\sum_{i=1}^n i = \frac{n(n + 1)}{2}. \quad (1.28)$$

Approccio “analitico”

Si intuisce che la somma cresce “come” n^2 (ci sono n addendi dal valore fino a n). Per cui si ipotizza

$$C(n) = \sum_{i=1}^n i = an^2 + bn + c.$$

Si ottiene, per sostituzione:

$$C(0) = 0 \text{ per cui } c = 0$$

$$C(1) = a + b = 1$$

$$C(2) = 4a + 2b = 3$$

Si ricava un sistema di due equazioni in due incognite:

$$\begin{cases} a + b = 1 \\ 4a + 2b = 3 \end{cases}$$

Risolviamo il sistema. Rimpiazziamo la II con $(4I - II)$, ottenendo

$$\begin{cases} a + b = 1 \\ 2b = 1 \end{cases}$$

da cui, $b = 1/2$ e $a = 1/2$. Quindi

$$C(n) = \frac{1}{2}n^2 + \frac{1}{2}n$$

che, raggruppando n al numeratore, diventa

$$C(n) = \frac{n(n+1)}{2}.$$

1.8.2 Somma di quadrati consecutivi

Calcoliamo $\sum_{i=1}^n i^2$. Usiamo due approcci diversi.

Approccio “geometrico”

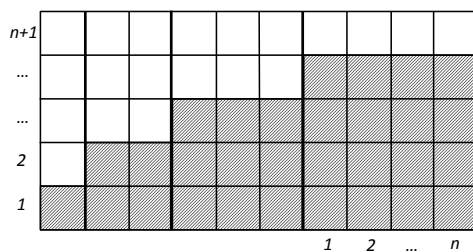


Figure 1.3: Area ombreggiata = $\sum_{i=1}^n i^2$.

Siano B la base e H l'altezza del rettangolo in Figura 1.3. Vogliamo calcolare l'area ombreggiata. Si ha

$$B = \sum_{i=1}^n i = \frac{n(n+1)}{2} \quad \text{e} \quad H = n+1.$$

L'area totale è $H \cdot B = \frac{n(n+1)^2}{2}$. L'area ombreggiata è pari a $\sum_{i=1}^n i^2$. L'area chiara è $\sum_{i=1}^n \sum_{j=1}^i j$. Si ha:

$$\sum_{i=1}^n \sum_{j=1}^i j = \sum_{i=1}^n \frac{i(i+1)}{2} = \frac{1}{2} \sum_{i=1}^n i^2 + \frac{1}{2} \sum_{i=1}^n i = \frac{1}{2} \sum_{i=1}^n i^2 + \frac{1}{2} \frac{n(n+1)}{2}. \quad (1.29)$$

Siccome area chiara + area scura = area totale, si ha

$$\frac{1}{2} \sum_{i=1}^n i^2 + \frac{n(n+1)}{4} + \sum_{i=1}^n i^2 = \frac{n(n+1)^2}{2} \quad (1.30)$$

$$\frac{3}{2} \sum_{i=1}^n i^2 = \frac{n(n+1)^2}{2} - \frac{n(n+1)}{4} = \frac{n(n+1)}{4} (2(n+1) - 1) \quad (1.31)$$

da cui

$$\sum_{i=1}^n i^2 = \frac{2}{3} \frac{n(n+1)(2n+1)}{4} = \frac{n(n+1)(2n+1)}{6}. \quad (1.32)$$

Approccio “analitico”

Si intuisce che la somma cresce “come” n^3 (ci sono n addendi dal valore fino a n^2). Per cui si ipotizza

$$C(n) = \sum_{i=1}^n i^2 = an^3 + bn^2 + cn + d.$$

Si ottiene, per sostituzione:

$$C(0) = 0 \text{ per cui } d = 0$$

$$C(1) = a + b + c = 1$$

$$C(2) = 8a + 4b + 2c = 1 + 4 = 5$$

$$C(3) = 27a + 9b + 3c = 1 + 4 + 9 = 14.$$

Si ricava un sistema di tre equazioni in tre incognite:

$$\begin{cases} a & + & b & + & c & = & 1 \\ 8a & + & 4b & + & 2c & = & 5 \\ 27a & + & 9b & + & 3c & = & 14 \end{cases}$$

Risolviamo il sistema. Rimpiazziamo la *II* con $(8I - II)$ e la *III* con $(27I - III)$. Otteniamo

$$\begin{cases} a & + & b & + & c & = & 1 \\ & & 4b & + & 6c & = & 3 \\ & & 18b & + & 24c & = & 13 \end{cases}$$

Continuando, si rimpiazza la *III* con $(18II - 4III)$ ottenendo

$$\begin{cases} a + b + c = 1 \\ 4b + 6c = 3 \\ 12c = 2 \end{cases}$$

A questo punto si risolve e si ha $c = 1/6$, $b = 1/2$ e $a = 1/3$. Ossia

$$C(n) = \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n$$

che, fissando il denominatore a 6 e raggruppando n al numeratore, diventa

$$C(n) = \frac{n(n+1)(2n+1)}{6}.$$

Esempio. (Indicizzazione di coppie.) Dato un intero n positivo, consideriamo l'insieme P di tutte le coppie di interi (a, b) con $1 \leq a < b \leq n$. Gli elementi di C possono essere ordinati secondo l'*ordine lessicografico*, in base al quale una coppia (a, b) precede ogni coppia (a', b') in cui $(a < a') \vee (a = a' \wedge b < b')$. Ad esempio, se $n = 5$, l'insieme P ordinato risulta

$$P = \{(1, 2), (1, 3), (1, 4), (1, 5), (2, 3), (2, 4), (2, 5), (3, 4), (3, 5), (4, 5)\}.$$

Abbiamo che $(1, 4)$ è la terza coppia di P , $(3, 5)$ la nona, e così via. Chiamiamo *indice* di una coppia (a, b) la sua posizione all'interno dell'insieme P ordinato, sicché l'indice di $(1, 3)$ è 2, e quello di $(3, 5)$ è 9. Si noti che l'indice è completamente determinato dai valori a, b, n .

Costruiamo una funzione $f(a, b)$ che, per un fissato n , data una coppia (a, b) con $1 \leq a < b \leq n$, restituisce l'indice della coppia rispetto all'ordine lessicografico. Una tale funzione è utile, ad esempio, in applicazioni informatiche in cui si vogliano memorizzare su un vettore monodimensionale, anziché su una matrice bidimensionale, dei valori indicizzati da due indici (quali a e b).

Consideriamo la seguente tabella, relativa a $n = 5$, contenente gli indici di tutte le coppie:

	$b = 1$	$b = 2$	$b = 3$	$b = 4$	$b = 5$
$a = 1$		1	2	3	4
$a = 2$			5	6	7
$a = 3$				8	9
$a = 4$					10
$a = 5$					

Consideriamo l'indice in riga $a = 4$ e colonna $b = 5$. Vediamo che, per arrivare alla riga a , dobbiamo saltare $a - 1$ righe e che la generica riga i , con $1 \leq i \leq a - 1$ contiene $n - i$ indici. Quindi, ci sono in tutto $\sum_{i=1}^{a-1} (n - i)$ indici nelle righe $1, \dots, a - 1$ (nell'esempio, sette indici). Infine, nella riga a , ci sono $b - a$ indici da scandire prima di arrivare a quello giusto (nell'esempio, due indici). Quindi la funzione che cerchiamo è

$$\begin{aligned}
f(a, b) &= \sum_{i=1}^{a-1} (n-i) + b - a \\
&= (a-1)n - \sum_{i=1}^{a-1} i + b - a \\
&= (a-1)n - \frac{a(a-1)}{2} + b - a \\
&= (a-1)\frac{2n-a}{2} + b - a.
\end{aligned}$$

◇

ESERCIZIO 1.43. Quanto vale la somma

$$1 \times 2 + 2 \times 3 + 3 \times 4 + \dots + n \times (n+1)?$$

◇

ESERCIZIO 1.44. Quanti quadrati contiene una griglia di lato n (ossia definita da $n+1$ linee parallele, a distanza unitaria, intersecate da $n+1$ linee parallele verticali a distanza unitaria)? ◇

1.8.3 Somma di potenze consecutive

Calcoliamo $S(n) := \sum_{i=0}^n a^i$, dove $a > 1$. Abbiamo, per $n \geq 0$,

$$S(n+1) = a^{n+1} + S(n). \quad (1.33)$$

Inoltre, moltiplicando $S(n)$ per a si ottiene

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

ossia

$$aS(n) = S(n+1) - 1. \quad (1.34)$$

Da (1.33) e (1.34) si ricava un sistema che possiamo risolvere rispetto a $S(n)$. Sostituendo il valore di $S(n+1)$ dato dall'equazione (1.33) nell'equazione (1.34), si ottiene

$$aS(n) = a^{n+1} + S(n) - 1 \quad (1.35)$$

da cui

$$S(n) = \frac{a^{n+1} - 1}{a - 1}. \quad (1.36)$$

Esempio. Calcoliamo $\sum_{i=12}^{40} 7^i$. Abbiamo $\sum_{i=12}^{40} 7^i = \sum_{i=0}^{40} 7^i - \sum_{i=0}^{11} 7^i = (7^{41} - 1)/6 - (7^{12} - 1)/6 = 7^{12}(7^{29} - 1)/6$. \diamond

ESERCIZIO 1.45. Il DNA consiste di 4 diversi nucleotidi: $\{A, C, T, G\}$. Quante sono le possibili sequenze di DNA lunghe al più 10 nucleotidi?

ESERCIZIO 1.46. Quanto vale $\sum_{i=0}^n a^{3i}$? \diamond

1.8.4 Il metodo di perturbazione

Dagli esempi precedenti (specialmente l'ultimo) possiamo evincere un metodo generale per tentare di risolvere le somme del tipo $S_n = \sum_{k=0}^n a_k$. Il metodo si chiama “perturbazione” e consiste nel cercare di creare un'equazione che abbia S_n sia a destra che a sinistra, ma non con lo stesso coefficiente, in modo che non si cancellino a vicenda. Questa equazione viene creata passando a S_{n+1} e mettendo di volta in volta in evidenza a_{n+1} e a_0 .

S_{n+1} è la somma di S_n ed a_{n+1} , che possiamo anche scrivere come

$$S_n + a_{n+1} = \sum_{0 \leq k \leq n+1} a_k$$

Mettiamo ora in evidenza a_0 a destra. Inoltre, siccome (legge commutativa) $\sum_{1 \leq k \leq n+1} a_k$ è lo stesso che $\sum_{0 \leq k \leq n} a_{k+1}$, otteniamo la relazione fondamentale

$$S_n + a_{n+1} = a_0 + \sum_{0 \leq k \leq n} a_{k+1}$$

Il trucco ora sta nel cercare di sviluppare $\sum_{0 \leq k \leq n} a_{k+1}$ in modo ricavarne (se possibile) S_n . In tal modo avremmo S_n sia a sinistra che a destra, e potremo risolvere rispetto a S_n .

Esempio. Come esempio di questa tecnica calcoliamo il valore di

$$S_n = \sum_{0 \leq k \leq n} k 2^k$$

Abbiamo

$$S_n + (n+1)2^{n+1} = 0 + \sum_{0 \leq k \leq n} (k+1)2^{k+1}. \quad (1.37)$$

Studiamo $\sum_{0 \leq k \leq n} (k+1)2^{k+1}$ cercando di mettere in evidenza S_n . Spezziamo la somma in due con la legge associativa.

$$\sum_{0 \leq k \leq n} (k+1)2^{k+1} = \sum_{0 \leq k \leq n} k2^{k+1} + \sum_{0 \leq k \leq n} 2^{k+1} = 2 \sum_{0 \leq k \leq n} k2^k + 2 \sum_{0 \leq k \leq n} 2^k$$

e, ricordando che $\sum_{0 \leq k \leq n} 2^k = 2^{n+1} - 1$, si ha

$$\sum_{0 \leq k \leq n} (k+1)2^{k+1} = 2S_n + 2^{n+2} - 2.$$

Sostituendo questo valore in (1.37) si ottiene

$$S_n + (n+1)2^{n+1} = 2S_n + 2^{n+2} - 2$$

da cui

$$S_n = (n+1)2^{n+1} - 2^{n+2} + 2 = 2^{n+1}(n-1) + 2.$$

◇

Esempio. Calcoliamo il valore di

$$S_n = \sum_{0 \leq k \leq n} \frac{k}{2^k}$$

Abbiamo

$$S_n + \frac{n+1}{2^{n+1}} = 0 + \sum_{0 \leq k \leq n} \frac{k+1}{2^{k+1}}. \quad (1.38)$$

Studiamo $\sum_{0 \leq k \leq n} (k+1)/2^{k+1}$ cercando di mettere in evidenza S_n . Spezziamo la somma in due con la legge associativa.

$$\sum_{0 \leq k \leq n} \frac{k+1}{2^{k+1}} = \sum_{0 \leq k \leq n} \frac{k}{2^{k+1}} + \sum_{0 \leq k \leq n} \frac{1}{2^{k+1}} = \frac{1}{2} \sum_{0 \leq k \leq n} \frac{k}{2^k} + \frac{1}{2} \sum_{0 \leq k \leq n} \frac{1}{2^k}$$

e, ricordando che $\sum_{0 \leq k \leq n} 1/2^k = 2 - \frac{1}{2^n}$, si ha

$$\sum_{0 \leq k \leq n} \frac{k+1}{2^{k+1}} = \frac{1}{2} \left(S_n + \frac{2^{n+1} - 1}{2^n} \right).$$

Sostituendo questo valore in (1.38) si ottiene

$$S_n + \frac{n+1}{2^{n+1}} = \frac{1}{2} S_n + \frac{2^{n+1} - 1}{2^{n+1}}$$

da cui

$$S_n = 2 \left(\frac{2^{n+1} - 1}{2^{n+1}} - \frac{n+1}{2^{n+1}} \right) = 2 \left(\frac{2^{n+1} - 1 - n - 1}{2^{n+1}} \right) = \frac{2^{n+1} - n - 2}{2^n}.$$

◇

ESERCIZIO 1.47. Si usi il metodo di perturbazione per (ri)calcolare $\sum_{i=0}^n c^i$, con $c > 1$.

◇

1.9 Calcolo delle probabilità

Sia S un insieme finito**. Una *misura di probabilità* è una funzione \Pr , definita sui sottoinsiemi di S , che soddisfa:

$$\Pr(S) = 1 \quad (1.39)$$

$$0 \leq \Pr(A) \leq 1 \quad \forall A \subseteq S \quad (1.40)$$

$$\Pr(A \cup B) = \Pr(A) + \Pr(B) \quad \forall A, B \subseteq S \text{ tali che } A \cap B = \emptyset. \quad (1.41)$$

L'insieme S viene detto *universo* e rappresenta tutti i possibili *risultati* di un esperimento (tipo il lancio di un dado o l'estrazione di una pallina numerata da un'urna). I risultati sono anche detti *punti* dello *spazio di probabilità*. Ogni sottoinsieme di S è detto un *evento*, e, se ha cardinalità 1, è detto *evento elementare*.

La probabilità si dice *distribuita uniformemente* se $\Pr(\{a\}) = 1/|S|$ per ogni $a \in S$, ossia se tutti gli eventi elementari sono *equiprobabili*. Ad esempio, i risultati del lancio di un dado danno luogo all'universo $S = \{1, 2, 3, 4, 5, 6\}$ e ogni risultato è equiprobabile (con probabilità $1/6$).

Si noti che, detta $p = 1/|S|$, se la distribuzione è uniforme, ogni evento A ha probabilità $\Pr(A) = p|A| = \frac{|A|}{|S|}$ e quindi la probabilità dipende unicamente dalla cardinarietà di A e da quella di S . In questo caso, calcolare la probabilità di un evento (i.e., di un insieme) coincide con il contarne il numero di elementi (nonchè con il contare il numero di elementi di S , che risulta generalmente più facile), per cui andranno utilizzate le tecniche combinatoriche che verranno acquisite nei prossimi capitoli.

Esempio. Il tamburo di una roulette contiene i numeri dallo 0 al 36 inclusi. Se viene lanciata una pallina, qual'è la probabilità che la stessa termini la sua corsa su un numero pari? Su un multiplo di 5? Su un numero primo?

Nel gioco della roulette, l'uscita di ogni specifico numero ha la medesima probabilità, i.e., $1/37$. Siccome sul tamburo si trovano 19 numeri pari (i.e., $0, 2, 4, \dots, 36$), la probabilità di uscita di un pari è $19/37$. I multipli di 5 sono $\{0, 5, 10, 15, 20, 25, 30, 35\}$, per cui la probabilità che esca uno di essi è $8/37$. Infine, ci sono 11 numeri primi, i.e., $\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31\}$ e la probabilità degli stessi è $11/37$. ◇

**L'assunzione che S sia finito non è strettamente necessaria per la definizione di probabilità, ma noi la facciamo in quanto risulterà sempre valida in tutti gli esempi considerati in questo libro.

ESERCIZIO 1.48. Qual è la probabilità che nel gioco della briscola, l'asso di briscola venga pescato come ultima carta? \diamond

Alle volte la probabilità di un evento può essere condizionata dal verificarsi di un secondo evento. Ad esempio, la probabilità che in un lancio di dado sia uscito un numero maggiore di 3 è $1/2$. Se però sappiamo che il numero uscito è pari, la probabilità che sia maggiore di 3 diventa $2/3$.

Si definisce *probabilità condizionata di A dato il verificarsi di B* il numero

$$\Pr(A|B) = \frac{\Pr(A \cap B)}{\Pr(B)}. \quad (1.42)$$

In pratica, sapendo che B si è verificato, la probabilità che anche A si sia verificato è data dalla frazione di elementi di A che sono anche elementi di B , rispetto a tutti gli elementi di B (che diventa, implicitamente, il nuovo universo). Si noti che dalla definizione segue $\Pr(B|B) = 1$ e $\Pr(A|B) = 0$ se $A \cap B = \emptyset$, o, come si dice in questo caso, se A e B sono eventi *incompatibili*.

Si dice che due eventi A e B sono *indipendenti* se

$$\Pr(A \cap B) = \Pr(A) \Pr(B).$$

Si noti che, per due eventi indipendenti, si ha $\Pr(A|B) = \Pr(A)$ (ossia, il verificarsi di A non dipende in alcun modo dal verificarsi di B , visto che la probabilità di A resta la stessa).

ESERCIZIO 1.49. Vengono lanciati tre dadi. Qual è la probabilità che su ciascuno dei tre la faccia rivolta verso l'alto contenga un numero dispari? \diamond

ESERCIZIO 1.50. Sapendo che briscola è “Spade”, qual è la probabilità che l'asso di briscola sia pescato come ultima carta? \diamond

Il teorema di Bayes. Dall'equazione (1.42) sappiamo che $\Pr(A \cap B) = \Pr(A|B) \Pr(B)$. Scambiando il ruolo di A e B abbiamo anche che $\Pr(B \cap A) = \Pr(B|A) \Pr(A)$ e quindi $\Pr(A|B) \Pr(B) = \Pr(B|A) \Pr(A)$. Questo risultato viene solitamente presentato nella forma

$$\Pr(B|A) = \frac{\Pr(A|B) \Pr(B)}{\Pr(A)}$$

ed è noto come teorema di Bayes. Vediamo un esempio di suo utilizzo.

Esempio. Il giocatore di tennis Doppiofallovic ha le seguenti statistiche nei suoi turni di servizio. Il 20% delle volte commette doppio fallo mentre il 50% delle volte gli entra la prima palla. Quando gli entra la prima palla vince il punto l'80% delle volte, mentre quando gli entra la seconda si aggiudica il punto nel 60% dei casi. Supponiamo di aver acceso la televisione nel mezzo di uno scambio, che Doppiofallovic finisce con l'aggiudicarsi. Sapendo che aveva servito Doppiofallovic e conoscendo le sue statistiche, qual'è la probabilità che gli fosse entrata la prima palla?

Se definiamo i seguenti eventi:

- A = Doppiofallovic si aggiudica il punto
- B = è entrata la prima palla
- C = è entrata la seconda palla

il nostro problema consiste nel determinare $\Pr(B|A)$.

Abbiamo $\Pr(B) = 50/100$, $\Pr(A|B) = 80/100$ e $\Pr(C) = 1 - (50/100 + 20/100) = 30/100$, in quanto entra la seconda palla solo quando non entra la prima e non fa doppio fallo. Per quel che riguarda $\Pr(A)$, essendo A l'unione degli eventi disgiunti $A \cap B$ e $A \cap C$, si ha $\Pr(A) = \Pr(A \cap B) + \Pr(A \cap C)$. Dalla definizione di probabilità condizionata abbiamo

$$\Pr(A \cap B) = \Pr(A|B) \Pr(B) = \frac{80}{100} \times \frac{50}{100} = \frac{40}{100}$$

$$\Pr(A \cap C) = \Pr(A|C) \Pr(C) = \frac{60}{100} \times \frac{30}{100} = \frac{18}{100}.$$

Abbiamo allora che $\Pr(A) = 40/100 + 18/100 = 58/100$, per cui, applicando il teorema di Bayes otteniamo

$$\Pr(B|A) = \frac{\Pr(A|B) \Pr(B)}{\Pr(A)} = \frac{80}{100} \times \frac{50}{100} \times \frac{100}{58} = \frac{40}{58} \simeq 69\%.$$

◇

ESERCIZIO 1.51. Ci sono tre scatole (indistinguibili dall'esterno), di cui la prima contiene due monete d'oro, la seconda una moneta d'oro e una d'argento e la terza due monete d'argento. Dopo aver scelto a caso una delle tre scatole, prendiamo, sempre a caso, una moneta al suo interno e scopriamo che è d'oro. Qual è la probabilità che anche l'altra moneta nella scatola sia d'oro? ◇

ESERCIZIO 1.52. In una stanza buia si trovano due scatole, ciascuna contenente 100 caramelle. Una scatola contiene solo caramelle al limone, mentre l'altra contiene 50 caramelle al limone e 50 alla menta. Scegliamo a caso una scatola e cominciamo ad assaggiarne le caramelle, ogni volta rimettendo nella scatola la caramella appena assaggiata. (i) La prima che assaggiamo è al limone. Con che probabilità proviene dalla scatola "mista"? (ii) Quante caramelle vanno assaggiate, nel caso peggiore, prima di poter distinguere le due scatole fra loro con una probabilità di successo pari almeno al 90%? ◇

Esempio. Si consideri il seguente gioco tra due persone: Un'urna contiene $b \geq 0$ palline bianche, $r \geq 1$ palline rosse e $v \geq 0$ palline verdi. A turno, ogni giocatore estrae una pallina. Il gioco termina non appena un giocatore estrae una pallina rossa, nel qual caso quel giocatore perde. Se un giocatore estrae una pallina verde, questa viene rimessa nell'urna, mentre se è bianca viene scartata. In entrambi i casi il giocatore passa la mano all'avversario. Si determini se conviene essere il giocatore che comincia, oppure il secondo, nel caso ($b = 1, r = 1, v = 1$).

Si indichi con $P_W(b, r, v)$ la probabilità di vincere quando ci si trova a dover muovere con un'urna di b, r, v palline, e con $P_L(b, r, v)$ la probabilità di perdere. Chiaramente (non essendo previsto il pareggio)

$P_W(b, r, v) = 1 - P_L(b, r, v)$. Quindi, vogliamo calcolare $P_L(1, 1, 1)$. Ci sono 3 casi: estraggo la rossa, estraggo la verde, estraggo la bianca. Si ha:

$$P_L(1, 1, 1) = 1/3 + 1/3P_W(1, 1, 1) + 1/3P_W(0, 1, 1).$$

Questo perchè, dopo il mio turno, la mia probabilità di perdere è la probabilità di vincere del mio avversario. Si noti inoltre che $P_W(0, 1, 1) > 0$. Si ha quindi

$$3P_L(1, 1, 1) = 1 + 1 - P_L(1, 1, 1) + P_W(0, 1, 1) > 2 - P_L(1, 1, 1)$$

da cui segue $P_L(1, 1, 1) > 1/2$. Quindi è meglio muovere per secondi perchè il primo ha maggiori probabilità di perdere che di vincere. \diamond

ESERCIZIO 1.53. Si consideri il gioco descritto in precedenza. Conviene muovere per primi se $(b = 2, r = 1, v = 1)$? E se l'urna contiene una sola pallina rossa e nessuna verde? \diamond

ESERCIZIO 1.54. Si consideri la seguente variante del gioco descritto in precedenza. Le palle rosse e verdi funzionano come prima, mentre, non appena si pesca una palla bianca, la stessa viene rimpiazzata nell'urna con una nuova palla rossa, e la mano passa all'avversario. Si calcoli la probabilità di vincere, muovendo per primi, dalla situazione $(b = 1, r = 1, v = 1)$. \diamond

1.9.1 Variabili casuali e valor medio

Una *variabile casuale* X , definita su uno spazio di probabilità S , è una funzione $X : S \mapsto R$ a valori reali. Per ogni numero reale v che la variabile può assumere, la probabilità che X assuma il valore v è indicata con

$$\Pr(X = v)$$

ed è definita come $\Pr(X = v) := \Pr(A)$ dove $A \subset S$ è l'insieme dei punti a tali che $X(a) = v$. Ad esempio, consideriamo il lancio di due dadi e sia X la variabile casuale che denota il valore della somma dei due numeri usciti. Lo spazio S ha 36 eventi elementari (coppie del tipo (a, b) con $a, b \in \{1, 2, \dots, 6\}$). Allora, si ha $\Pr(X = v) = 0$ per $v < 2$ o $v > 12$. Inoltre, $\Pr(X = 2) = 1/36 = \Pr(X = 12)$; $\Pr(X = 5) = 4/36$, eccetera.

Il *valor medio* (o *valore atteso*) di una variabile casuale è definito come

$$E[X] := \sum_v (v \cdot \Pr(X = v)). \quad (1.43)$$

Ad esempio, nel caso del lancio dei due dadi si ha, per $v \in 2, 3, \dots, 12$, $\Pr(X = v) = \min\{v - 1, 13 - v\}/36$ (si rifletta sul perchè di questa formula), da cui segue

$$E[X] = \frac{1}{36} (2 \cdot 1 + 3 \cdot 2 + 4 \cdot 3 + 5 \cdot 4 + 6 \cdot 5 + 7 \cdot 6 + 8 \cdot 5 + 9 \cdot 4 + 10 \cdot 3 + 11 \cdot 2 + 12 \cdot 1)$$

e quindi $E[X] = 7$.

Dal punto di vista degli elementi di S , il valore medio può essere anche scritto come

$$E[X] := \sum_{a \in S} (X(a) \cdot \Pr(\{a\})) \quad (1.44)$$

e, nel caso in cui $\Pr(\{a\}) = p$ per ogni a , si ottiene $E[X] := p \sum_{a \in S} X(a)$.

Per il valor medio vale la *linearità*: dati qualsiasi numeri $\alpha, \beta \in \mathbb{R}$ e variabili casuali X e Y , si ha

$$E[\alpha X + \beta Y] = \alpha E[X] + \beta E[Y]. \quad (1.45)$$

Esempio. Un allibratore ci propone il seguente gioco, al prezzo di 10 euro: lui lancerà una moneta fino a quando il lancio risulterà “croce”. Sia $k + 1$ il numero di lanci effettuati, sicchè k è il numero di “teste” ottenute. Se k non sarà un multiplo di 3, allora avremo vinto, e riceveremo 23 euro (la posta più 13 euro di guadagno), altrimenti avremo perso. Ci conviene partecipare a questa scommessa?

Denotiamo con p^S la nostra probabilità di successo a questo gioco. Detta G una variabile casuale che rappresenta il nostro guadagno, il valore medio di G a questo gioco è

$$E[G] = 13p^S + (-10)(1 - p^S) = 23p^S - 10$$

e quindi, l'equilibrio (in cui la partecipazione al gioco non risulta nè vantaggiosa nè svantaggiosa) si ha quando $E[G] = 0$, ossia $p^S = 10/23$. Per $p^S > 10/23$ ci conviene giocare, mentre per $p^S < 10/23$ ci conviene rifiutare la proposta. Detta L una variabile casuale che rappresenta il numero di teste, il nostro successo corrisponde all'evento “ $L \not\equiv 0(\text{mod } 3)$ ”. Ad esempio, le sequenze “TTT TTC” e “TTT TTT TC” sono vincenti, mentre sia “C” che “TTT C” che “TTT TTT C” sono perdenti. Per $i = 0, 1, 2$, denotiamo con p_i la probabilità dell'evento “ $L \equiv i(\text{mod } 3)$ ”, per cui la nostra probabilità di successo è $p^S = p_1 + p_2$. Abbiamo le seguenti relazioni:

$$p_0 = \frac{1}{2} + \frac{1}{2}p_2 \quad (1.46)$$

$$p_1 = \frac{1}{2}p_0 \quad (1.47)$$

$$p_2 = \frac{1}{2}p_1. \quad (1.48)$$

La (1.46) è dovuta al fatto che, per ottenere una sequenza di teste pari a un multiplo di 3 dobbiamo o ottenere una “croce” subito (probabilità $1/2$), o ottenere una “testa” seguita da un numero di teste pari a 2 modulo 3 (probabilità $1/2 \times p_2$). Similmente, (1.47) dice che per ottenere una sequenza di lunghezza $\equiv 1(\text{mod } 3)$, dobbiamo ottenere una “testa” seguita da una sequenza di lunghezza $\equiv 0(\text{mod } 3)$. Infine, (1.48) dice che una sequenza di lunghezza $\equiv 2(\text{mod } 3)$ è una “testa” seguita da una sequenza di lunghezza $\equiv 1(\text{mod } 3)$. Risolvendo il sistema di 3 equazioni in 3 variabili, si ottiene $p_0 = 4/7$, $p_1 = 2/7$ e $p_2 = 1/7$. Essendo $p_1 + p_2 = 3/7 \simeq 0.428 < 10/23 \simeq 0.434$, non ci conviene partecipare a questo gioco (come d'altronde potevamo prevedere, o l'allibratore non ce l'avrebbe offerto...). \diamond

Chapter 2

La matematica degli interi

2.1 Teoria dei numeri

In questa sezione ci occupiamo di alcune proprietà dei numeri interi che sono alla base della cosiddetta *Teoria dei Numeri*. Quest'ultima è una branca della matematica tra le più antiche, e i cui problemi, generalmente di formulazione molto semplice, risultano spesso estremamente difficili da risolvere. Non a caso, molte questioni la cui soluzione appariva difficile 2000 o più anni fa, sono tuttoggi ancora irrisolte. Tra esse, in particolare, troviamo alcune importanti congetture riguardo ai numeri primi.

2.1.1 MCD e mcm

Innanzitutto ricordiamo alcune definizioni relative alla divisione fra interi, operazione introdotta nella sezione 1.4. Siano a e b due interi. Diciamo che a *divide* b (o che a è un *divisore* di b , o che b è un *multiplo* di a) se esiste un intero m tale che $b = am$. Per indicare che a divide b , usiamo la notazione $a \mid b$. Se a non è un divisore di b , allora scriviamo $a \nmid b$.

ESERCIZIO 2.1. Dimostrare che se $a \mid b$ e $a \mid c$, allora $a \mid (b + c)$ e $a \mid (b - c)$. ◇

ESERCIZIO 2.2. Sia r il resto della divisione di b per a . Supponiamo che $c \mid a$ e $c \mid b$. Dimostrare che $c \mid r$. ◇

ESERCIZIO 2.3. Dimostrare che (i) per ogni intero a , si ha $a - 1 \mid a^2 - 1$; (ii) più in generale, che per ogni intero a e naturale positivo n , si ha $a - 1 \mid a^n - 1$. ◇

ESERCIZIO 2.4. Dati $a, b, n \in \mathbb{Z}$, sia $r = a \bmod n$. Dimostrare che $n \mid ab \iff n \mid rb$. ◇

ESERCIZIO 2.5. In una prima elementare ci sono 11 femmine e n maschi. La maestra distribuisce delle caramelle tra i bambini, dandone a ciascuno lo stesso numero. Sapendo che le caramelle distribuite sono in totale $n^2 + 9n - 2$, ci sono più maschi o più femmine nella classe? ◇

Dati due interi a e b , resta definito l'insieme dei loro divisori comuni. Il massimo di tale insieme, è detto il loro *Massimo Comun Divisore*, ed è denotato con $\text{MCD}(a, b)$. Ad esempio:

$$\text{MCD}(1, 6) = 1, \quad \text{MCD}(2, 6) = 2, \quad \text{MCD}(3, 6) = 3, \quad \text{MCD}(4, 6) = 2, \quad \text{MCD}(5, 6) = 1, \quad \text{MCD}(6, 6) = 6.$$

Due numeri per i quali il massimo comun divisore è 1 si dicono *relativamente primi*, o *coprimi*. Inoltre, risulta conveniente definire $\text{MCD}(a, 0) = a$ per ogni intero $a \geq 0$.

In modo simile alla nozione di MCD, si definisce il *minimo comune multiplo* di due interi, denotato con $\text{mcm}(a, b)$. Come tutti avranno immaginato, si tratta del più piccolo fra i multipli comuni positivi di a e b . Ad esempio:

$$\text{mcm}(1, 6) = 6, \quad \text{mcm}(2, 6) = 6, \quad \text{mcm}(3, 6) = 6, \quad \text{mcm}(4, 6) = 12, \quad \text{mcm}(5, 6) = 30, \quad \text{mcm}(6, 6) = 6.$$

L'algoritmo di Euclide per il MCD

Siano a e b due interi positivi. Descriviamo un algoritmo per il calcolo di $\text{MCD}(a, b)$ dovuto ad Euclide.

Algorithm 1 MCD

```

0.  if  $b > a$  then si scambino fra loro  $a$  e  $b$ ;
1.  loop
2.     $r := a \bmod b$ ;
3.    if  $r = 0$  then
4.      return  $b$  /*  $b$  è ora il MCD */;
5.    else
6.       $a := b$ ;
7.       $b := r$ ;
8.    endif
9.  forever
```

La procedura divide il maggiore dei due numeri per il minore, e rimpiazza il maggiore con il minore, e il minore con il resto di tale divisione. Questo processo viene ripetuto finchè il resto non diventa zero. Ad esempio supponiamo che sia $a = 300$ e $b = 18$. Abbiamo $300 = 16 \times 18 + 12$, per cui a diventa 18 e b diventa 12. A questo punto, $18 = 1 \times 12 + 6$, per cui a diventa 12 e b diventa 6. Infine $12 = 2 \times 6 + 0$, sicchè il procedimento si arresta e restituisce $\text{MCD}(300, 18) = 6$.

Veniamo ora alla correttezza dell'algoritmo. Vanno verificate due cose:

- (i) che l'algoritmo termina sempre;
- (ii) che il risultato restituito dopo la terminazione è effettivamente il MCD dei due numeri di ingresso.

Chiamiamo a_i, b_i, r_i i valori di a, b, r all'iterazione i -ma (ossia, dopo aver eseguito la linea 2 l' i -ma volta). Abbiamo $a_1 = a, b_1 = b, r_1 = a \bmod b$ e, in generale, $a_i = b_{i-1}, b_i = r_{i-1}$ e $r_i = a_i \bmod b_i$. Per

quel che riguarda la finitezza dell'algoritmo, facciamo la seguente osservazione: *Ad ogni iterazione, il resto corrente r_i decresce di almeno un'unità rispetto all'iterazione precedente.* Infatti, $r_i = a_i \bmod b_i < b_i = r_{i-1}$. Deduciamo che, siccome il resto è sempre nonnegativo, il ciclo non può ripetersi all'infinito. Per quel che riguarda la correttezza del risultato, detto C_k l'insieme dei divisori comuni di a_k e b_k , si ha il seguente lemma:

Lemma 4: Per ogni coppia di iterazioni successive si ha $C_i = C_{i-1}$.

Dim: (\subseteq) Sia $c \in C_i$, e quindi $c|a_i (= b_{i-1})$ e $c|b_i$. Dobbiamo far vedere che $c|a_{i-1}$. Abbiamo $a_{i-1} = qb_{i-1} + r_{i-1}$ (con $q = a_{i-1} \div b_{i-1}$) da cui $a_{i-1} = qb_{i-1} + b_i = qmc + nc$ per opportuni $m, n \in \mathbb{N}$. Quindi $c|a_{i-1}$ e si conclude che $C_i \subseteq C_{i-1}$.

(\supseteq) Sia $c \in C_{i-1}$, e quindi $c|a_{i-1}$ e $c|b_{i-1} (= a_i)$. Dobbiamo far vedere che $c|b_i$. Come prima, abbiamo $a_{i-1} = qb_{i-1} + r_{i-1} = qb_{i-1} + b_i$. Esistono allora $m, n \in \mathbb{N}$ per cui $mc = qnc + b_i$. Quindi $c|b_i$ e si conclude che $C_{i-1} \subseteq C_i$. ♣

In virtù di questo lemma, ad ogni iterazione dell'algoritmo i divisori comuni di a_i e b_i sono sempre i divisori comuni di a e b . Siccome al termine dell'algoritmo viene restituito certamente il $\text{MCD}(a_i, b_i)$ dei valori correnti, il risultato è il $\text{MCD}(a, b)$.

Facciamo un esempio un po' più complesso: abbiamo $\text{MCD}(89, 55) = \text{MCD}(55, 34) = \text{MCD}(34, 21) = \text{MCD}(21, 13) = \text{MCD}(13, 8) = \text{MCD}(8, 5) = \text{MCD}(5, 3) = \text{MCD}(3, 2) = \text{MCD}(2, 1) = 1$.

Abbiamo visto come l'algoritmo di Euclide termini in ogni caso. Ci chiediamo ora quante iterazioni siano necessarie per sua terminazione. Chiaramente, il numero di iterazioni dipenderà dai valori in ingresso e vogliamo formalizzare questa dipendenza il più accuratamente possibile. Siccome il resto r_i decresce di almeno un'unità ad ogni iterazione, dopo al massimo $r_1 (< b)$ iterazioni l'algoritmo deve terminare, e quindi abbiamo ottenuto una prima stima secondo la quale il numero massimo di iterazioni ha lo stesso ordine di grandezza del minimo fra i due numeri di cui vogliamo calcolare il MCD. Si tratta di una stima pressochè inutile qualora b sia un numero particolarmente grande. Ad esempio, se si tratta di un numero di 100 cifre decimali, sappiamo che non ci vorranno più di circa 10^{100} iterazioni prima di conoscere il risultato, ma ciò non ci rende particolarmente felici nel momento in cui stiamo per lanciare l'algoritmo. Una stima molto più stretta è basata su questa osservazione: *ad ogni coppia di iterazioni consecutive, il resto r_i perlomeno si dimezza.* Infatti, (i) sicuramente $r_{i+2} < r_{i+1}$. Inoltre, detto q il quoziente di a_{i+2} diviso b_{i+2} si ha $r_i = a_{i+2} = qb_{i+2} + r_{i+2} = qr_{i+1} + r_{i+2}$ da cui (ii) $r_{i+2} = r_i - qr_{i+1} < r_i - r_{i+1}$. Sommando le disuguaglianze (i) e (ii) si ottiene $r_{i+2} < r_i/2$. Sia ora T il numero totale di iterazioni dell'algoritmo (i.e., $r_T = 0$) e sia $t = \lfloor T/2 \rfloor$. Abbiamo $1 \leq r_{T-1} < b/2^{t-1}$ da cui $2^{t-1} < b$ e quindi $t-1 < \log_2 b$, che possiamo riscrivere come $t \leq \lceil \log_2 b \rceil$. Essendo $T \leq 2t + 1$ si ha

$$T \leq 2\lceil \log_2 b \rceil + 1 \simeq 2\log_2 b \text{ al crescere di } b.$$

Abbiamo quindi ottenuto una nuova stima del numero di iterazioni dell'algoritmo di Euclide, che ci dice, fondamentalmente, che esso è proporzionale non già ai valori di ingresso, ma *al loro logaritmo*. In particolare, se come nell'esempio precedente i valori d'ingresso avessero 100 cifre decimali, dovremmo attenderci al massimo circa $2 \times \log_2 10^{100}$ iterazioni. Questo valore è inferiore a 1000 iterazioni, il che, rispetto alle 10^{100} iterazioni della stima precedente, ci fa provare un certo sollievo al momento di lanciare l'algoritmo.

Il teorema di Bezout

TEOREMA 5: (Bezout). Siano a e b numeri naturali e sia $d = \text{MCD}(a, b)$. Allora esistono due numeri interi x e y tali che $d = ax + by$.

Di questo teorema daremo due dimostrazioni. La prima si basa sull'algoritmo di Euclide e descrive in che modo si possano calcolare i coefficienti x e y . La seconda è una dimostrazione per induzione.

Dim: (**metodo 1**) Supponiamo di eseguire l'algoritmo di Euclide per il $\text{MCD}(a, b)$ e denotiamo con a_i, b_i, q_i, r_i , per $i = 1, 2, \dots, T$ (dove T è il numero complessivo di iterazioni eseguite) i valori del dividendo, divisore, quoziente e resto all'iterazione i -ma. In generale, abbiamo $b_{i+1} = r_i$, $a_{i+1} = b_i$, $r_{i+1} = r_{i-1}$, e l'algoritmo termina con $r_T = 0$, restituendo $\text{MCD}(a, b) = b_T = r_{T-1}$. Abbiamo

$$r_1 = a_1 - q_1 b_1 = ax_1 + by_1$$

con $x_1 = 1$ e $y_1 = -q_1$. Proseguendo,

$$r_2 = -q_2 b_2 + a_2 = -q_2 r_1 + b_1 = -q_2(ax_1 + by_1) + b = a(-q_2 x_1) + b(-q_2 y_1 + 1) = ax_2 + by_2,$$

e, in generale,

$$r_i = -q_i r_{i-1} + r_{i-2} \tag{2.1}$$

$$= -q_i(ax_{i-1} + by_{i-1}) + ax_{i-2} + by_{i-2} \tag{2.2}$$

$$= a(-qx_{i-1} + x_{i-2}) + b(-qy_{i-1} + y_{i-2}) \tag{2.3}$$

$$= ax_i + by_i. \tag{2.4}$$

Siccome $\text{MCD}(a, b) = r_{T-1}$, si ha $\text{MCD}(a, b) = ax + by$ per $x = x_{T-1}$ e $y = y_{T-1}$.

(metodo 2) Dimostriamo il teorema per induzione su $b = \min\{a, b\}$. Caso base: Se $b = 1$ allora $d = 1$, e, per $x = 0$, $y = 1$ si ha $1 = ax + by$. Passo induttivo: Supponiamo per che per ogni coppia a, b , con $a \geq b$ e $b \in \{1, 2, \dots, n-1\}$ esistano $x, y \in \mathbb{Z}$ tali che $\text{MCD}(a, b) = ax + by$. Consideriamo una coppia a, b con $a \geq b$ e $b = n$, e siano q ed r il quoziente e il resto nella divisione di a per b . Se $r = 0$ allora $\text{MCD}(a, b) = b = ax + by$ per $x = 0$ e $y = 1$. Se invece $r > 0$, essendo $d = \text{MCD}(a, b) = \text{MCD}(b, r)$ dall'ipotesi induttiva abbiamo che esistono interi x', y' tali che $d = bx' + ry'$. Sostituendo $r = a - qb$ si ottiene $d = bx' + (a - qb)y' = ay' + b(x' - qy') = ax + by$ per $x = y'$ e $y = x' - qy'$. ♣

L'equazione $\text{MCD}(a, b) = ax + by$, soddisfatta da opportune coppie (anche non uniche) di interi x, y , è detta *identità di Bezout*. Ad esempio, $4 = 8 \times (-1) + 12 \times 1$ e $4 = 8 \times 2 + 12 \times (-1)$ sono identità di Bezout derivanti dal fatto che $\text{MCD}(8, 12) = 4$. L'identità di Bezout caratterizza il MCD, in quanto vale il seguente lemma.

Lemma 6: Se d divide sia a che b , ed esistono interi x, y tali che $d = ax + by$, allora $d = \text{MCD}(a, b)$.

Dim: Siccome d è un divisore comune di a e b , esso non può essere maggiore del loro MCD, ossia, $d \leq \text{MCD}(a, b)$. D'altro canto, essendo $\text{MCD}(a, b)$ un divisore comune di a e b , esso deve anche dividere $ax + by = d$, il che implica $\text{MCD}(a, b) \leq d$. ♣

Dal teorema di Bezout e dal Lemma 6 otteniamo il seguente corollario.

Lemma 7: Due numeri naturali a e b sono coprimi se e solo se esistono interi x e y tali che $ax + by = 1$.

2.1.2 Numeri primi e loro distribuzione

Un numero naturale $p > 1$ si dice *primo* se i suoi unici divisori positivi sono 1 e p stesso. I primi primi sono

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, \dots$$

Se $p > 1$ non è primo, allora si dice che p è un numero *composto*. In questo caso, esistono numeri naturali $a > 1$ e $b > 1$ tali che $p = ab$. Si noti che, per convenzione, 1 non è nè primo nè composto.

I numeri primi hanno affascinato i matematici sin dai tempi antichi. In tempi più recenti, con l'avvento dei computers e lo studio della codifica e protezione delle informazioni, si è scoperto che essi possono risultare particolarmente utili allo sviluppo di efficaci sistemi di *crittografia*. In particolare, sono stati sviluppati degli algoritmi di crittografia la cui robustezza si basa sull'assunto che risulta difficile, anche utilizzando dei potenti computers, trovare i fattori primi di un numero composto “sufficientemente grande”. Inoltre, questi sistemi di crittografia adoperano per la codifica/decodifica dei messaggi alcuni numeri primi “particolarmente grandi”. La crittografia è stata quindi il motore di numerose ricerche relativamente al problema di come verificare se un numero sia primo o no e di come generare numeri primi di molte cifre. Su entrambi i problemi sono stati ottenuti risultati notevoli (come ad esempio la costruzione di numeri primi con migliaia di cifre decimali), il cui studio risulta però troppo complesso per essere affrontato in questo testo introduttivo.

Abbiamo visto in sezione 1.2 come esistano infiniti numeri primi. Una domanda interessante sorge rispetto alla loro densità: quanti numeri composti si trovano, mediamente, tra due numeri primi? È facile dimostrare il seguente risultato:

TEOREMA 8: Per ogni $k \geq 1$, esiste un blocco di k numeri naturali consecutivi tale che nessuno di essi è un numero primo.

Dim: Sia $n = k + 1$. Consideriamo i numeri

$$n! + 2, n! + 3, \dots, n! + n.$$

Il primo di essi è divisibile per 2, il secondo per 3, e così via fino all'ultimo che è divisibile per n . Quindi, sono tutti numeri composti, e ce ne sono $n - 1 = k$. ♣

Per quanto esistano queste “isole” di numeri composti arbitrariamente larghe, in realtà esse non si presentano così spesso (in effetti, la costruzione utilizzata nella dimostrazione del teorema restituisce dei numeri enormi, e viene da chiedersi quanto, mediamente, siano lunghe le sequenze di numeri composti comprese nell'intervallo $1, \dots, N$ al variare di N). È stato dimostrato che per ogni $k \geq 1$, esistono numeri primi di k cifre, ma questo risultato lascia spazio a potenziali isole la cui lunghezza è dell'ordine di N stesso. Un risultato più preciso è il seguente:

TEOREMA 9: (Teorema dei numeri primi) Sia $\pi(N)$ il numero di primi nell'intervallo $1, 2, \dots, N$. Allora

$$\pi(N) \sim \frac{N}{\ln N}.$$

Quindi, una frazione pari a circa $1/\ln N$ dei numeri tra 1 e N è fatta di numeri primi. Si noti che N è esponenziale rispetto a $\ln N$ e quindi la gran maggioranza dei numeri è costituita da numeri composti. Inoltre, il teorema ci dà (approssimativamente, e per N “sufficientemente grande”) la probabilità che, preso a caso un numero tra 1 e N , esso sia composto. Ad esempio, la probabilità che un intero casuale nell’insieme $\{1, 2, \dots, 10000\}$ sia primo è circa $1/9.21$, ossia tra il 10% e l’11%.

Possiamo usare il teorema dei numeri primi per cercare di dare una risposta alla seguente domanda:

Quanti numeri primi esistono di k cifre decimali ciascuno?

Per rispondere a questa domanda, possiamo sottrarre i numeri primi nell’intervallo $[1, \dots, 10^{k-1}]$ da quelli nell’intervallo $[1, \dots, 10^k]$. In base al teorema dei numeri primi, tale quantità è circa

$$\frac{10^k}{k \ln 10} - \frac{10^{k-1}}{(k-1) \ln 10} = \frac{(9k-10)10^{k-1}}{k(k-1) \ln 10}.$$

Essendo

$$\frac{9k-10}{k-1} = 9 - \frac{1}{k-1}$$

molto prossimo a 9 per k sufficientemente grande, ricaviamo che il numero di primi di k cifre è circa

$$9 \times \frac{10^{k-1}}{k \ln 10}.$$

Siccome esistono in tutto $10^k - 10^{k-1} = 9 \cdot 10^{k-1}$ numeri di k cifre, abbiamo che la frazione di essi data dai numeri primi è

$$\frac{1}{k \ln 10} \simeq \frac{1}{2.3k}.$$

Quindi, tra gli interi di k cifre, circa uno ogni $2.3k$ è primo. (Ovviamente si tratta di una stima approssimativa, che diventa via via più precisa al crescere di k).

Primi di Mersenne e di Fermat Tra i molti argomenti di studio relativi ai numeri primi, uno dei più affascinanti è quello di determinare qualche funzione che restituisca dei numeri primi per ogni scelta dei parametri di ingresso su un opportuno dominio. Si consideri ad esempio l’espressione

$$M(n) = 2^n - 1$$

per n un numero primo. Abbiamo $M(2) = 3$ (primo), $M(3) = 7$ (primo), $M(5) = 31$ (primo), $M(7) = 127$ (primo). La formula sembra quindi funzionare, ma il successivo valore di n genera un numero composto: $M(11) = 2047 = 23 \times 89$. I numeri della forma $2^n - 1$ vengono chiamati *numeri di Mersenne*, in onore del matematico francese Marin Mersenne che per primo ne investigò le caratteristiche nel diciassettesimo secolo. In particolare, i numeri primi di questa forma sono detti *primi di Mersenne*. I più piccoli primi di Mersenne, oltre ai quattro appena citati, includono $M(13)$, $M(17)$, $M(19)$, $M(61)$, $M(89)$ e $M(107)$ e

$$M(127) = 170\,141\,183\,460\,469\,231\,731\,687\,303\,715\,884\,105\,727.$$

Ad oggi, il più grande primo di Mersenne noto è $M(57885161) = 2^{57885161} - 1$, che ha più di diciassette milioni di cifre decimali.

Abbiamo visto che l'essere n primo non è condizione sufficiente per la primalità di $2^n - 1$. Essa è però una condizione necessaria.

TEOREMA 10: Se $M(n) = 2^n - 1$ è primo, allora anche n è primo.

Dim: Supponiamo n composto, e siano a, b suoi divisori proprii in modo che $n = ab$. Essendo $\sum_{i=0}^{b-1} (2^a)^i = \frac{(2^a)^b - 1}{2^a - 1}$ segue

$$2^n - 1 = 2^{ab} - 1 = \left(\sum_{i=0}^{b-1} (2^a)^i \right) (2^a - 1)$$

e quindi $M(n)$ è un numero composto. ♣

Una formula simile a quella di Mersenne fu proposta da Pierre De Fermat, e anch'essa sembra inizialmente funzionare bene per la generazione di numeri primi. In particolare, chiamiamo *numero di Fermat* un numero della forma

$$F(n) = 2^{2^n} + 1$$

per $n \in \mathbb{N}$. I numeri di Fermat che risultano primi sono detti *primi di Fermat*. Abbiamo $F(0) = 3$ (primo), $F(1) = 5$ (primo), $F(2) = 17$ (primo), $F(3) = 257$ (primo), $F(4) = 65537$ (primo). Essendo che per ogni valore di $n \leq 4$ si otteneva un numero primo, Fermat ipotizzò che la formula restituisse un primo per ogni n . In effetti all'epoca (nel 1640) era difficile verificare anche solo se $F(5) = 2^{32} + 1$ fosse primo, trattandosi di un numero piuttosto grande da scomporre in fattori senza l'uso di calcolatori elettronici. Nel secolo successivo Eulero scoprì che ogni divisore di $F(n)$ deve essere della forma $k \cdot 2^{n+2} + 1$. Nel caso di $F(5)$, per $k = 1, 2, 3, 4, 5$ troviamo i valori 129, 257, 385, 513, 641. Di essi, i potenziali divisori sono solo 257 e 641 (in quanto primi), e 641 divide $F(5)$. Ad oggi non sono noti primi di Fermat maggiori di $F(4)$ e si ritiene molto probabile che i primi di Fermat siano in numero finito.

Un'altra formula interessante per la generazione di numeri primi è la seguente:

$$n^2 - 79n + 1601.$$

Può essere verificato che questa formula fornisce, sorprendentemente, dei numeri primi per ogni $n \in \{0, 1, \dots, 79\}$. Purtroppo però, per $n = 80$ la formula restituisce un numero composto.

Alcune congetture sui primi. Riportiamo in questa sezione alcune interessanti congetture che riguardano i numeri primi. Nonostante per qualcuna di esse (grazie soprattutto al massiccio uso di potenti computers) si siano ottenuti dei progressi, su molte altre siamo sostanzialmente fermi al momento in cui esse furono formulate (in alcuni casi, centinaia di anni fa):

- (*Congettura di Goldbach*) Ogni numero naturale pari > 2 può essere espresso come somma di due primi. Ad esempio, $8 = 3 + 5$; $16 = 3 + 13$; $80 = 37 + 43$; ecc. Questa congettura è stata verificata essere soddisfatta da tutti i naturali pari fino a circa 10^{18} .
- (*Congettura di Lemoine*) Ogni numero naturale dispari > 5 può essere espresso come somma di un primo con il doppio di un primo. In termini algebrici, viene congetturato che l'equazione $2n+1 = x+2y$ ha sempre soluzioni x, y nell'insieme dei numeri primi, per $n > 2$. Ad esempio $47 = 13 + 2 \times 17 = 37 + 2 \times 5 = 41 + 2 \times 3 = 43 + 2 \times 2$. Questa congettura è stata verificata essere soddisfatta da tutti i naturali dispari fino a circa 10^9 .

- (*I Primi gemelli*) Esistono infinite coppie $(a_1, b_1), (a_2, b_2), \dots$, di numeri primi tali che $b_i - a_i = 2$ per ogni i . Due tali primi si dicono *gemelli*. Ad esempio, le prime coppie di questo tipo sono

$$(3, 5), (5, 7), (11, 13), (17, 19), (41, 43), (71, 73), (101, 103), (107, 109), (137, 139), \dots$$

Ad oggi, è stato verificato che esistono 808,675,888,577,436 coppie di primi gemelli $\leq 10^{18}$. Inoltre, sono stati individuati primi gemelli con più di 100,000 cifre.

- (*Congettura di Legendre*) Per ogni naturale $n > 1$ esiste sempre almeno un numero primo compreso nell'intervallo tra n^2 e $(n+1)^2$. (Una congettura dall'enunciato simile è il *postulato di Bertrand*, che afferma che, per ogni $n > 1$, esiste sempre un primo compreso nell'intervallo tra n e $2n$. Questa congettura è stata poi dimostrata essere vera ed è quindi oggi un teorema. Esistono diverse dimostrazioni di questo risultato, e la più elegante fra esse è una prova combinatorica del grande matematico ungherese Paul Erdos).
- (*Primi di Mersenne e di Fermat*) Esistono infiniti primi di Mersenne. Nel senso opposto a questa congettura ve n'è una che ipotizza che gli unici numeri primi di Fermat si abbiano in corrispondenza di $n = 0, 1, 2, 3, 4$.

2.1.3 Fattorizzazione in primi

Sia n un numero naturale maggiore di 1. In questa sezione vedremo che n è sempre esprimibile, in modo univoco, come un prodotto di un numero finito di fattori primi (dove per “prodotto” di un singolo fattore si intende il fattore stesso). Questo prodotto viene detto una *fattorizzazione* di n in primi. Diciamo che due fattorizzazioni sono uguali se contengono gli stessi primi, ognuno ripetuto lo stesso numero di volte. In particolare, questo significa che dati due prodotti $p_1 \times p_2 \times \dots \times p_k$ e $q_1 \times q_2 \times \dots \times q_r$, essi sono la stessa fattorizzazione se $k = r$ ed è possibile riordinare i termini p_i , chiamando $p'_1 \times \dots \times p'_k$ il prodotto riordinato, in modo tale che risulti $p'_i = q_i$ per $i = 1, \dots, k$.

TEOREMA 11: (Esistenza della fattorizzazione) Ogni numero naturale $n \geq 2$ è esprimibile come un prodotto di un numero finito di fattori primi.

Dim: Per induzione. Il caso base è $n = 2$: siccome 2 è primo, allora n coincide con la sua fattorizzazione, data da un unico fattore. Supponiamo ora vero l'asserto per ogni numero in $\{2, 3, \dots, n-1\}$ e dimostriamolo per n . Se n è primo, allora n coincide con la sua fattorizzazione, data da un unico fattore. Altrimenti, siano a, b , con $1 < a, b < n$, tali che $n = ab$. Per induzione, esiste una fattorizzazione in primi di a , sia essa $a = p_1 \times \dots \times p_k$, e una di b , sia essa $b = q_1 \times \dots \times q_r$. Ma allora esiste la fattorizzazione di n data da $n = p_1 \times \dots \times p_k \times q_1 \times \dots \times q_r$. ♣

Dimostreremo ora il *Teorema Fondamentale dell'Aritmetica*, che afferma che la fattorizzazione di un numero in fattori primi è di fatto unica. Per questa dimostrazione, abbiamo bisogno di un risultato preliminare.

TEOREMA 12: Sia $p > 1$ un numero naturale. p è primo se e solo se per ogni coppia di numeri naturali a e b , se $p|ab$ allora $p|a$ oppure $p|b$.

Dim: (\Rightarrow) Supponiamo che p sia primo, che $p|ab$ e che $p \nmid a$. Si ottiene che $\text{MCD}(a, p) = 1$, in quanto, essendo p un numero primo, il massimo comun divisore può essere solo 1 oppure p , ma non può essere p , visto che $p \nmid a$. Per il teorema di Bezout, esistono interi x e y tali che $1 = ax + py$. Allora $b = b \cdot 1 = abx + pby$. Siccome $p|ab$, otteniamo che $p|b$.

(\Leftarrow) Supponiamo che p abbia la proprietà suddetta e scriviamo $p = ab$, con $0 < a < p$. Siccome $p \nmid a$, deve essere $p|b$, quindi $b = pc$ per qualche $c \in \mathbb{N}$. Ne segue $p = ab = apc$, ossia $0 = p(1 - ac)$. Ma allora $ac = 1$ e quindi $a = 1$. In conclusione, p non ha divisori propri maggiori di 1 e minori di p stesso, e quindi è primo. ♣

COROLLARIO 13: Sia p un numero primo e supponiamo che $p|a_1 \times a_2 \times \cdots \times a_r$. Allora $p|a_i$ per almeno un i , $1 \leq i \leq r$.

Dim: La dimostrazione è facile, per induzione su r . ♣

TEOREMA 14: (Teorema fondamentale dell'aritmetica) Ogni numero naturale $n \geq 2$ è esprimibile in un unico modo come un prodotto di un numero finito di fattori primi.

Dim: Abbiamo già dimostrato l'esistenza della fattorizzazione, per cui ci basta fare vedere che la fattorizzazione è unica. Supponiamo per assurdo che esistano dei numeri maggiori di 1 che ammettono fattorizzazioni diverse. In particolare, sia \bar{n} il minimo tra tali controesempi. Indichiamo due fattorizzazioni diverse di \bar{n} con

$$\bar{n} = p_1 \times \cdots \times p_k = q_1 \times \cdots \times q_r.$$

Siccome $p_k|q_1 \times \cdots \times q_r$, allora, in base al corollario 13, p_k divide almeno uno dei q_i . Essendo tutti i q_i primi, ciò implica che $p_k = q_t$ per un $t \in \{1, 2, \dots, r\}$. Senza perdita di generalità, supponiamo $t = r$. Ma allora, dividendo entrambe le fattorizzazioni per $p_k (= q_r)$ e detto $\hat{n} = p_1 \times p_2 \times \cdots \times p_{k-1}$, si ha

$$\hat{n} = p_1 \times \cdots \times p_{k-1} = q_1 \times \cdots \times q_{r-1}$$

dove le fattorizzazioni $p_1 \times \cdots \times p_{k-1}$ e $q_1 \times \cdots \times q_{r-1}$ sono diverse perchè erano diverse le fattorizzazioni di \bar{n} . Ma allora \bar{n} non sarebbe il più piccolo controesempio, in quanto $\hat{n} < \bar{n}$. ♣

Per convenzione, nel riportare la fattorizzazione di un numero, i fattori vengono sempre elencati in ordine non-decrescente. Inoltre, vengono raggruppati i fattori uguali, la cui molteplicità diventa l'esponente del corrispondente fattore. Alcuni esempi: $100 = 2^2 \times 5^2$; $150 = 2 \times 3^2 \times 5$; $30492 = 2^2 \times 3^3 \times 7 \times 11^2$ ecc.

Si può poi pensare di estendere la fattorizzazione a *tutti* i numeri primi, in modo tale che ogni numero può essere rappresentato come il prodotto di tutti i primi, ciascuno elevato ad un opportuno esponente. Tale esponente risulterà 0 per quasi tutti i fattori, e sarà diverso da 0 solo per un numero finito di fattori. Quindi, per ogni naturale $n \geq 2$ esistono naturali k_1, k_2, \dots , tali che

$$n = 2^{k_1} \times 3^{k_2} \times 5^{k_3} \times 7^{k_4} \times 11^{k_5} \times \cdots$$

Quando è nota la fattorizzazione in primi di due numeri a e b , diventa molto facile calcolare il loro MCD e mcm. Infatti, supponiamo che le fattorizzazioni in primi siano $a = p_1^{n_1} \times p_2^{n_2} \times \cdots \times p_k^{n_k}$ e $b =$

$p_1^{m_1} \times p_2^{m_2} \times \dots \times p_k^{m_k}$ (dove ciascuna fattorizzazione è stata estesa in modo da coinvolgere gli stessi divisori primi. Chiaramente, alcuni degli esponenti n_i e m_i possono essere nulli, in corrispondenza dei fattori primi che dividono solo uno dei due numeri). Abbiamo allora il seguente risultato (la cui dimostrazione è lasciata al lettore)

$$\begin{aligned} \text{MCD}(a, b) &= p_1^{\min(n_1, m_1)} \times p_2^{\min(n_2, m_2)} \times \dots \times p_k^{\min(n_k, m_k)} \\ \text{mcm}(a, b) &= p_1^{\max(n_1, m_1)} \times p_2^{\max(n_2, m_2)} \times \dots \times p_k^{\max(n_k, m_k)}. \end{aligned}$$

Ad esempio, sia $a = 18 = 2 \times 3^2$ e $b = 60 = 2^2 \times 3 \times 5$. Abbiamo allora $\text{MCD}(18, 60) = 2 \times 3 = 6$ e $\text{mcm}(18, 60) = 2^2 \times 3^2 \times 5 = 180$.

ESERCIZIO 2.6. Dimostrare che per qualsiasi coppia di interi a e b si ha $\text{MCD}(a, b) \times \text{mcm}(a, b) = ab$. \diamond

ESERCIZIO 2.7. Dimostrare che per ogni numero naturale dispari n si ha $\text{MCD}(2^{n-1} + 1, 2^n - 1) = 1$. \diamond

Per quel che riguarda la fattorizzazione in primi del fattoriale di n , abbiamo il seguente teorema (noto come Teorema di Legendre),

TEOREMA 15: Il numero $n!$ contiene il fattore primo p esattamente

$$\sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor$$

volte.

Dim: Innanzitutto, esattamente $\left\lfloor \frac{n}{p} \right\rfloor$ dei fattori di $n! = 1 \times 2 \times 3 \times \dots \times n$ sono divisibili per p . Inoltre, $\left\lfloor \frac{n}{p^2} \right\rfloor$ di tali fattori sono divisibili anche per p^2 , altri $\left\lfloor \frac{n}{p^3} \right\rfloor$ sono divisibili anche per p^3 e così via. \clubsuit

Ad esempio, nello sviluppo di $15!$, il fattore primo 3 compare $\left\lfloor \frac{15}{3} \right\rfloor + \left\lfloor \frac{15}{9} \right\rfloor = 5 + 1 = 6$ volte. Similmente, il 2 compare $7 + 3 + 1 = 11$ volte, il 5 compare 3 volte, il 7 compare 2 volte, mentre l'11 e il 13 compaiono una volta ciascuno. Quindi $15! = 2^{11} \times 3^6 \times 5^3 \times 7^2 \times 11 \times 13$.

ESERCIZIO 2.8. Con quanti zeri termina il numero $56!$? \diamond

2.1.4 Il piccolo teorema di Fermat

Lemma 16: Siano p un numero primo e $a \in \mathbb{Z}$ tale che $p \nmid a$. Allora, presi $i, j \in \{0, 1, \dots, p-1\}$ con $i \neq j$ si ha $ia \not\equiv ja \pmod{p}$.

Dim: Senza perdita di generalità sia $j > i$ e supponiamo per assurdo che $ia \equiv ja \pmod{p}$. Quindi, $p \mid (ja - ia) = a(j - i)$, e, visto che $p \nmid a$, deve essere $p \mid (j - i)$. Ma $0 < j - i < p$ da cui l'assurdo. \clubsuit

TEOREMA 17: (**Piccolo teorema di Fermat**) Sia p un numero primo e $a \in \mathbb{Z}$. Se $p \nmid a$, allora $a^{p-1} \equiv 1 \pmod{p}$.

Dim: Siccome p ed a sono coprimi, per il Lemma 16 i numeri $\{0, a, 2a, \dots, (p-1)a\}$, sono tutti diversi modulo p e quindi sono congruenti (non necessariamente in quest'ordine) con i numeri $\{0, 1, 2, \dots, p-1\}$. Siccome $x' \equiv x'' \pmod{p}$ e $y' \equiv y'' \pmod{p}$ implicano $x'y' \equiv x''y'' \pmod{p}$, allora

$$a \times 2a \times \dots \times (p-1)a \equiv 1 \times 2 \times \dots \times (p-1) \pmod{p}$$

e quindi

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

Abbiamo allora che $p \mid ((p-1)!(a^{p-1} - 1))$, e, visto che $p \nmid (p-1)!$, deve essere $p \mid (a^{p-1} - 1)$. Quindi $a^{p-1} \equiv 1 \pmod{p}$. ♣

COROLLARIO 18: Sia p un numero primo. Allora, per ogni $a \in \mathbb{Z}$ si ha $a^p \equiv a \pmod{p}$.

2.1.5 Test di primalità

Dato un numero n , consideriamo il problema di determinare se n è primo o composto. Il piccolo teorema di Fermat ci dice che, se n è primo, per ogni $a \in \{1, \dots, n-1\}$, deve risultare $a^{n-1} \equiv 1 \pmod{n}$, ma si tratta solo di una condizione necessaria e non sufficiente per la primalità di n . Prendiamo allora a caso un intero $1 \leq a < n$ ed eseguiamo i seguenti test (di cui il secondo va eseguito solo qualora il primo non abbia già determinato che n è composto):

1. **if** $\text{MCD}(a, n) > 1$ **return** “composto”
2. Sia $r := a^{n-1} \pmod{n}$. **if** $r \neq 1$ **return** “composto” **else return** “forse primo”.

Si noti che il secondo test (detto il *test di Fermat*) viene eseguito solo quando a è coprimo con n . Osserviamo che se 1. o 2. restituiscono “composto” allora certamente n è un numero composto. In particolare, se a risulta coprimo con n e $r \neq 1$, diciamo che a è un *testimone di Fermat* (essendo un testimone del fatto che n sia composto), mentre se otteniamo $r = 1$, la nostra fiducia che n sia primo aumenta, anche se non ne abbiamo ancora la certezza. Se ora ripetessimo questo esperimento un certo numero di volte, e ogni volta ottenessimo “forse primo”, saremmo portati a ritenere che n sia probabilmente primo. Per poter quantificare questa probabilità ci sono però due problemi da considerare:

- (P1.) Esistono dei numeri composti, detti i *numeri di Carmichael*, per i quali il test di Fermat dà esito positivo (i.e., $r = 1$) per ogni $a \in \{1, \dots, n-1\}$ coprimo con n e dovremmo conoscere quanti sono tali numeri rispetto ai primi.
- (P2.) Quand'anche un numero n composto non fosse un numero di Carmichael, dovremmo conoscere la frazione (o almeno un limite inferiore della stessa) di numeri $a \in \{1, \dots, n-1\}$, coprimi con n , per i quali il test di Fermat dà esito positivo. Ogni tale numero è detto un *bugiardo di Fermat* per n , mentre n viene detto uno *pseudoprimo di Fermat* (relativamente ad a).

Facciamo alcuni esempi. Vogliamo verificare se 119 è un numero primo, e usiamo a tal fine il test di Fermat su un valore di a “casuale”. Ad esempio, prendiamo $a = 6$, visto che il nome “Fermat” si compone di 6 lettere. Le seguenti congruenze vanno tutte intese modulo 119:

$$6^{118} \equiv (6^3)^{39} \cdot 6 \equiv 97^{39} \cdot 6 \equiv (97^3)^{13} \cdot 6 \equiv 62^{13} \cdot 6 \equiv (62^6)^2 \cdot 62 \cdot 6 \equiv 8^2 \cdot 62 \cdot 6 \equiv 8$$

e quindi 119 non è primo (in effetti, $119 = 7 \times 17$). Similmente, proviamo a verificare se 71 è primo, usando il valore “casuale” $a = 17$ (essendo Pierre De Fermat nato il 17 agosto). Abbiamo le seguenti congruenze modulo 71:

$$17^{70} \equiv ((17^2)^5)^7 \equiv ((5^5)^7) \equiv 1^7 \equiv 1$$

e quindi 71 potrebbe essere primo. In effetti, se ripetessimo il test anche per altre basi otterremmo sempre 1, perchè 71 è proprio primo.

La presenza degli pseudoprimi, e, soprattutto, dei numeri di Carmichael, getta delle ombre sull'utilità del test di Fermat. Ad esempio, il numero 341 non è primo (essendo $341 = 11 \cdot 31$), ma il test di Fermat con $a = 2$ restituisce $2^{340} \equiv 1 \pmod{341}$. Ripetendo il test con, ad esempio, $a = 3$, otteniamo

$$3^{340} \equiv (((3^6)^7)^4)^2 \times 3^4 \equiv ((47^7)^4)^2 \times 81 \equiv (163^4)^2 \times 81 \equiv 159^2 \times 81 \equiv 56 \pmod{341}$$

e quindi deduciamo che 341 è un numero composto. Si può verificare che 99 dei 299 numeri coprimi con 341 nell'intervallo $\{2, \dots, 340\}$ sono dei bugiardi di Fermat per il numero 341. Se invece consideriamo il numero $561 = 3 \times 11 \times 17$, ci sono 319 numeri ad esso coprimi nell'intervallo $\{2, \dots, 560\}$, ed ognuno di essi è un bugiardo di Fermat. In effetti, 561 è un numero di Carmichael.

Relativamente ai problemi (P1.) e (P2.) del test di Fermat si possono fare le seguenti considerazioni:

- (P1.) Per quanto sia stato dimostrato che esistono infiniti numeri di Carmichael, è stato anche dimostrato che essi sono estremamente rari (ad esempio, vi sono 78498 primi nell'insieme $\{1, 2, \dots, 10^6\}$, ma solo 43 numeri di Carmichael). In questo senso, quindi, la loro esistenza non pregiudica in modo irrimediabile l'utilità del test di Fermat. (Esistono inoltre dei test alternativi al test di Fermat per aggirare il problema dato dai numeri di Carmichael).
- (P2.) Quando applichiamo il test di Fermat a un numero non di Carmichael, esso risulta molto efficace in quanto con poche ripetizioni dello stesso possiamo raggiungere una confidenza estremamente alta sulla veridicità della risposta. In particolare, la probabilità che un tale numero n sia composto ma risulti potenzialmente primo dopo k applicazioni del test di Fermat è inferiore a $\frac{1}{2^k}$. Infatti, almeno metà dei numeri $a \in \{1, \dots, n-1\}$ coprimi con n sono testimoni di Fermat, in base al seguente lemma:

Lemma 19: Sia a un testimone di Fermat, e siano a_1, a_2, \dots, a_s dei bugiardi di Fermat. Allora $a'_i := a \times a_i$ è un testimone di Fermat per ogni $i = 1, \dots, s$.

Dim: Per ogni $i = 1, \dots, s$, si ha $(aa_i)^{n-1} \equiv a^{n-1}a_i^{n-1} \equiv a^{n-1} \not\equiv 1 \pmod{n}$. ♣

ESERCIZIO 2.9. Verificare che 4321 è un numero composto, applicando il test di Fermat per $a = 2$. ◇

ESERCIZIO 2.10. Dimostrare che ogni numero di Carmichael è dispari. ◇

2.2 Pari e Dispari

Ci sono alcuni problemi della matematica combinatorica la cui soluzione più semplice ed elegante è quella di ricorrere ad argomenti di *parità* e/o *simmetria*. Il concetto di parità è ben noto, e sappiamo che gli interi si

ripartiscono in due classi, i numeri pari e quelli dispari. Diciamo che due numeri hanno la stessa parità se appartengono alla medesima classe, ossia se sono entrambi pari o entrambi dispari. Il concetto apparentemente elementare di parità è alle volte indispensabile nella risoluzione di problemi che, qualora venissero affrontati senza farvi ricorso, potrebbero risultare di complessità estrema. L'unico modo per convincersi di ciò è quello di fare degli esempi, per cui, cominciamo.

Esempio (1). Pavimentazione di rettangoli. Nel gioco della battaglia navale, ogni nave è rappresentata da un rettangolo di $L \times 1$ quadratini, piazzati in orizzontale o in verticale, all'interno di un'area di gioco ricavata su un foglio a quadretti. In particolare, l'area di gioco è essa stessa un rettangolo, con B quadratini di base e H di altezza. Supponiamo ora di considerare solo navi di due quadratini ciascuna ($L = 2$) e ci chiediamo se sia possibile riempire completamente l'area di gioco con tali navi. Una condizione necessaria affinché questo risulti possibile è che almeno uno tra H e B sia pari. Infatti, in caso contrario, l'area di gioco conterrebbe un numero dispari di quadratini, ma l'area coperta dalle navi consisterebbe sempre di un numero pari di quadratini, dato che ogni nave copre un numero pari di quadratini. Non è difficile dimostrare che la condizione è anche sufficiente per l'esistenza di una copertura perfetta. Consideriamo ora un'area di gioco quadrata e in cui la base B sia pari. Quest'area ha un numero pari di quadratini ed è copribile in modo perfetto con navi di lunghezza 2. Supponiamo ora di rimuovere dall'area di gioco due quadratini, quello in alto a sinistra (riga 1, colonna 1) e quello in basso a destra (riga B , colonna B) e di chiederci se esista ancora una copertura perfetta dell'area risultante con navi di due quadratini ciascuna. Per quanto l'area di gioco così modificata abbia ancora un numero pari di quadratini, la copertura perfetta non è più possibile. Il modo migliore di dimostrarlo è quello di utilizzare un argomento di parità. Supponiamo di colorare l'area di gioco iniziale con due colori, come in una scacchiera. L'area conterrebbe $B^2/2$ quadratini neri ed altrettanti bianchi. I due quadratini rimossi si trovano entrambi sulla stessa diagonale della scacchiera e quindi hanno lo stesso colore (diciamo nero). Dopo la loro rimozione, l'area di gioco conterrebbe più quadratini bianchi che neri, ma ogni nave copre esattamente un quadratino bianco e uno nero e quindi una copertura non sarebbe possibile.

Consideriamo ora navi di lunghezza $L = 3$. Chiaramente, per poter coprire perfettamente un'area di gioco, è necessario che $B \times H$ sia divisibile per 3. Questo implica che almeno uno tra B e H sia un multiplo di 3. Supponiamo allora di prendere un'area di gioco 6×7 (che banalmente ammette una copertura perfetta con navi di lunghezza 3, disposte due per riga) e di rimuovere tre qualsiasi quadratini da tre dei quattro angoli. Ci chiediamo ora se l'area risultante ammetta ancora una copertura perfetta. Anche in questo caso, la risposta è che una copertura perfetta non è più possibile, e la dimostrazione si basa su una colorazione dell'area di gioco con 3 colori (chiamiamoli 1, 2 e 3) secondo il seguente schema:

1	2	3	1	2	3
2	3	1	2	3	1
3	1	2	3	1	2
1	2	3	1	2	3
2	3	1	2	3	1
3	1	2	3	1	2
1	2	3	1	2	3

Si noti che ogni tre quadratini consecutivi, siano essi orizzontali o verticali, presentano tutti i tre colori e quindi ogni nave copre un quadratino di ogni colore. In particolare, se esistesse una copertura perfetta, l'area di gioco dovrebbe contenere lo stesso numero di quadratini per ciascuno dei tre colori. Inizialmente ci sono

14 quadratini di ciascun colore. Rimuovendo 3 quadratini d'angolo, vediamo che non viene rimosso alcun quadratino di colore 2 e quindi resterebbero più quadratini di colore 2 che di altri colori. Questo implica che una copertura perfetta diventa impossibile.

Problemi del tipo appena esposto, in cui un'area del piano deve essere coperta utilizzando delle particolari forme prefissate (in questo caso dei rettangoli), vengono detti problemi di *pavimentazione* (in inglese, *tiling*) e le forme utilizzate sono chiamate piastrelle o tasselli (in inglese, *tiles*). Si tratta di problemi che possono risultare estremamente complessi, a seconda della forma della regione da piastrellare e delle piastrelle che è possibile utilizzare.

Esempio (2). Il giro del cavallo. Nel gioco degli scacchi, il cavallo effettua una caratteristica mossa “ad L”. In particolare, dette (x, y) le coordinate della casella in cui si trova, il cavallo può muovere verso ciascuna (ammesso che esista) tra 8 caselle del tipo $(x \pm \delta_x, y \pm \delta_y)$, con $\delta_x, \delta_y \in \{1, 2\}$ e $\delta_x \neq \delta_y$.

Supponiamo ora di avere a disposizione una scacchiera 7×7 e di aver posizionato il cavallo in riga 1, colonna 2. Ci chiediamo se, partendo da lì ed effettuando sempre mosse ad L, si possa riuscire a visitare una ed una sola volta tutte le caselle della scacchiera. Vogliamo dimostrare che questo è impossibile.

La soluzione migliore è ricorrere ad un argomento di parità. Supponiamo che le caselle siano colorate, nel classico modo, nere e bianche. Senza perdita di generalità, supponiamo che la casella $(1, 1)$ sia nera e quindi la $(1, 2)$ è bianca. Siccome il lato della scacchiera è un numero dispari, ci sono in tutto un numero dispari di caselle. In particolare, ci sono 25 caselle nere e 24 bianche. Dopo aver posizionato il cavallo sulla casella iniziale, dobbiamo effettuare 48 mosse, visto che ad ogni mossa viene visitata una nuova casella. Siccome ad ogni mossa il colore della casella di arrivo è diverso da quello della casella di partenza, dopo un numero pari di mosse il cavallo ha visitato un numero uguale di caselle bianche e nere. Quindi, avrebbe visitato 24 caselle bianche e 24 nere. Ma la casella iniziale era bianca, e quindi ci sarebbero 25 caselle bianche, assurdo.

Esempio (3). Le lampadine. Ci sono n lampadine, inizialmente tutte spente. Ad ogni iterazione, possiamo azionare l'interruttore di esattamente $n - 1$ lampadine, e questa operazione può essere ripetuta più volte, con l'obiettivo finale di accendere tutte le lampadine. Dimostrare che ciò è possibile se e solo se n è pari.

(i) Sia n pari. Per $i = 1, \dots, n$ ripetiamo l'operazione : “azionare tutti gli interruttori tranne l' i -esimo”. In questo modo, ogni lampadina viene azionata (accesa/spenta) $n - 1$ volte (un numero dispari) e quindi, siccome all'inizio era spenta, alla fine è accesa.

(ii) Supponiamo ora che n sia dispari ma che, per assurdo, esista una soluzione. Sia k_i il numero di volte in cui l'interruttore i viene premuto nella soluzione. Siccome alla fine la lampadina i è accesa, k_i deve essere dispari. Chiamiamo $K = \sum_{i=1}^n k_i$. Siccome K è la somma di un numero dispari di termini dispari, K è dispari. Ma K è anche il numero complessivo di interruttori premuti, e ad ogni iterazione vengono premuti $n - 1$ interruttori. Quindi, K è un multiplo di $n - 1$. Ma $n - 1$ è un numero pari e K deve essere pari, da cui l'assurdo.

Esempio (4). Ordinamento a blocchi. Consideriamo il seguente puzzle: è data una permutazione di n elementi, che vogliamo ordinare tramite una sequenza di mosse. Ad ogni mossa, possiamo prendere un blocco consecutivo di 3 elementi ed invertirne l'ordine. Ad esempio, possiamo passare da $(2, \mathbf{1}, \mathbf{3}, \mathbf{5}, 4, 6, 7)$

a $(2, \mathbf{5}, \mathbf{3}, 1, 4, 6, 7)$. Immaginiamo che partendo dalla permutazione ordinata, qualcuno abbia effettuato un gran numero di mosse e ci abbia poi presentato la permutazione mescolata risultante. Il gioco richiede ora di trovare una sequenza di mosse (tanto più corta, tanto meglio) che riporti la permutazione mescolata nella permutazione originale. Ad esempio, se ci viene presentata la permutazione $(3, 4, 1, 2, 7, 8, 5, 6)$, possiamo ordinarla in 4 mosse come segue:

$$(3, 4, 1, 2, 7, \mathbf{8}, \mathbf{5}, \mathbf{6}) \mapsto (3, 4, 1, 2, \mathbf{7}, \mathbf{6}, \mathbf{5}, \mathbf{8}) \mapsto (\mathbf{3}, \mathbf{4}, 1, 2, 5, 6, 7, 8) \mapsto (1, \mathbf{4}, \mathbf{3}, \mathbf{2}, 5, 6, 7, 8) \mapsto (1, 2, 3, 4, 5, 6, 7, 8)$$

Supponiamo ora che il nostro avversario ci presenti la permutazione $(1, 4, 6, 2, 5, 7, 3, 8)$ e ci sfidi a risolverla. Possiamo dimostrare che è impossibile ordinarla, e che quindi l'avversario ci sta imborogliando. La dimostrazione è la seguente. Ogni mossa coinvolge tre elementi consecutivi, dei quali quello in posizione centrale sta fermo, mentre gli altri due si scambiano di posto. In particolare, ogni elemento che si muove, lo fa di due caselle, e quindi passa da una posizione (di indice) pari ad una pari, o da una dispari ad una dispari. Quindi, se la permutazione mescolata è stata ottenuta dalla permutazione identica, i numeri dispari devono sempre e comunque occupare posizioni di indice dispari, e quelli pari posizioni di indice pari. Ora, nella nostra permutazione il numero 6 si trova in posizione 3 (oppure il 7 in posizione 6), e quindi non è possibile riordinare questa permutazione con mosse legali.

2.2.1 Il segno delle permutazioni.

Sia \mathcal{S}_n l'insieme di tutte le permutazioni dei numeri $\{1, 2, \dots, n\}$. Data una permutazione $\pi = (\pi_1, \dots, \pi_n) \in \mathcal{S}_n$, una *trasposizione* τ_{ab} , con $a, b \in \{1, 2, \dots, n\}$ e $a \neq b$ è una funzione che trasforma π in una nuova permutazione, identica a π eccezion fatta per gli elementi π_a e π_b che vengono scambiati fra loro. In particolare, supponendo $a < b$,

$$\tau_{ab}(\pi) = (\pi_1, \dots, \pi_{a-1}, \pi_b, \pi_{a+1}, \dots, \pi_{b-1}, \pi_a, \pi_{b+1}, \dots, \pi_n).$$

Ogni permutazione $\sigma \in \mathcal{S}_n$ può essere ottenuta (in più modi) da π con una sequenza di trasposizioni. Infatti, con una trasposizione, possiamo far sì che π_1 diventi uguale a σ_1 . Con un'ulteriore trasposizione portiamo σ_2 in posizione 2, e così via, finché π coincide con σ . Ad esempio, se $\pi = (2, 1, 3, 6, 5, 4)$ e $\sigma = (3, 1, 4, 5, 6, 2)$ possiamo trasformare π in σ con 3 trasposizioni come segue:

$$(\mathbf{2}, 1, \mathbf{3}, 6, 5, 4) \mapsto (3, 1, \mathbf{2}, 6, 5, \mathbf{4}) \mapsto (3, 1, 4, \mathbf{6}, \mathbf{5}, 2) \mapsto (3, 1, 4, 5, 6, 2)$$

Facciamo ora vedere che se σ può essere ottenuta da π con k trasposizioni, allora ogni modo di ottenere σ da π richiede un numero di trasposizioni che ha la stessa parità di k . Senza perdita di generalità (eventualmente rinominando gli elementi delle due permutazioni) possiamo sempre assumere che σ sia la permutazione identica. Abbiamo il seguente teorema.

TEOREMA 20: Data una permutazione π , o tutti i modi di trasformare π nella permutazione identica richiedono un numero pari di trasposizioni, o richiedono tutti un numero dispari di trasposizioni.

Dim: Consideriamo in π tutte le coppie $\{\pi_i, \pi_j\}$ tali che $i < j$ ma $\pi_i > \pi_j$. Si tratta di coppie di elementi che compaiono in un ordine diverso nella permutazione di partenza e in quella di arrivo. Chiamiamo ogni

coppia di questo tipo un'*inversione*, e diciamo che π_i fa *inversione* con π_j . Supponiamo che vengano trasposti due qualsiasi elementi π_a e π_b . Ogni elemento in posizione k con $a < k < b$:

- se non faceva inversione con nessuno dei due ora la fa con tutti e due.
- se faceva inversione solo con uno dei due, allora adesso la fa solo con l'altro.
- se faceva inversione con entrambi, ora non la fa con nessuno dei due.

Quindi, relativamente agli elementi tra a e b , il numero complessivo di inversioni mantiene la stessa parità. Similmente, gli elementi in posizione $k < a$ o $k > b$ non possono dare luogo a nuove inversioni in quanto rimangono nello stesso ordine relativamente a π_a e π_b . Infine, la coppia $\{\pi_a, \pi_b\}$ se era un'inversione ora non lo è più, mentre se non lo era ora lo diventa. In conclusione, il numero totale di inversioni cambia di parità. Questo implica che se la permutazione di partenza aveva un numero dispari di inversioni, sarà necessario un numero dispari di trasposizioni per eliminarle tutte, mentre se le inversioni erano in numero pari, servirà un numero pari di trasposizioni. ♣

In base a quanto appena osservato, le permutazioni si ripartiscono in due classi, chiamate rispettivamente permutazioni pari e permutazioni dispari. Le permutazioni pari sono tutte quelle ottenibili con un numero pari di trasposizioni a partire dalla permutazione identica mentre le restanti permutazioni sono dispari. Essendoci una corrispondenza biunivoca tra le due classi, esistono $n!/2$ permutazioni pari ed altrettante permutazioni dispari. Per convenzione, le permutazioni pari sono dette di segno $+1$, mentre quelle dispari di segno -1 .

Esempio (5). Il gioco del 15. In un popolare gioco di ingegno, all'interno di una piccola cornice di plastica quadrata di lato 4, si trovano 15 tasselli quadrati di lato 1, numerati da 1 a 15, ed una posizione libera (detta il "buco"). Ogni tassello adiacente al buco può essere fatto slittare nel buco stesso. Questa mossa ha l'effetto di muovere il tassello, ma, alternativamente, può essere vista come una mossa che muove il buco. Il buco può perciò muoversi al massimo in 4 posizioni rispetto alla posizione corrente, ossia in alto, in basso, a sinistra o a destra. Ad esempio, spostando il buco in alto possiamo effettuare la seguente mossa

1	2	3	4
5		6	8
9	10	7	11
13	14	15	12

 \mapsto

1		3	4
5	2	6	8
9	10	7	11
13	14	15	12

Nel gioco del 15 si parte da una configurazione arbitraria, ottenuta dalla configurazione ordinata applicando un buon numero di mosse casuali. La configurazione ordinata è quella in cui la casella in alto a sinistra è 1, i valori crescono spostandosi da sinistra a destra e da una riga alla successiva, e la casella in basso a destra è il buco. L'obiettivo è quello di riportare tutti i tasselli nella configurazione ordinata tramite una sequenza di mosse (più breve possibile). Supponiamo ora che ci venga presentata la configurazione

	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

e che ci venga chiesto di risolverla. Possiamo provare fin che vogliamo ma non potremo mai riportare i tasselli nella configurazione ordinata. Per convincerci di ciò consideriamo la permutazione di 16 elementi ottenuta leggendo una configurazione riga per riga, dall'alto in basso, e chiamando "16" il buco. Ogni mossa del buco corrisponde a una trasposizione. Ad esempio, data la configurazione

5	1	12	3
4	15	6	2
8	9		11
7	13	14	10

equivalente alla permutazione

$$(5, 1, 12, 3, 4, 15, 6, 2, 8, 9, \mathbf{16}, 11, 7, 13, 14, 10)$$

ogni mossa del buco è una trasposizione:

- Mossa a sinistra: $(5, 1, 12, 3, 4, 15, 6, 2, 8, \mathbf{16}, 9, 11, 7, 13, 14, 10)$
- Mossa a destra: $(5, 1, 12, 3, 4, 15, 6, 2, 8, 9, 11, \mathbf{16}, 7, 13, 14, 10)$
- Mossa in alto: $(5, 1, 12, 3, 4, 15, \mathbf{16}, 2, 8, 9, 6, 11, 7, 13, 14, 10)$
- Mossa in basso: $(5, 1, 12, 3, 4, 15, 6, 2, 8, 9, 14, 11, 7, 13, \mathbf{16}, 10)$

In particolare, quindi, ad ogni mossa *la parità della permutazione corrente cambia*. Nel nostro specifico esempio, la permutazione di arrivo è pari (0 inversioni), mentre quella di partenza è dispari (ci sono esattamente 15 inversioni). Se coloriamo le 16 posizioni dei tasselli di bianco e nero, come le caselle di una scacchiera, notiamo che il buco deve passare dall'angolo alto a sinistra a quello basso a destra, che hanno lo stesso colore, e quindi deve essere mosso un numero pari di volte. Questo implica che la parità della permutazione di partenza sarà la stessa di quella di arrivo. Siccome la permutazione di partenza è dispari e quella di arrivo è pari, il problema non ammette soluzione. Chiaramente, la configurazione di partenza non era stata ottenuta dalla configurazione ordinata tramite mosse legali.

ESERCIZIO 2.11. Un mucchio contiene $n = 416$ sassolini. Due giocatori, che chiameremo A e B , si sfidano al seguente gioco. Ad ogni turno, il giocatore a cui tocca può rimuovere da un minimo di 1 a un massimo di 4 sassolini, a suo piacimento. Comincia A , e il giocatore che rimuove l'ultimo sassolino perde. Supponendo che ciascuno giochi con una strategia ottimale, chi vince tra A e B e perchè? Come cambia il problema se $n = 1013$? Qual'è in questo caso la mossa iniziale migliore per A ? \diamond

Chapter 3

Piccioni e buche

In questo capitolo studiamo un principio elementare ma molto importante, il *principio della piccionaia*. In pratica, il principio dice che, se molti piccioni volano in una piccionaia con poche buche, in almeno una buca finiranno due o più piccioni.

3.1 Il principio della piccionaia, forma semplice

La forma più semplice del principio è la seguente:

TEOREMA 21: Se $n + 1$ oggetti vengono posti in n contenitori, allora almeno un contenitore conterrà due o più oggetti.

Dim: Per assurdo, se ogni contenitore contenesse al più un oggetto, si avrebbe che il numero totale di oggetti sarebbe al più n . Ma noi abbiamo supposto che tale numero sia $n + 1$. ♣

ESERCIZIO 3.1. Si dimostri il principio della piccionaia per induzione. ◇

Si noti che nè il teorema nè la sua dimostrazione danno indicazioni su quale contenitore abbia più di un oggetto. L'unica cosa che possiamo affermare con certezza è l'esistenza di un tale contenitore. Si noti inoltre che il principio vale solo se si hanno almeno $n + 1$ oggetti. Infatti, si possono mettere n oggetti in n contenitori senza che due oggetti vadano nello stesso contenitore.

Esempio. In un gruppo di 367 persone ce ne sono almeno due con lo stesso compleanno. ◇

Esempio. Una persona possiede n paia di identici guanti di lana, ogni paio di un colore diverso. Quanti guanti deve prendere come minimo, al buio, per essere sicuro di aver selezionato almeno un paio di guanti dello stesso colore?

Prendendo n guanti, non può avere la certezza di un paio completo (potrebbero essere tutti di colore diverso). Con $n + 1$ guanti, ce ne devono essere due dello stesso colore.

Si supponga ora che tutte le paia di guanti abbiano lo stesso colore, ma il guanto destro e il sinistro siano distinguibili. Quanti guanti vanno presi, nel caso peggiore, per essere sicuri di selezionare un paio sinistro/destro con cui poter uscire? \diamond

Dal principio della piccionaia seguono due altri semplici principii:

1. Se n oggetti vengono posti in n scatole, e nessuna scatola è vuota, allora ogni scatola contiene esattamente un oggetto.
2. Se n oggetti vengono posti in n scatole, e nessuna scatola contiene più di un oggetto, allora ogni scatola contiene esattamente un oggetto.

Per esercizio li si dimostri.

Esempio. Un campione di tennis ha 9 settimane per prepararsi a un grande torneo. Decide allora di giocare almeno una partita di allenamento al giorno, ma, per non stancarsi troppo, non più di 10 partite alla settimana. Si dimostri che esiste una successione di giorni durante i quali il campione gioca esattamente 35 partite.

Sia p_1 il numero di partite giocate fino al primo giorno, p_2 il numero di partite giocate fino al secondo (ossia giocate il primo e il secondo giorno) e così via fino a p_{63} . Si ha $p_1 < p_2 < \dots < p_{63}$. Inoltre, siccome in ogni settimana non gioca più di 10 partite, $p_{63} \leq 9 \times 10 = 90$. Quindi

$$1 \leq p_1 < p_2 < \dots < p_{63} \leq 90.$$

Sommando 35 a ogni numero p_1, \dots, p_{63} abbiamo ancora una sequenza crescente:

$$36 \leq p_1 + 35 < p_2 + 35 < \dots < p_{63} + 35 \leq 125.$$

Quindi, ciascuno dei 126 numeri

$$p_1, p_2, \dots, p_{63}, p_1 + 35, p_2 + 35, \dots, p_{63} + 35$$

è un numero compreso tra 1 e 125. Ne consegue che almeno due numeri sono uguali. Questi non possono essere del tipo p_i, p_j nè del tipo $p_i + 35, p_j + 35$, quindi esistono i e j tali che $p_i = p_j + 35$. Ne consegue che nei giorni $j + 1, j + 2, \dots, i$ il tennista ha giocato esattamente 35 partite. \diamond

Esempio. Si scelgano 101 interi compresi tra 1 e 200. Si dimostri che tra gli interi scelti ce ne sono almeno due tali che uno di essi è divisibile per l'altro.

Nella fattorizzazione di ogni intero possiamo raggruppare tutti i fattori 2, in modo che l'intero risulti una potenza di 2 per un numero dispari, ossia del tipo $2^k \times d$ con d dispari. Siccome i nostri numeri sono compresi tra 1 e 200, d deve essere uno tra 1, 3, 5, \dots , 199. Ci sono 100 tali numeri dispari e abbiamo preso 101 interi, per cui (almeno) due di questi hanno lo stesso d , ossia sono del tipo $a = 2^n \times d$ e $b = 2^m \times d$. Per

cui, se $a \leq b$, a divide b , altrimenti b divide a . \diamond

ESERCIZIO 3.2. (difficile) Dimostrare che, scelti 100 numeri compresi tra 1 e 200, di cui almeno uno sia < 16 , allora fra i numeri scelti ci sono due numeri tali che l'uno divide l'altro. \diamond

Esempio. Dimostrare che, dati 52 interi qualsiasi, ce ne sono sempre almeno due la cui differenza è un multiplo di 100 o due la cui somma è un multiplo di 100.

Innanzitutto notiamo come sostituendo 52 con 51 l'affermazione risulti falsa. Infatti, se prendiamo gli interi $\{0, 1, 2, \dots, 50\}$ allora la differenza di qualsiasi due numeri è compresa tra -50 e 50 ma mai nulla, mentre la somma è compresa tra 1 e 99. Sia allora l'insieme dei nostri numeri $A = \{a_1, a_2, \dots, a_{52}\}$ e consideriamo l'insieme $B = \{b_1, b_2, \dots, b_{52}\}$ dove $b_i = (a_i \bmod 100)$ per ogni i . Se avviene che per due indici diversi i e j si ha $b_i = b_j$, allora $a_i \equiv a_j \pmod{100}$ e quindi $a_i - a_j$ è multiplo di 100. In caso contrario, consideriamo le 49 coppie di valori $\{1, 99\}, \{2, 98\}, \dots, \{49, 51\}$. L'insieme $B - \{0, 50\}$ ha almeno 50 elementi. Ogni elemento b_i appartiene ad esattamente una delle coppie. Per il principio della piccionaia, esistono due b che appartengono alla stessa coppia, siano essi b_i e b_j . Quindi $b_i + b_j = 100 \equiv 0 \pmod{100}$ e perciò $a_i + a_j \equiv 0 \pmod{100}$. \diamond

ESERCIZIO 3.3. Dimostrare che, presi 5 punti qualsiasi all'interno di: (i) un quadrato di lato 2, ce ne sono due la cui distanza è al massimo $\sqrt{2}$; (ii) un triangolo equilatero di lato 1, ce ne sono due la cui distanza è al massimo $\frac{1}{2}$. \diamond

3.2 Il principio della piccionaia, forma forte

Il seguente teorema generalizza il Teorema 21:

TEOREMA 22: Siano r_1, r_2, \dots, r_n interi positivi. Se $r_1 + r_2 + \dots + r_n - n + 1$ oggetti vengono posti in n scatole, allora, o la prima scatola contiene almeno r_1 oggetti, o la seconda ne contiene almeno r_2, \dots , o la n -sima ne contiene almeno r_n .

Dim: Per assurdo. Supponiamo che per ogni $1 \leq i \leq n$ la scatola i contenga meno di r_i oggetti. In particolare, ne contiene al massimo $r_i - 1$. Allora, il numero totale di oggetti sarebbe al massimo $(r_1 - 1) + (r_2 - 1) + \dots + (r_n - 1)$, ossia, al massimo $r_1 + r_2 + \dots + r_n - n$. Ma noi abbiamo supposto che gli oggetti fossero $r_1 + r_2 + \dots + r_n - n + 1$. \clubsuit

Si noti che sarebbe possibile distribuire $r_1 + r_2 + \dots + r_n - n$ oggetti in n contenitori senza mettere r_i (o più) oggetti nel contenitore i -mo (mettendone $r_1 - 1$ nel primo, $r_2 - 1$ nel secondo, ecc.).

Questo teorema generalizza il precedente, in quanto, se $r_1 = r_2 = \dots = r_n = 2$ si ottiene esattamente il Teorema 21.

Come importanti conseguenze del Teorema 22 studiamo il caso in cui $r_1 = r_2 = \dots = r_n = q$. In questo caso si ha

- Se $n(q-1)+1$ oggetti sono messi in n scatole, allora almeno una delle scatole contiene q o più oggetti, o, allo stesso modo
- Se la media di n interi non-negativi a_1, a_2, \dots, a_n è maggiore di $q-1$

$$\frac{a_1 + a_2 + \dots + a_n}{n} > q - 1$$

allora almeno uno dei numeri a_1, \dots, a_n è maggiore o uguale a q .

Quest'ultimo risultato è particolarmente importante e va ricordato, per cui lo ripetiamo, anche se cambiandolo un po':

Il massimo di n numeri naturali non può essere più piccolo della loro media

Chiaramente, se prendiamo n numeri tutti più piccoli di q , anche la media sarà più piccola di q . Per cui, se si sa che la media è almeno pari a q , anche uno dei numeri deve essere almeno pari a q . In particolare, siccome la media è almeno pari alla media (in effetti, è proprio pari alla media!), almeno uno dei numeri (e tanto più il massimo) deve valere almeno quanto la media.

ESERCIZIO 3.4. Avendo a disposizione solo rose, margherite e tulipani, si vuole comporre un mazzo di fiori che abbia almeno 10 rose, o almeno 5 margherite, o almeno 8 tulipani. Supponendo di creare il mazzo scegliendo a caso il fiore da aggiungere di volta in volta, quanti fiori saranno necessari, al massimo, per ottenere un mazzo con le caratteristiche desiderate? \diamond

ESERCIZIO 3.5. John, Mary e Paul sono tre attori che appaiono in esattamente 10 film. Nessuno di loro ha però girato tutti i film. In particolare, John è presente in 8 dei 10 film, mentre Mary e Paul in 7. In quanti dei 10 film, come minimo, appaiono tutti e 3 gli attori insieme? In quanti come massimo? \diamond

Esempio. Un bambino ha 3 album nuovi di figurine, uno da 100 uno da 80 e uno da 60 figurine. In strada trova un venditore che vende bustine di figurine dei 3 album. Ogni bustina contiene 2 figurine, non necessariamente dello stesso album. Nessuna bustina contiene due figurine uguali nè una medesima figurina può trovarsi in due bustine diverse. Quante bustine deve acquistare come minimo il bambino per essere sicuro di completare almeno un album?

Ci sono 3 scatole (i 3 album). Per essere sicuro di completare uno dei tre album, il bambino ha bisogno di $(100-1) + (80-1) + (60-1) + 1 = 238$ figurine. Siccome le figurine vengono in pacchetti da 2, dovrà acquistarne come minimo 119 pacchetti. \diamond

ESERCIZIO 3.6. Dimostrare che, presi comunque 7 interi, ce ne sono sempre almeno due la cui somma o la cui differenza è un multiplo di 10. \diamond

Esempio. Supponiamo di avere due dischi concentrici, entrambi divisi in 200 settori uguali fra loro. Nel disco esterno, si dipingano arbitrariamente 100 settori rossi e gli altri 100 blu. Nel disco interno, si dipingano a piacere i settori con i colori rosso e blu, ma senza alcun vincolo (ossia non devono necessariamente esserci 100 settori rossi e 100 blu). Si dimostri che è possibile ruotare il disco interno in modo che ci siano almeno 100 settori sul disco interno che vengono a combaciare con settori dello stesso colore sul disco esterno.

Cominciamo con l'osservare che, tenendo fermo il disco esterno, ci sono 200 possibili rotazioni del disco interno rispetto al disco esterno (una per ogni possibile settore j del disco interno, che viene allineato al settore 1 del disco esterno). Contiamo tutte le volte che due settori dello stesso colore vengono allineati, su tutte le 200 possibili rotazioni. Siccome il disco esterno ha 100 settori di ognuno dei due colori, ogni settore del disco interno sarà (al girare del disco interno) allineato con esattamente 100 settori del disco esterno dello suo colore. Per cui, il numero totale di volte che due settori dello stesso colore sono allineati sarà di 200 (numero dei settori interni) volte 100 (numero di volte che ogni settore si allinea a un settore dello stesso colore), pari a 20000. Quindi, il numero medio di coppie di settori dello stesso colore per ogni possibile rotazione è $20000/200 = 100$. Per cui c'è almeno una rotazione che porta ad avere questo numero medio o più, ossia almeno 100 settori che combaciano con settori dello stesso colore. \diamond

Il metodo probabilistico. Quest'ultimo esempio è particolarmente importante, e merita una riflessione. Infatti, il ragionamento può essere interpretato come un esempio del *metodo probabilistico*, i.e., una tecnica utilizzata per dimostrare l'esistenza di un oggetto dalle caratteristiche desiderate facendo uso di un argomento probabilistico. Fondamentalmente, l'idea è quella di considerare uno spazio di probabilità il cui universo (i.e., l'insieme degli eventi elementari) sia un sovrainsieme dell'insieme (sia esso A) di oggetti di cui vogliamo dimostrare l'esistenza. Per dimostrare che $A \neq \emptyset$, si può allora cercare di dimostrare che $\Pr(A) > 0$. Un modo di fare ciò è quello di considerare il valor medio di un'opportuna variabile casuale che assuma valore zero sugli oggetti che non appartengono ad A . Se il valore medio della variabile risulta non-nullo, allora almeno uno degli oggetti in A deve aver probabilità non nulla di realizzazione.

Nel nostro esempio, introduciamo un'interpretazione probabilistica supponendo che il cerchio interno possa ruotare su un perno (come il tamburo di una roulette) relativamente a quello esterno, che invece rimane fisso. Imprimendo una forza sul cerchio interno, lo stesso ruota, in maniera casuale, fino a fermarsi in una delle 200 posizioni possibili. A questa posizione associamo la variabile casuale Z pari al numero di settori allineati a settori del medesimo colore. In base al ragionamento esposto al punto precedente, sappiamo che $E[Z] = 100$. Definiamo inoltre due variabili casuali X e Y al seguente modo:

$$X = \begin{cases} 0 & \text{se } Z < 100 \\ Z & \text{altrimenti.} \end{cases}$$

$$Y = \begin{cases} Z & \text{se } Z < 100 \\ 0 & \text{altrimenti.} \end{cases}$$

(si noti che X vale 0 su tutte le rotazioni che non soddisfano al requisito richiesto dal problema). Chiaramente, $Z = X + Y$ e quindi $E[Z] = E[X] + E[Y]$. Inoltre, $E[Y] < 100$, in quanto la variabile Y non può mai assumere un valore superiore a 99. Ne segue che $E[X] \geq 1$ e quindi esiste almeno un caso per il quale $X > 0$.

ESERCIZIO 3.7. Dimostrare che, in qualsiasi modo si dispongano i numeri $1, 2, \dots, 10$ intorno a un cerchio, ci saranno sempre almeno tre numeri consecutivi la cui somma è almeno 17. \diamond

ESERCIZIO 3.8. Ad una festa si presentano 100 persone. Ogni persona è amica di un numero pari di altre persone (al limite 0). Dimostrare che ci sono almeno 3 persone con lo stesso numero di amici. \diamond

ESERCIZIO 3.9. Dimostrare che:

1. comunque si prendano $n + 1$ numeri nell'insieme $\{1, 2, \dots, 2n\}$, ce ne sono sempre almeno due la cui differenza è pari a 1.
2. comunque si prendano $n + 1$ numeri nell'insieme $\{1, 2, \dots, 3n\}$, ce ne sono sempre almeno due la cui differenza è ≤ 2 .

◇

ESERCIZIO 3.10. Si consideri una famiglia F di sottoinsiemi di $\{1, 2, \dots, n\}$ tale che ogni due elementi di F hanno intersezione non vuota. Quanto vale, al massimo, $|F|$? ◇

Chapter 4

Contiamo!

4.1 Principii fondamentali: somma e prodotto

In questa sezione studiamo i seguenti problemi:

- (a) Ci sono elementi di k tipi diversi, dei quali n_1 del primo tipo, n_2 del secondo tipo, ..., n_k dell'ultimo tipo. In quanti modi si può scegliere un elemento del primo tipo o del secondo tipo, ..., o dell'ultimo tipo?
- (b) Come prima, ci sono elementi di k tipi diversi, dei quali n_1 del primo tipo, n_2 del secondo tipo, ..., n_k dell'ultimo tipo. In quanti modi si può scegliere un elemento del primo tipo e uno del secondo tipo, ... e uno dell'ultimo tipo?

4.1.1 Il principio della somma

Dato un insieme S , una partizione di S è una collezione S_1, \dots, S_k di sottoinsiemi di S tali che

$$S = S_1 \cup S_2 \cup \dots S_k$$

e

$$S_i \cap S_j = \emptyset \quad (\text{per ogni } i \neq j)$$

Data una tale partizione, il *principio della somma* afferma che:

$$|S| = |S_1| + |S_2| + \dots + |S_n|. \quad (4.1)$$

Esempio. Per contare il numero di iscritti all'università di Udine, si possono sommare gli iscritti di Ingegneria agli iscritti di Scienze, a quelli di Lingue, ecc (tutte le facoltà). Oppure, si possono sommare gli iscritti provenienti da Udine, a quelli provenienti da Gorizia, da Trieste, da Padova, da ... (tutte le possibili provenienze) \diamond

Esempio. Per un ruolo di comparsa si presentano 3 giovani uomini, 2 giovani donne, e 5 anziani. In quanti modi può essere scelta la comparsa? In $3+2+5 = 10$ modi. \diamond

Alle volte, per contare la cardinalità di S può convenire non tanto partizionare S in sottoinsiemi, ma considerare un sovrainsieme A di S e il complementare C di S rispetto ad A , a patto che le cardinalità di A e di C siano facili da calcolare. In tal caso infatti, il principio della somma applicato ad A da'

$$|A| = |S| + |C| \quad (4.2)$$

da cui

$$|S| = |A| - |C|. \quad (4.3)$$

Esempio. Quanti sono i numeri di due cifre che non contengono la cifra 0 e che hanno cifre diverse fra loro? Possiamo considerare come sovrainsieme l'insieme A di tutti i numeri di due cifre. $|A| = 100$. Il complementare C di S in questo esempio è dato dall'insieme dei numeri che hanno almeno una cifra 0, o hanno entrambe le cifre uguali. Ripartiamo C come C_1 (l'insieme dei numeri che hanno la prima cifra uguale a 0), C_2 (l'insieme dei numeri che hanno la seconda, ma non la prima, cifra uguale a 0) e C_3 (l'insieme dei numeri che hanno entrambe le cifre uguali, ma diverse da 0). Abbiamo $C_1 = \{00, 01, \dots, 09\}$, e quindi $|C_1| = 10$; $C_2 = \{10, 20, \dots, 90\}$, e quindi $|C_2| = 9$; $C_3 = \{11, 22, \dots, 99\}$, e quindi $|C_3| = 9$. Ne consegue $|S| = |A| - (|C_1| + |C_2| + |C_3|) = 100 - (10 + 9 + 9) = 72$. \diamond

4.1.2 I numeri di Fibonacci

Consideriamo il seguente problemino. Supponiamo che una coppia di conigli possa riprodursi a partire dall'età di 2 mesi. A partire da quell'età, la coppia si riproduce ogni mese, dando luogo a una nuova coppia di conigli. Supponendo di partire con una coppia appena nata, e che i conigli vivano in eterno (bella vita la loro!) ci si chiede quante coppie si avranno dopo n mesi. Chiamiamo F_n questo numero.

Per il principio della somma, le coppie di conigli vive dopo n mesi si possono partizionare come coppie che erano già vive e coppie appena nate. Le coppie di conigli già vivi sono in numero F_{n-1} , mentre le coppie appena nate sono tante quante le coppie che erano vive due mesi prima (ricordiamo che, dall'età di due mesi in poi ogni coppia si riproduce mensilmente) e quindi sono F_{n-2} .

La legge generale risulta perciò, per $n \geq 2$

$$F_n = F_{n-1} + F_{n-2}$$

mentre i casi iniziali sono $F_0 = 1$ e $F_1 = 1$. I primi valori di questa successione sono

$$1, 1, 2, 3, 5, 8, 13, 21, \dots \quad (4.4)$$

La successione (4.4) è nota come successione dei *numeri di Fibonacci* in onore del loro scopritore, il matematico pisano Leonardo Fibonacci, vissuto nel 1200 circa. È una successione molto importante, in

quanto i numeri di Fibonacci si ritrovano in innumerevoli situazioni, ed esistono anche pubblicazioni scientifiche periodiche dedicate alle loro applicazioni. Vediamo ora alcuni semplici esempi in cui compaiono i numeri di Fibonacci.

Esempio. Si supponga di voler parcheggiare delle limousine e delle utilitarie sul lato di una strada rettilinea. Ogni limousine occupa 2 spazi di parcheggio, mentre un'utilitaria ne occupa uno solo. Ci chiediamo in quanti modi diversi si possono parcheggiare questi due tipi di macchina in modo da riempire tutti gli spazi a disposizione.

Chiamiamo M_n il numero di modi di riempire n spazi. Supponiamo gli spazi numerati da 1 a n . Possiamo distinguere due situazioni. O lo spazio 1 è occupato da un'utilitaria, e quindi restano gli altri $n - 1$ spazi da riempire (in M_{n-1} modi) o lo spazio 1 è occupato da una limousine. In questo caso, la limousine occupa anche lo spazio 2, e restano gli altri $n - 2$ spazi da riempire (in M_{n-2} modi). Si deduce $M_n = M_{n-1} + M_{n-2}$. Siccome $M_1 = 1$ e $M_2 = 2$, si ricava che la sequenza M_n è esattamente la sequenza dei numeri di Fibonacci di indice ≥ 1 . \diamond

Esempio. Si consideri una scacchiera $2 \times n$. Un pezzo del domino copre esattamente 2 caselle di tale scacchiera. Ci si chiede in quanti modi si possono disporre n pezzi del domino in modo da coprire tutte le caselle della scacchiera. Chiamiamo D_n il numero di tali modi.

Consideriamo la scacchiera come composta da 2 righe e n colonne, numerate da 1 a n . Possiamo distinguere due situazioni. O la colonna 1 è coperta da un domino posizionato verticalmente, e quindi restano le altre $n - 1$ colonne da coprire (in D_{n-1} modi) o la colonna 1 è coperta da due domino posizionati orizzontalmente. In questo caso, i due pezzi coprono anche la colonna 2, e restano le altre $n - 2$ colonne da coprire (in D_{n-2} modi). Si deduce $D_n = D_{n-1} + D_{n-2}$. Siccome $D_1 = 1$ e $D_2 = 2$, si ricava che la sequenza D_n è esattamente la sequenza dei numeri di Fibonacci di indice ≥ 1 . \diamond

Per avere una semplice stima della crescita dei numeri di Fibonacci, possiamo procedere come segue. Sappiamo che $F_{n-2} < F_{n-1}$. Sommando F_{n-2} ad entrambi i membri si ottiene $2F_{n-2} < F_n$. Se invece sommiamo F_{n-1} ad entrambi i membri otteniamo $F_n < 2F_{n-1}$. Quindi, per $n \geq 2$,

$$2F_{n-2} < F_n < 2F_{n-1}.$$

Applicando la stessa relazione a F_{n-2} e F_{n-1} , si ottiene che

$$2 \times 2F_{n-4} < F_n < 2 \times 2F_{n-2}.$$

Proseguendo, si arriva a concludere che

$$2^{\lfloor \frac{n}{2} \rfloor} < F_n < 2^{n-1}$$

e da queste disuguaglianze si evince la crescita esponenziale della funzione F_n .

La formula (4.4) che definisce la successione dei numeri di Fibonacci è una formula ricorsiva. Esiste anche una formula chiusa (ossia una funzione di n) che permette di calcolare direttamente l' n -simo numero

di Fibonacci. Tale formula risulta un po' particolare, in quanto, pur contenendo il numero irrazionale $\sqrt{5}$, fornisce valori interi per ogni valore di n :

$$F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n \right). \quad (4.5)$$

Questa formula può essere dimostrata per induzione (si vedano gli esercizi), ma la dimostrazione non getta alcuna luce su come si sia potuta escogitare una formula di questo tipo. In effetti, la discussione su come si possa pervenire a congetturare una formula come questa per la generazione dei numeri di Fibonacci esula dagli argomenti trattati in questo testo ed è stata pertanto omessa.

Il valore $(1 + \sqrt{5})/2 \simeq 1.618$ è detto *sezione aurea* e si ritrova in molti fenomeni della natura e in costruzioni geometriche (ad esempio, le foglie in alcune piante nascono “a spirale” sul fusto, e sono spaziate l'una dall'altra da una frazione di giro pari alla sezione aurea. Come ulteriore esempio, la sezione aurea è pari al rapporto tra la diagonale e il lato di un pentagono regolare). Se consideriamo il rapporto tra due numeri di Fibonacci consecutivi, F_{n+1}/F_n si può dimostrare che tale valore tende a un limite ben preciso, e tale limite è la sezione aurea.

ESERCIZIO 4.1. Quanti numeri di Fibonacci compresi tra F_{300} e F_{400} sono dispari? ◇

ESERCIZIO 4.2. Dimostrare che, per ogni $n \geq 0$, si ha $\sum_{k=0}^n F_k = F_{n+2} - 1$. ◇

ESERCIZIO 4.3. Dimostrare la validità della formula (4.5) per induzione. ◇

ESERCIZIO 4.4. Si dimostri che, per ogni $n \geq 2$ si ha

- (i) $F_{n-1} \cdot F_{n+1} = F_n^2 + 1$, se n è pari
- (ii) $F_{n-1} \cdot F_{n+1} = F_n^2 - 1$, se n è dispari.

◇

ESERCIZIO 4.5. Si riconsideri l'algoritmo di Euclide per il MCD di due numeri descritto in sez. 2.1.1. Utilizzando tale algoritmo su due numeri di Fibonacci consecutivi, quante iterazioni risultano necessarie? ◇

4.1.3 Il principio del prodotto

Sia S l'insieme di tutte le coppie ordinate del tipo (a, b) , dove il primo elemento può essere scelto in p modi, e, per ogni scelta del primo, si può scegliere il secondo in q modi. Allora

$$|S| = p \times q. \quad (4.6)$$

Possiamo dimostrare questo principio tramite il principio della somma. Siano $\{a_1, \dots, a_p\}$ le p scelte possibili per a . Ripartiamo S in questo modo: tutte le coppie che cominciano per a_1 (ossia del tipo (a_1, b) , con q scelte per b), quelle che cominciano per a_2 (ossia del tipo (a_2, b)), ecc., fino a quelle che cominciano per a_p

(ossia del tipo (a_p, b)). Ognuno di questi sottoinsiemi ha q elementi e ci sono p sottoinsiemi, per cui $S = p \times q$.

Esempio. Riconsideriamo l'esempio precedente. Per creare un numero di 2 cifre, in cui nessuna cifra è 0, e le cifre sono diverse, possiamo scegliere la prima cifra in 9 modi (tutte tranne la 0) e la seconda in 8 modi (tutte tranne la 0 e la prima). Per cui, ci sono $9 \times 8 = 72$ possibilità. \diamond

Il principio precedente si estende immediatamente al caso più generale di più di due scelte in sequenza. Ad esempio, supponendo di dover scegliere una sequenza di n elementi (a_1, \dots, a_n) , in cui ci sono p_1 modi di scegliere a_1 , p_2 modi (indipendentemente da a_1) di scegliere a_2 , p_3 modi (indipendentemente da a_1 e a_2) di scegliere a_3 , ecc fino a a_n , il numero totale di possibili n -ple diverse è

$$p_1 \times p_2 \times \dots \times p_n. \quad (4.7)$$

Esempio. Riconsideriamo l'esempio delle comparse. Supponendo servano esattamente un giovane uomo, una giovane donna e un anziano, ci sono $2 \times 3 \times 5 = 30$ modi di scegliere queste tre comparse. \diamond

Esempio. Ad uno sportello di un ufficio pubblico, che dovrebbe aprire ma risulta ancora chiuso da un pezzo, vi sono n persone in coda. Nella lunga attesa, ognuno fa amicizia con le due persone a lui vicine, quella che lo precede e quella che lo segue (tranne il primo e l'ultimo della fila, che fanno amicizia con una persona sola). All'improvviso, viene comunicato che sarà aperto un'altro sportello al posto di quello previsto, e le persone si affrettano a cambiare sportello. Ne segue una ressa, e la coda che si forma al nuovo sportello è di fatto una permutazione casuale delle persone della vecchia coda. Anche lo sportello nuovo non apre, e ancora una volta si crea l'occasione per delle nuove amicizie. In particolare, fanno amicizia ora tutti quelli che prima non erano in posizioni consecutive nella coda ma adesso lo sono. Ci chiediamo quante sono, mediamente, le nuove amicizie che vengono a crearsi nella nuova coda, e quante sono, mediamente, le persone che si ritrovano vicine solo a persone che già conoscevano.

Sia $(1, 2, \dots, n)$ la permutazione corrispondente alla coda iniziale, e π la permutazione corrispondente alla coda nuova. Per $i = 1, \dots, n-1$, diciamo che in posizione i c'è un *breakpoint* se $|\pi_i - \pi_{i+1}| > 1$. In pratica un breakpoint corrisponde a una coppia di elementi che fanno amicizia in π e che non si conoscevano nella coda originale. Ad esempio, nella permutazione seguente i breakpoints sono evidenziati con delle frecce:

$$3 \uparrow 5 \quad 4 \uparrow 1 \uparrow 7 \quad 8 \quad 9 \uparrow 6 \uparrow 2 \uparrow 10 \quad 11$$

In questo esempio vi sono 6 breakpoints. Si noti che la permutazione ordinata $(1, \dots, n)$ non ha breakpoints, così come non ne ha la permutazione $(n, n-1, \dots, 2, 1)$. È facile convincersi che queste sono le uniche permutazioni senza breakpoints, ed ogni altra permutazione ha almeno un breakpoint.

Lemma 23: Si denoti con X il numero di breakpoints in una permutazione casuale di n elementi (i.e., presa con distribuzione uniforme fra le $n!$ possibili). Allora

$$E[X] = \frac{(n-1)(n-2)}{n}. \quad (4.8)$$

Dim: Per $i = 1, \dots, n-1$, sia Z_i una variabile casuale che vale 1 se si verifica l'evento "in posizione i c'è un breakpoint" e 0 altrimenti. Pertanto, $X = \sum_{i=1}^{n-1} Z_i$. Dalla linearità del valor medio, segue $E[X] = E[\sum_{i=1}^{n-1} Z_i] = \sum_{i=1}^{n-1} E[Z_i] = \sum_{i=1}^{n-1} \Pr(Z_i = 1)$.

Sia $i \in \{1, \dots, n-1\}$. Per il principio della somma, il numero di permutazioni che hanno un breakpoint in posizione i è ottenibile sommando (i) il numero di permutazioni per le quali $\pi_i \in \{2, \dots, n-1\}$ con (ii) il numero di permutazioni per le quali $\pi_i \in \{1, n\}$. Ogni permutazione di tipo (i) è ottenibile scegliendo il valore di π_i ($n-2$ possibilità), poi il valore di π_{i+1} ($n-3$ possibilità, in quanto deve essere diverso da $\pi_i \pm 1$ e da π_i), e infine il valore dei restanti $n-2$ elementi di π ($(n-2)!$ possibilità). Per il principio del prodotto, esistono quindi $(n-2)(n-3)(n-2)!$ permutazioni di tipo (i). Similmente, ogni permutazione di tipo (ii) è ottenibile scegliendo il valore di π_i (2 possibilità), poi il valore di π_{i+1} ($n-2$ possibilità, in quanto deve essere diverso da 2 (se $\pi_i = 1$), o da $n-1$ (se $\pi_i = n$), e da π_i), e infine il valore dei restanti $n-2$ elementi di π ($(n-2)!$ possibilità). Per il principio del prodotto, esistono quindi $2(n-2)(n-2)!$ permutazioni di tipo (ii). In conclusione, le permutazioni con un breakpoint in posizione i sono

$$\left((n-2)(n-3) + 2(n-2)\right)(n-2)! = (n-2)(n-1)!$$

da cui

$$E[Z_i] = \frac{(n-2)(n-1)!}{n!} = \frac{n-2}{n}.$$

Dalla linearità del valor medio si ottiene

$$E[X] = \sum_{i=1}^{n-1} \frac{n-2}{n} = \frac{(n-1)(n-2)}{n}. \quad (4.9)$$



Passiamo ora alla seconda parte della domanda, in cui ci chiediamo, fondamentalmente, quanti sono gli elementi di π che non hanno un breakpoint nè alla loro sinistra nè alla loro destra. Anche qui possiamo usare un approccio simile al precedente. Per ogni $i = 1, \dots, n$, sia Y_i una variabile casuale binaria tale che $Y_i = 1$ se l'elemento di valore i (si noti che i è il valore dell'elemento, non la sua posizione all'interno di π) ha gli stessi vicini sia in π che nella permutazione ordinata, mentre $Y_i = 0$ altrimenti. Sia $Y = \sum_{i=1}^n Y_i$, e quindi $E[Y] = \sum_{i=1}^n \Pr(Y_i = 1)$.

Per $i = 2, \dots, n-1$ consideriamo la tripla di valori $(i-1, i, i+1)$. Per costruire una permutazione che contiene tale tripla in posizioni consecutive (nell'ordine crescente o decrescente), possiamo scegliere l'ordine della stessa (in 2 modi), e poi costruire una permutazione in cui la tripla funge da "singolo elemento", da mescolarsi con gli altri $n-3$ valori (in tutto, $(n-2)!$ modi). Abbiamo quindi, per $i = 2, \dots, n-1$

$$E[Y_i] = \frac{2(n-2)!}{n!} = \frac{2}{n(n-1)}.$$

Per $i = 1$ consideriamo la coppia di valori $(1, 2)$. Perchè i abbia gli stessi vicini sia nella permutazione iniziale che in π bisogna che π inizi con la coppia $(1, 2)$ (vi sono $(n-2)!$ possibilità) o finisca con la coppia $(2, 1)$ (anche qui, $(n-2)!$ possibilità). Analoghe considerazioni valgono per il caso $i = n$. Otteniamo che, anche per $i \in \{1, n\}$,

$$E[Y_i] = \frac{2(n-2)!}{n!} = \frac{2}{n(n-1)}.$$

In conclusione

$$E[Y] = \sum_{i=1}^n \frac{2}{n(n-1)} = \frac{2}{n-1} \quad (4.10)$$

e quindi il numero di persone che rimane accanto agli stessi vicini tende velocemente a 0 al crescere di n . \diamond

ESERCIZIO 4.6. Supponiamo di avere 20 caramelle, tutte diverse fra loro, e 12 bambini. Si calcoli in quanti modi diversi si possono distribuire le caramelle tra i bambini (notare che non è richiesto che ogni bambino riceva almeno una caramella, possono andare anche tutte allo stesso bambino!). \diamond

ESERCIZIO 4.7. Ci sono ancora 12 bambini (quelli di prima). Supponiamo di avere 20 sacchetti, ognuno con molte (> 12) caramelle uguali fra loro. Ogni sacchetto ha caramelle di gusto diverso rispetto a quelle degli altri sacchetti. Si calcoli in quanti modi si possono dare caramelle ai bambini in maniera tale che ogni bambino non riceva due o più caramelle dello stesso gusto. \diamond

ESERCIZIO 4.8. Ci sono 11 bambini (quelli di prima, tranne uno che è a casa con il mal di pancia dovuto a troppe caramelle). Decidono di giocare a calcetto, 5 contro 5 e 1 in porta per tutti. Hanno a disposizione 5 magliette rosse e 5 bianche, numerate con numeri diversi (il numero indica il ruolo). In quanti modi possono formarsi le squadre (una rossa e una bianca)? \diamond

ESERCIZIO 4.9. Quante sono le possibili sequenze di DNA diverse di lunghezza n ?

ESERCIZIO 4.10. Una sequenza proteica è una sequenza di amino acidi. Esistono 20 amino acidi, numerati da 1 a 20. Quante sono le possibili sequenze proteiche di lunghezza n che cominciano con l'amino acido 10 e non contengono l'amino acido 10 in alcun'altra posizione?

ESERCIZIO 4.11. Ogni persona ha 23 coppie di cromosomi. Nel fare un figlio, ogni genitore contribuisce con un cromosoma di ogni sua coppia, ossia con 23 cromosomi singoli. La fusione di 23 cromosomi del padre con 23 cromosomi della madre forma di nuovo un individuo completo, ossia con 23 coppie. In quanti modi diversi può avvenire questa ricombinazione?

4.2 Combinazioni (sottoinsiemi)

Studiamo il problema di determinare il numero di sottoinsiemi di un insieme.

Siano n gli elementi di un insieme $A = \{a_1, \dots, a_n\}$. Un sottoinsieme si può creare rispondendo alle domande: contiene a_1 ? contiene a_2 ? ... contiene a_n ? Ogni domanda ha due possibili risposte. Ci sono in tutto

$$2 \cdot 2 \cdot 2 \cdots 2 \cdot 2 = 2^n \quad (4.11)$$

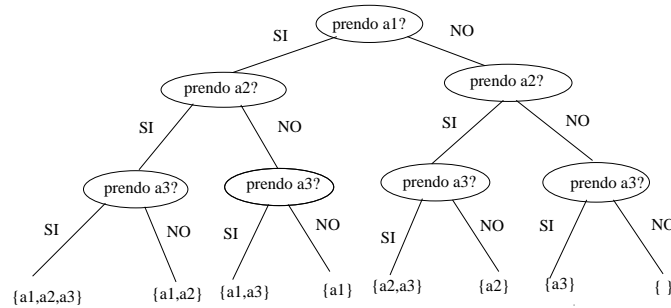


Figure 4.1: Albero binario di tutti i sottoinsiemi

possibili risposte, ossia 2^n possibili sottoinsiemi. Il sottoinsieme vuoto corrisponde a tutte risposte “no”, A stesso corrisponde a tutte risposte “sì”.

In Figura 4.1 è descritto un diagramma (detto *albero*) in cui si può vedere come, dopo k decisioni ci siano 2^k possibilità. In fondo al diagramma (nelle *foglie* dell'albero) si trovano tutti i possibili sottoinsiemi.

Un sottoinsieme ha cardinalità k solo se ci sono state k risposte “sì” e $n - k$ risposte “no”. Vediamo in quanti modi questo può avvenire. Per definizione il numero di modi di scegliere k oggetti da n (ad esempio, scegliere a quali delle n domande si è risposto “sì”), è detto n su k (scritto $\binom{n}{k}$) ed è detto anche *coefficiente binomiale*. Per vedere quanto vale $\binom{n}{k}$ si può ragionare così. Supponiamo di rendere diversi tra loro i k “sì” (ad esempio colorandoli rosso, blu, verde, ..., con k colori diversi). Allo stesso modo, si rendano diversi gli $n - k$ “no”. A questo punto, ci sono $n!$ modi diversi di rispondere alle n domande, in cui ci sono i k “sì” mescolati con gli $n - k$ “no”. Ora si fissi uno di questi modi (una tra le $n!$ permutazioni). Scambiando fra loro i vari “sì” in uno qualsiasi dei $k!$ modi, restano identificati gli stessi k elementi. E anche scambiando fra loro (permutando) gli $n - k$ “no”. Per cui, la stessa scelta di elementi è identificata da $k!(n - k)!$ permutazioni diverse (quelle in cui restano fisse le posizioni dei “sì” e dei “no”). Ne consegue che il numero di scelte di elementi è

$$\binom{n}{k} = \frac{n!}{k!(n - k)!} \quad (4.12)$$

Un modo pratico di ricordare la formula, è di disporre k numeri decrescenti, a partire da n , al numeratore, e a partire da k al denominatore, e calcolare la frazione. Ad es:

$$\binom{14}{5} = \frac{14 \cdot 13 \cdot 12 \cdot 11 \cdot 10}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 14 \cdot 13 \cdot 11 = 2002. \quad (4.13)$$

Esempio. Nel gioco del lotto, quante sono le possibili cinquine su una ruota fissa? Sono $\binom{90}{5} = 43'949'268. \diamond$

Vediamo ora alcune formule importanti sul coefficiente binomiale:

TEOREMA 24: Per il coefficiente binomiale si ha

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

Dim: Fissato un elemento, ci sono due possibilità per fare un sottoinsieme di k elementi: o l'elemento non è nel sottoinsieme (e quindi ci sono $\binom{n-1}{k}$ sottoinsiemi possibili di questo tipo), oppure è nel sottoinsieme (e quindi bisogna scegliere $k-1$ altri elementi fra i rimanenti $n-1$). ♣

ESERCIZIO 4.12. Dimostrare il teorema 24 algebricamente, a partire dalla formula per il coefficiente binomiale. ◇

Il ragionamento precedente può essere generalizzato in questo modo. Dovendo scegliere un sottoinsieme di dimensione k , si supponga di fissare p elementi, con $1 \leq p \leq k$. Allora, o l'insieme non contiene alcuno di questi p elementi, o ne contiene uno, o ne contiene due, ..., o li contiene tutti. In ognuna di queste situazioni, supponendo che il sottoinsieme ne contenga i tra i p fissati, i rimanenti $k-i$ vanno scelti dagli $n-p$ non fissati. Inoltre, gli i possono essere presi in $\binom{p}{i}$ modi. Ne consegue:

$$\binom{n}{k} = \sum_{i=0}^p \binom{p}{i} \binom{n-p}{k-i}. \quad (4.14)$$

TEOREMA 25: Per il coefficiente binomiale vale

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

Dim: Si può dimostrare dalla formula. Oppure, pensando al significato: scegliere i k elementi da tenere equivale a scegliere gli $n-k$ da scartare. ♣

Altre formule importanti:

$$\binom{n}{n} = \binom{n}{0} = 1$$

$$\binom{n}{1} = n$$

$$\binom{n}{2} = \frac{n(n-1)}{2} \text{ (il numero di coppie distinte di 2 elementi)}$$

$$\binom{n}{p} = 0, \text{ per } p > n$$

ESERCIZIO 4.13. Quanto vale $\sum_{i=0}^n \binom{n}{i}$? ◇

ESERCIZIO 4.14. In serie A ci sono 20 squadre. Ogni squadra ha una rosa di 2 portieri, 6 difensori, 5 centrocampisti e 5 attaccanti. Una squadra deve scendere in campo con 1 portiere, 4 difensori, 4 centrocampisti e

2 attaccanti. In quanti modi ogni allenatore può scegliere la formazione da mandare in campo? In quanti modi il selezionatore della nazionale può convocare un gruppo di 3 portieri, 7 difensori, 6 centrocampisti e 6 attaccanti attingendo da tutte le squadre? \diamond

ESERCIZIO 4.15. Tra i giochi presenti nel sistema operativo Windows ce n'è uno chiamato **Purple Place**. In questo gioco, bisogna indovinare i colori di 5 caratteristiche di un personaggio creato dal programma. Le caratteristiche sono, nell'ordine: berretto, occhi, naso, bocca e vestito. Esistono 5 colori possibili: rosa, viola, giallo, blu e verde. L'obiettivo è indovinare il colore di ciascuna caratteristica effettuando una serie di tentativi, e cercando di minimizzare il numero di tali tentativi. Ad ogni tentativo bisogna specificare i 5 colori (le ripetizioni di colori sono ammesse in due o più caratteristiche), e il programma risponde con 2 numeri (g, s) , dove g è il numero di ipotesi "esatte" (i.e., caratteristiche del colore giusto), e s è il numero di ipotesi "quasi" esatte (i.e., tra le caratteristiche non azzeccate, quanti sono i colori che appaiono nella soluzione, ma in caratteristiche diverse da quelle ipotizzate). Ad esempio, se la soluzione corretta fosse (viola, viola, giallo, verde, blu), il tentativo (viola, giallo, rosa, rosa, blu) avrebbe come risposta $(2, 1)$ (essendo esatte la prima e ultima caratteristica, e sbagliato, ma presente, il giallo), mentre il tentativo (giallo, viola, blu, blu, verde) darebbe per risultato $(1, 3)$ (giusto il secondo viola, e sbagliati giallo, blu e verde). Supponiamo ora di avere appena incominciato una partita e di aver effettuato il tentativo (rosa, viola, giallo, blu e verde) a cui il programma ha risposto $(2, 1)$. Quante sono, potenzialmente, le soluzioni corrette compatibili con la risposta $(2, 1)$ al nostro primo tentativo? \diamond

Esempio. Quanti sono i sistemi al totocalcio da 9 triple e 4 fisse? Ci sono 13 partite. Le triple possono essere scelte in $\binom{13}{9} = 715$ modi. Per ognuno di tali modi, si possono completare le rimanenti 4 parite in $3^4 = 729$ modi (ossia ogni fissa può essere scelta tra 1, 2 e X, e se ne devono scegliere 4). In totale abbiamo $715 \times 729 = 521235$ possibilità. \diamond

ESERCIZIO 4.16. Dati a, b e c tali che $a + b + c = 13$, quanti sono i sistemi da a fisse, b doppie e c triple? \diamond

ESERCIZIO 4.17. In un'aula ci sono due file ciascuna di 8 banchi. Ci sono 14 studenti, 5 dei quali si siedono sempre in prima fila e 4 dei quali sempre in ultima fila. In quanti modi si possono sedere tutti gli studenti? \diamond

Esempio. Dimostriamo che per ogni $n \in \mathbb{N}^+$ si ha

$$2^n < \binom{2n}{n} < 4^n. \quad (4.15)$$

Il valore $\binom{2n}{n}$ è pari al numero di sottoinsiemi di cardinalità n dell'insieme $A = \{1, \dots, 2n\}$. Supponiamo di raggruppare gli elementi di A a due a due

$$(1, 2), (3, 4), \dots, (2n-1, n)$$

e consideriamo il seguente modo di costruire un sottoinsieme di A di cardinalità n : per ognuna delle n coppie, prendiamo il primo elemento della coppia oppure il secondo, ma non entrambi. Questo modo di procedere dà luogo a 2^n possibili sottoinsiemi. Inoltre, alcuni sottoinsiemi di cardinalità n non possono essere prodotti da questa procedura (ad esempio, un sottoinsieme che non contenga nè 1 nè 2). Ne deduciamo che

$$2^n < \binom{2n}{n}.$$

Per quel che riguarda la seconda disuguaglianza in (4.15), si noti che $4^n = 2^{2n}$ è il numero di tutti i sottoinsiemi di A (compresi \emptyset e A stesso), e quindi

$$\binom{2n}{n} < 4^n.$$

◇

ESERCIZIO 4.18. Si dimostrino le disuguaglianze (4.15) per induzione.

◇

Esempio. Nel gioco del poker all'italiana (*5 cards draw*), qualora ci siano n giocatori, la carta più piccola utilizzata vale $11 - n$. Ad esempio, 4 giocatori utilizzano un mazzo che consiste delle seguenti carte: A, K, Q, J, 10, 9, 8, 7 (un totale di $4 \times 8 = 32$ carte). Ci chiediamo qual è la probabilità che 5 carte prese a caso da questo mazzo realizzino un full e qual è la probabilità che realizzino “colore”.

Un full è formato da un tris più una coppia. Il tris può essere scelto in $8 \times \binom{4}{3} = 32$ modi. Infatti, ci sono 8 possibilità di scegliere se il tris è d'assi, di re, ecc. e, una volta scelto questo, ci sono 4 carte di quel tipo (ad es. 4 assi) nel mazzo, da cui ne dobbiamo scegliere 3. La coppia può essere scelta in $7 \times \binom{4}{2} = 42$ modi. Infatti, il ragionamento è lo stesso di prima, ma, siccome la coppia deve essere diversa dal tris, si hanno solo 7 possibilità per scegliere il tipo di coppia. In totale abbiamo $32 \times 42 = 1344$ modi di formare un full con 5 carte.

Un colore è dato da 5 carte dello stesso seme. Il seme può essere scelto in 4 modi. Una volta scelto il seme, ci sono 8 carte di quel seme nel mazzo, da cui ne dobbiamo scegliere 5 (in $\binom{8}{5} = 56$ modi). Quindi, in totale ci sono $4 \times 56 = 224$ mani che realizzano il colore. In conclusione, se ci sono 4 giocatori, è 6 volte più probabile realizzare full che colore, e quindi il colore batte il full nella scala dei valori.

Diversa è la situazione qualora ci fossero più giocatori. Si consideri un caso limite di 9 giocatori. Il mazzo consiste delle seguenti carte: A, K, Q, J, 10, 9, 8, 7, 6, 5, 4, 3, 2 (un totale di $4 \times 13 = 52$ carte).

Un full può essere scelto in $13 \times \binom{4}{3} \times 12 \times \binom{4}{2} = 3744$ modi diversi. Un colore può essere scelto in $4 \times \binom{13}{5} = 5148$ modi. Per cui, in questo caso, un colore è più probabile di un full, per cui il full batte il colore nella scala dei valori.

◇

ESERCIZIO 4.19. Detto n il numero di giocatori, supponiamo che un mazzo di carte contenga solo le carte dalla $11 - n$ all'asso (es., se $n = 4$, dal 7 all'asso). Si determini il numero massimo di giocatori per il quale il full è più probabile del colore.

◇

4.2.1 Il triangolo di Pascal

Il *triangolo di Pascal* è ottenuto in questo modo: si creano delle righe (numerate da 0 in poi) e in ogni riga i ci sono $i + 1$ elementi (numerati da 0 a i). L'elemento k della riga n vale $\binom{n}{k}$. Disponendoli in triangolo si ottiene lo schema

$$\begin{array}{cccccccc}
& & & & 1 & & & \\
& & & & 1 & & 1 & \\
& & & 1 & 2 & & 1 & \\
& & 1 & 3 & 3 & & 1 & \\
& 1 & 4 & 6 & 4 & & 1 & \\
1 & 5 & 10 & 10 & 5 & & 1 &
\end{array}$$

Si noti che per via del teorema 24 un elemento è ottenuto dalla somma dei due elementi sopra a lui (a sinistra e a destra).

Supponiamo di volere calcolare lo sviluppo di $(a + b)^n$, i.e.,

$$\Pi = (a + b)(a + b) \cdots (a + b).$$

Lo sviluppo sarà del tipo $\sum c(i, j)a^i b^j$, dove la somma è estesa a tutte le coppie di i e j tali che $i + j = n$. Scegliendo a da i termini in Π e b dai rimanenti $n - i$ si ottiene un termine $a^i b^{n-i}$. Questo può essere fatto in $\binom{n}{i}$ modi (per cui $c(i, j) = \binom{n}{i} = \binom{n}{j}$ nell'espressione precedente). Si ottiene perciò

$$(a + b)^n = \sum_{i=0}^n \binom{n}{i} a^i b^{n-i} \quad (4.16)$$

Ad es. dalla riga 5 del triangolo di Pascal, si ottiene

$$(a + b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5 \quad (4.17)$$

Processi Bernoulliani.

Si consideri un esperimento che può terminare in due modi, denominati “successo” e “fallimento”. Denotiamo con p e con $q = 1 - p$ la probabilità di successo e di fallimento, rispettivamente. Ad esempio, se l'esperimento consiste nel lancio di una moneta e se definiamo l'uscita di testa come successo e quella di croce come fallimento, abbiamo $p = q = 1/2$. Se invece l'esperimento consiste nel lancio di un dado e se chiamiamo successo l'uscita di un numero maggiore di 2, abbiamo $p = 2/3$ e $q = 1/3$.

Si supponga di ripetere più volte l'esperimento. Se le probabilità di successo e di fallimento sono costanti, cioè non dipendono dai risultati precedenti, si parla di un *processo bernoulliano*. Esempi includono, oltre al lancio di dadi e/o monete, le uscite di numeri alla roulette, lotterie, ecc. Supponiamo di ripetere un processo bernoulliano per n volte. Ci chiediamo qual è la probabilità di ottenere *esattamente* k successi. Denotiamo tale probabilità come $\text{Pr}(n, k)$. Abbiamo

$$\text{Pr}(n, k) = \binom{n}{k} p^k q^{n-k}. \quad (4.18)$$

Infatti, si possono scegliere i k successi (e, implicitamente, anche gli $n - k$ fallimenti) in $\binom{n}{k}$ modi, e la probabilità che si verifichino esattamente quei successi è $p^k q^{n-k}$, in quanto gli eventi sono indipendenti.

Infine la probabilità di avere *almeno* k successi in n tentativi è

$$\sum_{i=k}^n \binom{n}{i} p^i q^{n-i}.$$

Esempio. L'allineamento di 2 sequenze di DNA, una di lunghezza n e l'altra di lunghezza $m \geq n$, consiste nel disporle una sopra l'altra, inserendo spazi (detti *gap*, e indicati con “-”) nelle due in modo che diventino della stessa lunghezza, ma senza mai mettere due gap uno sopra l'altro.

Ad esempio, questo è un possibile allineamento delle sequenze ATCCGA e TCAAAGA:

A	T	C	C	-	-	-	G	A
-	T	-	C	A	A	A	G	A

Mentre il seguente allineamento non risulta valido:

A	-	T	C	C	-	-	-	G	A
-	-	T	C	A	A	-	A	G	A

Quanti sono i possibili allineamenti validi di due sequenze?

Si può ragionare così: la lunghezza l delle due sequenze allineate va da un minimo di m a un massimo di $n + m$. Per ognuna di tali lunghezze, si può piazzare la sequenza più piccola (la prima) in $\binom{l}{n}$ modi, occupando n delle l posizioni con lettere, e le rimanenti $l - n$ con gaps. Siccome a ognuno dei gap deve corrispondere una lettera vera della seconda sequenza, restano $m - (l - n)$ lettere da mettere nelle n posizioni corrispondenti a lettere della prima sequenza. Otteniamo che gli allineamenti sono in tutto

$$\sum_{l=m}^{n+m} \binom{l}{n} \binom{n}{m-l+n}.$$

◇

ESERCIZIO 4.20. Dimostrare che

$$3^n = \sum_{k=0}^n \binom{n}{k} 2^k$$

◇

4.3 Disposizioni (sottoinsiemi ordinati)

Supponiamo di voler selezionare una sequenza di k oggetti da un insieme di n , e che quindi l'ordine degli oggetti abbia importanza (come insiemi, $\{3, 1, 2\} = \{1, 2, 3\}$, ma come sequenze $(3, 1, 2) \neq (1, 2, 3)$).

I sottoinsiemi ordinati di dimensione k si dicono anche *disposizioni di n oggetti a k* e il loro numero è indicato con $D(n, k)$. Siccome ogni sottoinsieme di dimensione k può essere ordinato in $k!$ modi, abbiamo

$$D(n, k) = \binom{n}{k} k! \quad (4.19)$$

Mnemonicamente, $D(n, k)$ è il prodotto dei primi k numeri decrescenti, a partire da n :

$$D(n, k) = \frac{n!}{(n-k)!} = n(n-1) \cdots (n-k+1).$$

Casi speciali: $D(n, 0) = 1$, $D(n, 1) = n$, $D(n, n) = n!$ e $D(n, m) = 0$ per $m > n$.

Esempio. Al campionato di una nazione calcisticamente “minore” partecipano 18 squadre. La squadra vincitrice del campionato viene ammessa alla Champions League. La seconda classificata accede all’Europa League nel tabellone principale, mentre la terza è ammessa ai preliminari di Europa League. In quanti modi possono essere prese le tre squadre che parteciperanno a queste competizioni europee? Siccome l’ordine è importante, i modi sono $18 \cdot 17 \cdot 16 = 4896$. \diamond

ESERCIZIO 4.21. Quanti codici di 4 lettere diverse si possono formare scegliendo le lettere dall’insieme $\{A, B, K, L, M, P\}$? \diamond

ESERCIZIO 4.22. In quanti modi p ragazzi possono essere assegnati a q famiglie disposte a ospitarli, al più uno per famiglia, per una vacanza all’estero, con $p \leq q$? \diamond

4.4 Ripetizioni e multi-insiemi

Un *multi-insieme* è costituito da un insieme $S = \{a_1, \dots, a_k\}$ in cui gli elementi possono essere ripetuti più volte. Il numero di volte che a_i è presente in S si indica con n_i ed è detto *numero di ripetizioni*. La scrittura concisa di un multi-insieme è

$$\{n_1 \cdot a_1, n_2 \cdot a_2, \dots, n_k \cdot a_k\} \quad (4.20)$$

Ad esempio, un multi-insieme con tre A, quattro B e due C si indica come

$$\{3 \cdot A, 4 \cdot B, 2 \cdot C\}$$

Una possibile permutazione di questi elementi è AABCABBCB. Un’altra è BBACCABAB. Vogliamo contare quante sono le permutazioni di un multi-insieme.

Esempio. Quanti sono gli anagrammi della parola MISSISSIPPI?

Si può guardare alla parola come al multi-insieme $\{1 \cdot M, 4 \cdot I, 4 \cdot S, 2 \cdot P\}$. Supponiamo di considerare tutte le $11!$ permutazioni delle lettere (i.e., gli anagrammi). Per ognuna di tali permutazioni, possiamo scambiare

fra di loro le I (o le S, o le P,...) e l'anagramma rimane lo stesso. Le 4 I si possono riordinare in $4!$ modi, e similmente per le altre lettere. Si ottiene un totale di $\frac{11!}{1! \cdot 4! \cdot 4! \cdot 2!}$ possibilità. \diamond

Generalizziamo il risultato dell'esercizio precedente:

TEOREMA 26: Sia S un multi-insieme con oggetti di k tipi e numeri di ripetizione n_1, n_2, \dots, n_k . Sia n la dimensione di S , dove $n = n_1 + n_2 + \dots + n_k$. Allora il numero di permutazioni di S è

$$\frac{n!}{n_1! n_2! \dots n_k!}.$$

Dim: Siano a_1, a_2, \dots, a_k gli elementi di S , con a_i ripetuto n_i volte, per $i = 1, \dots, k$. Possiamo costruire una permutazione di S in questo modo. Dobbiamo riempire n posizioni con i nostri oggetti. Prima piazziamo gli n_1 elementi di tipo a_1 . Questo può essere fatto in $\binom{n}{n_1}$ modi. Tra le rimanenti $n - n_1$ posizioni, piazziamo gli n_2 elementi di tipo a_2 . Questo si può fare in $\binom{n-n_1}{n_2}$ modi. Proseguiamo in questo modo fino alla fine, ossia fino a piazzare gli n_k oggetti di tipo a_k nelle $n - n_1 - n_2 - \dots - n_{k-1}$ posizioni rimaste (si noti che $n_k = n - n_1 - n_2 - \dots - n_{k-1}$ e quindi questo può essere fatto in un unico modo). Si ottiene che il numero di permutazioni è

$$\binom{n}{n_1} \binom{n-n_1}{n_2} \binom{n-n_1-n_2}{n_3} \dots \binom{n-n_1-n_2-\dots-n_{k-1}}{n_k}$$

Dalla definizione di coefficiente binomiale, si ottiene che il numero è uguale a

$$\frac{n!}{n_1!(n-n_1)!} \cdot \frac{(n-n_1)!}{n_2!(n-n_1-n_2)!} \cdot \frac{(n-n_1-n_2)!}{n_3!(n-n_1-n_2-n_3)!} \dots$$

Semplificando numeratori e denominatori, si ottiene

$$\frac{n!}{n_1! n_2! \dots n_k!}.$$



Esempio. Le strade di Manhattan sono di due tipi, i.e., Avenues e Streets. Le Avenues sono tutte parallele fra loro, e perpendicolari alle Streets, tutte parallele fra loro. Un impiegato abita all'incrocio fra la 10a Street e la 25a Ave. Il suo ufficio si trova all'incrocio fra la 16a Street e la 29a Ave. Supponendo che cammini sempre in direzione dell'ufficio (ossia verso Street e Ave sempre crescenti), in quanti modi diversi può recarsi da casa all'ufficio?

L'impiegato deve percorrere 6 blocchi in direzione Nord e 4 blocchi in direzione Est. Ogni stringa con 6 N e 4 E, come NNENEEENN oppure NENNNNEEE, ecc., rappresenta una soluzione. Quindi, ci sono $\frac{10!}{6! 4!}$ possibili soluzioni. Nel caso generale, se la griglia consta di m righe e n colonne, ci sono $\frac{(m+n)!}{m! n!}$ soluzioni. \diamond

4.4.1 Combinazioni con ripetizioni

Supponiamo dato un multi-insieme $S = \{n_1 \cdot a_1, n_2 \cdot a_2, \dots, n_k \cdot a_k\}$ e di voler prendere r elementi di S . Ogni sottoinsieme di r elementi di S si chiama una r -combinazione di S .

Esempio. Sia $S = \{2 \cdot a, 1 \cdot b, 3 \cdot c\}$. Allora le 3-combinazioni di S sono: $\{2 \cdot a, 1 \cdot b\}$, $\{2 \cdot a, 1 \cdot c\}$, $\{1 \cdot a, 1 \cdot b, 1 \cdot c\}$, $\{1 \cdot a, 2 \cdot c\}$, $\{1 \cdot b, 2 \cdot c\}$ e $\{3 \cdot c\}$. \diamond

Supponiamo $n_i \geq r$ per ogni i (in modo tale che ci sia una quantità sufficiente di elementi di tipo a_i per poter, al limite, prendere gli r elementi tutti dello stesso tipo). Per calcolare quante sono le r -combinazioni di S , dobbiamo scegliere quanti prenderne per ognuno dei k tipi, in modo da prenderne esattamente r in totale.

Questo problema corrisponde al problema di ripartire r elementi in k gruppi, che a sua volta corrisponde a risolvere l'equazione

$$x_1 + x_2 + \dots + x_k = r \quad (4.21)$$

dove ogni x_i è un numero intero, $0 \leq x_i \leq r$. Ci chiediamo quante sono le soluzioni diverse. Consideriamo r simboli uguali (ad es. A) e aggiungiamo $k - 1$ simboli che serviranno da separatori (ad es il simbolo “|”). Piazzando i separatori all'interno delle A, le ripartiamo in k blocchi, delimitati dai separatori. La dimensione del blocco i è il valore x_i , che soddisfa l'equazione (4.21).

Ad esempio, se $r = 8$ e $k = 4$, scrivendo

AA|A|AAA|AA

identifichiamo la soluzione $x_1 = 2, x_2 = 1, x_3 = 3, x_4 = 2$. Invece, la scrittura

A|||AAAAAA

identifica la soluzione $x_1 = 1, x_2 = 0, x_3 = 0, x_4 = 7$.

In quanti modi si possono mescolare $k - 1$ “|” con r “A”? Abbiamo un totale di $r + k - 1$ posizioni. Dobbiamo scegliere le r posizioni occupate dalle A (le rimanenti sono occupate dai separatori). Si ottengono

$$\binom{r + k - 1}{r} \quad (4.22)$$

possibilità. Abbiamo perciò dimostrato il seguente teorema:

TEOREMA 27: Il numero di r -combinazioni di un multi-insieme $S = \{n_1 \cdot a_1, n_2 \cdot a_2, \dots, n_k \cdot a_k\}$, con $n_i \geq r$ per ogni $i = 1, \dots, k$, è

$$\binom{r + k - 1}{r}.$$

Si noti che, essendo la scelta delle posizioni delle A equivalente alla scelta delle posizioni dei separatori, un modo alternativo per calcolare le r -combinazioni è dato dal valore $\binom{r+k-1}{k-1}$.

ESERCIZIO 4.23. Ho 8 caramelle dello stesso tipo. In quanti modi diversi posso darle a 10 bambini? \diamond

ESERCIZIO 4.24. Potendo scegliere fra 10 tipi di fiori, quanti mazzi diversi che contengano esattamente 20 fiori sono possibili? \diamond

Esempio. Quante sono le sequenze non-decrescenti di 10 numeri, ciascuno appartenente all'insieme $\{1, \dots, 50\}$? Quante quelle crescenti?

Una sequenza è non-decrescente se $y_1 \leq y_2 \leq \dots \leq y_{10}$ ed è crescente se $y_1 < y_2 < \dots < y_{10}$. Per formare una sequenza non-decrescente basta decidere quanti “1” prendere, quanti “2”, ecc., fino a quanti “50” prendere, stando attenti a prendere in tutto esattamente 10 numeri. Detto x_i il numero di volte che i appare nella sequenza, avremo pertanto che le sequenze sono tante quante le soluzioni intere non-negative di

$$x_1 + x_2 + \dots + x_{50} = 10$$

ossia $\binom{59}{10}$. Nel caso invece si voglia una sequenza crescente, basta notare che, una volta presi i 10 elementi, c'è un unico modo in cui li posso disporre a formare una sequenza crescente. Quindi, le sequenze crescenti sono tante quanti i sottoinsiemi di 10 elementi, vale a dire $\binom{50}{10}$. \diamond

Esempio. Immaginiamo che ogni persona dotata di portafoglio abbia, nello stesso, al più 15 banconote, in tagli da 5, 10, 20, 50 e 100 euro. Sotto queste ipotesi, qual'è la probabilità che a Padova non ci siano due persone con gli stessi tagli nello stesso numero?

Supponiamo che un portafoglio contenga l banconote. Ci sono 5 tagli, per cui esistono $\binom{l+4}{4}$ portafogli diversi con l banconote. Il massimo di possibilità si ha per $l = 15$ in cui sono $\binom{19}{4} = 3876$. Anche ammettendo che per ogni altro l ci fossero altrettante possibilità ci sarebbero al più $16 \times 3876 = 62016$ portafogli diversi. Dando per scontato che a Padova il numero di persone con il portafoglio sia maggiore di questo valore, per il principio della piccionaia ci sono almeno due persone con gli stessi tagli, nelle stesse quantità. \diamond

Generalizzazione a valori interi limitati. Siano dati k valori interi b_1, \dots, b_k e un intero $r \geq \sum_{i=1}^k b_i$. Ci chiediamo quante soluzioni ha l'equazione

$$\sum_{i=1}^k x_i = r \tag{4.23}$$

in cui le variabili x_i possono assumere solo valori interi tali che $x_i \geq b_i$ per ogni $i = 1, \dots, k$.

Per risolvere questo tipo di equazioni, introduciamo k variabili non-negative y_1, \dots, y_k , per le quali

$$y_i = x_i - b_i \quad \forall i = 1, \dots, k.$$

Essendo $x_i = y_i + b_i$ per ogni i , l'equazione (4.23) può essere riscritta come

$$\sum_{i=1}^k y_i = r - \sum_{i=1}^k b_i \quad (4.24)$$

in cui tutte le variabili y_i assumono dei valori in \mathbb{N} e anche in termine noto è un numero naturale. In base al teorema 27, il numero di soluzioni di (4.23) è

$$\binom{r - \sum_{i=1}^k b_i - k + 1}{k - 1}.$$

ESERCIZIO 4.25. Quante sono le soluzioni intere dell'equazione

$$x_1 + x_2 + x_3 + x_4 = 30$$

che soddisfano $x_1 \geq 2$, $x_2 \geq 0$, $x_3 \geq -5$ e $x_4 \geq 8$?

◇

ESERCIZIO 4.26. Avendo a disposizione 100 mele, 80 pere, 100 arance e 40 banane, quanti diversi cesti di frutta si possono comporre che contengano esattamente 30 frutti?

◇

ESERCIZIO 4.27. Ci sono 20 bastoncini disposti su una fila, e dobbiamo sceglierne 6:

| | | | | | | | | | | | | | | | | | | |

1. In quanti modi si può fare questa scelta?
2. In quanti modi se non possiamo mai prendere due bastoncini consecutivi?
3. In quanti modi se tra ogni coppia di bastoncini scelti devono esserci almeno due bastoncini?

◇

Chapter 5

Il principio di inclusione-esclusione

5.1 Il principio base

Sia S un insieme su cui sono definite alcune proprietà P_1, P_2, \dots, P_m . Ogni elemento di S può possedere o meno la proprietà P_i , per $i = 1, \dots, m$. Ad esempio, se $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ e P_1 è la proprietà “essere dispari”, e P_2 è la proprietà “essere divisibile per 3”, allora

- 9 possiede sia la P_1 che la P_2
- 5 possiede la P_1 ma non la P_2
- 6 possiede la P_2 ma non la P_1
- 8 non possiede nè la P_1 nè la P_2

Denotiamo con A_i l'insieme degli elementi di S che possiedono la proprietà P_i , per $i = 1, \dots, m$. Indichiamo inoltre con \bar{A}_i il *complementare* di A_i in S , ossia l'insieme degli elementi di S che *non* possiedono la proprietà P_i . L'insieme degli elementi di S che *non possiede alcuna* delle proprietà sarà pertanto

$$\bar{A}_1 \cap \bar{A}_2 \cap \dots \cap \bar{A}_m.$$

Il seguente teorema è noto come *principio di inclusione-esclusione*:

TEOREMA 28: Il numero di elementi di S che non possiede alcuna delle proprietà P_1, \dots, P_m è

$$\begin{aligned} |\bar{A}_1 \cap \bar{A}_2 \cap \dots \cap \bar{A}_m| &= |S| \\ &\quad - \sum_{\{i_1\}} |A_{i_1}| \\ &\quad + \sum_{\{i_1, i_2\}} |A_{i_1} \cap A_{i_2}| \\ &\quad - \sum_{\{i_1, i_2, i_3\}} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| \\ &\quad \dots \\ &\quad + (-1)^d \sum_{\{i_1, \dots, i_d\}} |A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_d}| \\ &\quad \dots \\ &\quad + (-1)^m |A_1 \cap A_2 \cap \dots \cap A_m| \end{aligned} \tag{5.1}$$

dove gli indici della generica somma $\sum_{\{i_1, \dots, i_d\}}$ sono tutti i sottoinsiemi di $\{1, \dots, m\}$ di cardinalità d .

Ad esempio, se $m = 3$ il teorema afferma che

$$\begin{aligned} |\bar{A}_1 \cap \bar{A}_2 \cap \bar{A}_3| &= |S| - (|A_1| + |A_2| + |A_3|) \\ &\quad + (|A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3|) \\ &\quad - |A_1 \cap A_2 \cap A_3| \end{aligned}$$

Dimostriamo il teorema.

Dim: Facciamo vedere che ogni elemento di S che non ha alcuna delle proprietà contribuisce 1 al valore della somma a destra nell'equazione (5.11), mentre un elemento che ha $n > 0$ delle proprietà contribuisce 0 al valore di tale somma. Pertanto, il valore di tale somma è esattamente pari al numero di elementi che non hanno nessuna delle proprietà.

Consideriamo allora un elemento x che non ha alcuna delle proprietà. Si ha che $x \in S$ ma $x \notin A_i$ per $i = 1, \dots, m$. Pertanto il contributo di x alla somma in questione è

$$1 - 0 + 0 - 0 + \dots + (-1)^m 0 = 1.$$

Supponiamo ora che y sia un elemento che ha esattamente $n \geq 1$ delle proprietà. Il contributo di y a $|S|$ è 1. Il contributo di y a $\sum_{\{i_1\}} |A_{i_1}|$ è $n = \binom{n}{1}$, perchè y possiede esattamente n proprietà, e pertanto è in esattamente n degli insiemi A_1, \dots, A_m . Il contributo di y a $\sum_{\{i_1, i_2\}} |A_{i_1} \cap A_{i_2}|$ è $\binom{n}{2}$, perchè ci sono $\binom{n}{2}$ modi di scegliere 2 proprietà possedute da y , ossia due insiemi A_{i_1} e A_{i_2} ai quali y appartiene. Analogamente, il contributo di y a $\sum_{\{i_1, i_2, i_3\}} |A_{i_1} \cap A_{i_2} \cap A_{i_3}|$ è $\binom{n}{3}$. Proseguendo in questo modo, il contributo netto di y alla somma in (5.11) è

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \dots + (-1)^m \binom{n}{m}$$

che, essendo $n \leq m$, è uguale a

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \dots + (-1)^n \binom{n}{n}. \quad (5.2)$$

Sviluppando il valore dell'espressione $(1 - 1)^n$ secondo il triangolo di Pascal, si nota che tale espressione è esattamente uguale a (5.2), che pertanto deve valere 0. Quindi il contributo di y alla somma (5.11) è 0, e il teorema è dimostrato. ♣

Si noti che, nel descrivere il teorema, abbiamo usato una forma “negata”, chiedendoci quanti sono gli elementi che *non* possiedono alcuna delle proprietà. Siccome l'insieme degli elementi che possiedono *almeno una delle proprietà* è chiaramente il complementare del nostro, possiamo facilmente esprimere il teorema anche in una versione “afferzata” che, per comodità, riportiamo qui:

Sia S un insieme e siano P_1, P_2, \dots, P_m alcune proprietà che ogni elemento di S può possedere o meno. Denotiamo con A_i l'insieme degli elementi di S che possiedono la proprietà P_i . L'insieme degli elementi di S che *possiede almeno una* delle proprietà è pertanto $A_1 \cup A_2 \cup \dots \cup A_m$.

Il principio di inclusione-esclusione ci dice allora che il numero di elementi di S che possiedono almeno una delle proprietà P_1, \dots, P_m è

$$\begin{aligned}
 |A_1 \cup A_2 \cup \dots \cup A_m| &= \sum_{\{i_1\}} |A_{i_1}| \\
 &\quad - \sum_{\{i_1, i_2\}} |A_{i_1} \cap A_{i_2}| \\
 &\quad + \sum_{\{i_1, i_2, i_3\}} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| \\
 &\quad \dots \\
 &\quad - (-1)^d \sum_{\{i_1, \dots, i_d\}} |A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_d}| \\
 &\quad \dots \\
 &\quad - (-1)^m |A_1 \cap A_2 \cap \dots \cap A_m|.
 \end{aligned} \tag{5.3}$$

Esempio. Quanti sono i numeri compresi tra 1 e 1000 che non sono divisibili per 5, nè per 6, nè per 8?

Usiamo il principio di inclusione-esclusione. Identifichiamo S come l'insieme $\{1, 2, \dots, 1000\}$. La proprietà P_1 è quella di essere divisibile per 5. La proprietà P_2 è quella di essere divisibile per 6. La proprietà P_3 è quella di essere divisibile per 8. Abbiamo che

$$|A_1| = \lfloor \frac{1000}{5} \rfloor = 200$$

$$|A_2| = \lfloor \frac{1000}{6} \rfloor = 166$$

$$|A_3| = \lfloor \frac{1000}{8} \rfloor = 125.$$

Un numero è in $A_1 \cap A_2$ se è divisibile per il minimo comune multiplo di 5 e 6, ossia per $\text{mcm}\{5, 6\} = 30$. Analogamente si ragiona per i numeri in $A_1 \cap A_3$ (divisibili per $\text{mcm}\{5, 8\} = 40$) e i numeri in $A_2 \cap A_3$ (divisibili per $\text{mcm}\{6, 8\} = 24$). Abbiamo

$$|A_1 \cap A_2| = \lfloor \frac{1000}{30} \rfloor = 33$$

$$|A_1 \cap A_3| = \lfloor \frac{1000}{40} \rfloor = 25$$

$$|A_2 \cap A_3| = \lfloor \frac{1000}{24} \rfloor = 41.$$

Infine, un numero è in $A_1 \cap A_2 \cap A_3$ se è divisibile per il minimo comune multiplo di 5, 6 e 8, ossia per $\text{mcm}\{5, 6, 8\} = 120$. Si ha

$$|A_1 \cap A_2 \cap A_3| = \lfloor \frac{1000}{120} \rfloor = 8.$$

In conclusione, si hanno $1000 - (200 + 166 + 125) + (33 + 25 + 41) - 8 = 600$ numeri del tipo desiderato.
 \diamond

Esempio. Quante sono le permutazioni delle lettere

C,A,N,E,D,I,U,G,O

in cui non si legge nè la parola “CANE”, nè la parola “DI”, nè la parola “UGO”? Ad esempio, la permutazione NEDUOICAG va bene, così come UIDEACGON, mentre non vanno bene OGCANEIDU nè EIDCUGOAN.

Usiamo il principio di inclusione-esclusione. Identifichiamo S come l'insieme di tutte le permutazioni delle 9 lettere date. La proprietà P_1 è quella di contenere la parola “CANE”. La proprietà P_2 è quella di contenere la parola “DI”. La proprietà P_3 è quella di contenere la parola “UGO”. L'insieme A_1 corrisponde a tutte le permutazioni dei 6 simboli

$$\{\text{CANE}, D, I, U, G, O\}$$

e pertanto $|A_1| = 6!$. Similmente, A_2 sono le permutazioni degli 8 simboli $\{C, A, N, E, DI, U, G, O\}$ e $|A_2| = 8!$. Infine, A_3 corrisponde alle permutazioni dei 7 simboli $\{C, A, N, E, D, I, UGO\}$ e $|A_3| = 7!$. L'insieme $A_1 \cap A_2$ corrisponde a tutte le permutazioni dei simboli $\{\text{CANE}, DI, U, G, O\}$, e pertanto $|A_1 \cap A_2| = 5!$. Analogamente $|A_1 \cap A_3| = 4!$ e $|A_2 \cap A_3| = 6!$. Infine, $A_1 \cap A_2 \cap A_3$ corrisponde a tutte le permutazioni di $\{\text{CANE}, DI, UGO\}$ e $|A_1 \cap A_2 \cap A_3| = 3!$. Per il principio di inclusione-esclusione, il numero di permutazioni cercato è $9! - (6! + 8! + 7!) + (5! + 4! + 6!) - 3!$ ossia $362880 - 720 - 40320 - 5040 + 120 + 24 + 720 - 6 = 317658$. \diamond

Esempio. Quante sono le soluzioni dell'equazione

$$x_1 + x_2 + x_3 + x_4 + x_5 = 30 \quad (5.4)$$

in cui tutte le variabili assumono valori in \mathbb{N} ed inoltre $x_1 \leq 5$ e $x_2 \leq 3$? Un modo di risolvere il problema è quello di considerare tutte le coppie di valori ammissibili per (x_1, x_2) (in base al principio del prodotto, si tratta di 24 casi) e per ciascuno di questi casi sostituire i valori di x_1 e x_2 nell'espressione (5.4) ottenendo un'equazione in tre variabili intere non-negative, della quale sappiamo calcolare il numero di soluzioni (si veda la sezione 4.4.1). Per il principio della somma, sommando questi 24 risultati otterremo il numero di soluzioni del problema. Nel caso specifico, tale numero è

$$\sum_{x_1=0}^5 \sum_{x_2=0}^3 \binom{30 - (x_1 + x_2) + 2}{2} = 9122$$

Un modo alternativo di risolvere il problema si basa sul principio di inclusione-esclusione, e richiede di considerare solo quattro casi al posto di 24. In particolare, introduciamo le due proprietà $P_1 :=$ “nella soluzione si ha $x_1 \geq 6$ ” e $P_2 :=$ “nella soluzione si ha $x_2 \geq 4$ ”, sicchè il nostro problema consiste nel calcolare $|\bar{A}_1 \cap \bar{A}_2|$, che sappiamo essere pari a $|S| - (|A_1| + |A_2|) + |A_1 \cap A_2|$. L'insieme S contiene tutte le soluzioni di (5.4) e quindi

$$|S| = \binom{34}{4} = 46376.$$

A_1 consiste di tutte le soluzioni per le quali $x_1 \geq 6$. Per calcolare $|A_1|$ introduciamo una nuova variabile non-negativa, che chiameremo y_1 , tale che $x_1 = 6 + y_1$. Sostituendo x_1 con $6 + y_1$ in (5.4), otteniamo che $|A_1|$ è pari al numero di soluzioni intere non-negative dell'equazione $y_1 + x_2 + x_3 + x_4 + x_5 = 24$, e quindi

$$|A_1| = \binom{28}{4} = 20475.$$

In modo perfettamente analogo, sostituendo x_2 con $4 + y_2$ (dove y_2 è una nuova variabile ≥ 0) otteniamo che $|A_2|$ è pari al numero di soluzioni intere non-negative dell'equazione $x_1 + y_2 + x_3 + x_4 + x_5 = 26$, e quindi

$$|A_2| = \binom{30}{4} = 27405.$$

Infine, le soluzioni in $A_1 \cap A_2$ hanno $x_1 \geq 6$ e $x_2 \geq 4$. Operando le medesime sostituzioni di cui sopra, su x_1 e x_2 contemporaneamente, otteniamo che $|A_1 \cap A_2|$ è pari al numero di soluzioni intere non-negative dell'equazione $y_1 + y_2 + x_3 + x_4 + x_5 = 20$, e quindi

$$|A_1 \cap A_2| = \binom{24}{4} = 10626.$$

Mettendo tutto insieme, abbiamo

$$|\bar{A}_1 \cap \bar{A}_2| = |S| - (|A_1| + |A_2|) + |A_1 \cap A_2| = 46376 - 20475 - 27405 + 10626 = 9122.$$

◇

ESERCIZIO 5.1. Quante sono le permutazioni delle 10 lettere

V, I, V, A, L, A, V, I, T, A

in cui non si legge nè “VIVA”, nè “LA” nè “VITA”?

◇

ESERCIZIO 5.2. Quante sono le permutazioni delle 6 lettere

V, I, A, V, A, I

in cui non si legge nè “VIA” nè “VAI”?

◇

ESERCIZIO 5.3. Quanti interi compresi tra 0 e 99999 hanno fra le loro cifre sia 2 che 5 che 8?

◇

ESERCIZIO 5.4. In quanti modi si possono piazzare 8 torri su una scacchiera 8×8 in modo che nessuna attacchi alcuna delle altre? In quanti modi se supponiamo di avere 3 torri di colore rosso, tre blu e 2 nere (con le torri dello stesso colore indistinguibili fra loro)? In quanti modi infine se tutte le torri sono distinguibili fra loro?

◇

Esempio. Consideriamo due problemi la cui soluzione richiede di applicare il principio di inclusione-esclusione, e che si presentano nell'ambito di un popolare gioco di carte, il poker *Texas Hold'em*.

Questo gioco utilizza un mazzo completo di 52 carte. Ad ogni giocatore vengono distribuite due carte coperte private. Questa fase è detta il *preflop*. Vengono poi scoperte 5 carte comuni, prima tre (il *flop*), poi una (il *turn*), e infine l'ultima (il *river*). A questo punto, vince la mano il giocatore che realizza il punto più

alto, fatto da 5 carte su 7, combinando le sue due carte con le cinque carte comuni. È stato verificato che la mano più forte che un giocatore può ricevere preflop (ossia quella che alla fine chiude mediamente il punto migliore) è una coppia di assi.

Supponiamo che al tavolo siano seduti $n = 9$ giocatori. Ci chiediamo:

1. **Preflop eccezionali:** Qual è la probabilità che almeno un giocatore riceva una coppia d'assi preflop?
2. **Colore:** Supponiamo che, delle 5 carte comuni, esattamente 3 siano di cuori. Con che probabilità almeno uno dei 9 giocatori ha in mano due carte di cuori?

Modi di distribuire le carte. Ai fini del calcolo delle probabilità di cui sopra, ci servirà rispondere, come prima cosa, alla seguente domanda: “In quanti modi g giocatori possono ricevere ciascuno due carte prese da un mazzo di c carte?”

Chiamiamo $\text{DIST}(c, g)$ questo valore. Chiaramente, $\text{DIST}(c, g) = 0$ se $c < 2g$. Se $c \geq 2g$ abbiamo i seguenti risultati:

(i) Se $c = 2g$

$$\text{DIST}(2g, g) = \frac{(2g)!}{2^g}$$

Per vedere ciò, ragioniamo così: consideriamo una permutazione π delle $2g$ carte. Immaginiamo che il primo giocatore riceva, nell'ordine, le carte π_1 e π_2 , il secondo π_3, π_4 , eccetera, fino all'ultimo che riceve π_{2g-1}, π_{2g} . Ogni permutazione identifica le carte ricevute dai giocatori, ma ai fini del gioco l'ordine delle due carte non è importante, e conta solo quali sono le carte. Quindi, ci sono diverse permutazioni che identificano le stesse coppie. Le prime due carte possono essere ordinate in 2 modi, le seconde pure, ecc, e quindi dobbiamo dividere il numero di permutazioni per 2^g .

(ii) Se $c > 2g$

$$\text{DIST}(c, g) = \binom{c}{2g} \text{DIST}(2g, g) = \binom{c}{2g} \frac{(2g)!}{2^g}$$

Questa formula si giustifica considerando che, da un mazzo di c carte, possiamo prima scegliere le $2g$ carte che saranno distribuite, e poi distribuirle in $\text{DIST}(2g, g)$ modi.

Ad esempio, il numero di modi in cui 9 giocatori possono ricevere due carte preflop è

$$\text{DIST}(52, 9) = \frac{52 \cdot 51 \cdots 36 \cdot 35}{2^9} \simeq 5 \cdot 10^{26}.$$

Preflop eccezionali. Consideriamo l'evento “almeno un giocatore ha coppia d'assi”. Per $i = 1, \dots, 9$, chiamiamo P_i la proprietà: “il giocatore i ha ricevuto una coppia di assi” e sia A_i l'insieme di tutte le distribuzioni in cui P_i è soddisfatta. Siccome ci sono 4 assi nel mazzo, abbiamo

$$|A_i| = \binom{4}{2} \text{DIST}(50, 8)$$

(in particolare, la probabilità che P_i si verifichi è $|A_i|/\text{DIST}(52, 9) = 1/221$. Questa probabilità si poteva calcolare anche come $\binom{4}{2}/\binom{52}{2}$).

Per $1 \leq i < j \leq 9$, sia P_{ij} l'evento congiunto “Sia il giocatore i che il giocatore j hanno ricevuto coppia d'assi”. Scelti i due assi del giocatore i (in $\binom{4}{2}$ modi), gli assi di j sono univocamente determinati, per cui

$$|A_i \cap A_j| = \binom{4}{2} \text{DIST}(48, 7)$$

(in particolare, la probabilità che P_{ij} accada vale $|A_i \cap A_j|/\text{DIST}(52, 9) = 1/270725$).

Se consideriamo l'evento di aver ricevuto coppia d'assi relativamente a tre o più giocatori, il numero di modi in cui ciò può avvenire è chiaramente zero, visto che nel mazzo ci sono solo 4 assi.

A questo punto, per il principio di inclusione-esclusione, il numero complessivo di modi in cui l'evento “Almeno un giocatore ha ricevuto due assi” può verificarsi è

$$\sum_{i=1}^9 |A_i| - \sum_{1 \leq i < j \leq 9} |A_i \cap A_j|$$

da cui, dividendo per $\text{DIST}(52, 9)$ abbiamo la probabilità

$$\sum_{i=1}^9 \frac{1}{221} - \sum_{1 \leq i < j \leq 9} \frac{1}{270725} = \frac{21978}{541450} \simeq 0.04059100$$

Quindi, circa una volta ogni 25 mani giocate, c'è (almeno) un giocatore al tavolo che riceve una coppia di assi.

Probabilità di colore. Supponiamo che siano state girate le 5 carte comuni, e che esattamente 3 di esse siano dello stesso seme (diciamo cuori). Assumendo che tutti i 9 giocatori siano ancora in gioco, ci chiediamo qual è la probabilità che uno di essi abbia in mano due carte di cuori e che quindi abbia chiuso il colore.

Per $i = 1, \dots, 9$, chiamiamo P_i la proprietà: “le carte in mano al giocatore i sono entrambe di cuori”, e sia A_i l'insieme di tutti i modi in cui le carte possono essere distribuite preflop che soddisfano la proprietà P_i . Denotiamo inoltre con S l'insieme di tutti i modi in cui le carte possono essere state distribuite. Siccome 5 delle carte sono in tavola, faccia in su, abbiamo

$$|S| = \text{DIST}(47, 9). \quad (5.5)$$

Ora, $|A_i|$ è identico per ogni i , e vale

$$|A_i| = \binom{10}{2} \text{DIST}(45, 8) \quad (5.6)$$

La ragione di ciò è che le due carte di cuori del giocatore i possono essere scelte tra 10 carte, e, scelte queste, le rimanenti 45 carte sono distribuite a 8 giocatori. Analogamente, il numero di modi in cui due giocatori i

e j ricevono ciascuno due carte di cuori è

$$|A_i \cap A_j| = \binom{10}{2} \binom{8}{2} \text{DIST}(43, 7). \quad (5.7)$$

Le distribuzioni che danno colore a tre giocatori i , j e k , sono in tutto

$$|A_i \cap A_j \cap A_k| = \binom{10}{2} \binom{8}{2} \binom{6}{2} \text{DIST}(41, 6). \quad (5.8)$$

Continuando, otteniamo delle espressioni simili per il caso di 4 e 5 giocatori, ossia

$$|A_i \cap A_j \cap A_k \cap A_u| = \binom{10}{2} \binom{8}{2} \binom{6}{2} \binom{4}{2} \text{DIST}(39, 5) \quad (5.9)$$

$$|A_i \cap A_j \cap A_k \cap A_u \cap A_v| = \binom{10}{2} \binom{8}{2} \binom{6}{2} \binom{4}{2} \binom{2}{2} \text{DIST}(37, 4), \quad (5.10)$$

mentre per 6 o più giocatori, il numero di modi in cui ciascuno di loro può ricevere due carte di cuori è chiaramente zero, visto che nel mazzo sono rimaste in tutto soltanto 10 carte di cuori.

In base al principio di inclusione-esclusione, il numero di distribuzioni che soddisfano almeno una delle P_i (ossia tali che almeno un giocatore ha chiuso il colore) è $r = |A_1 \cup A_2 \cup \dots \cup A_m|$, con

$$\begin{aligned} r = & \sum_{\{i\}} |A_i| \\ & - \sum_{\{i,j\}} |A_i \cap A_j| \\ & + \sum_{\{i,j,k\}} |A_i \cap A_j \cap A_k| \\ & - \sum_{\{i,j,k,u\}} |A_i \cap A_j \cap A_k \cap A_u| \\ & + \sum_{\{i,j,k,u,v\}} |A_i \cap A_j \cap A_k \cap A_u \cap A_v| \end{aligned} \quad (5.11)$$

Considerando che ci sono $\binom{9}{k}$ modi di scegliere k giocatori dai nostri 9, otteniamo

$$\begin{aligned} r = & 9|A_1| \\ & - \binom{9}{2}|A_1 \cap A_2| \\ & + \binom{9}{3}|A_1 \cap A_2 \cap A_3| \\ & - \binom{9}{4}|A_1 \cap A_2 \cap A_3 \cap A_4| \\ & + \binom{9}{5}|A_1 \cap A_2 \cap A_3 \cap A_4 \cap A_5| \end{aligned}$$

Dalle nostre formule precedenti (5.5)-(5.10), otteniamo che

$$\begin{aligned} r = & 9 \binom{10}{2} \text{DIST}(45, 8) - \binom{9}{2} \binom{10}{2} \binom{8}{2} \text{DIST}(43, 7) \\ & + \binom{9}{3} \binom{10}{2} \binom{8}{2} \binom{6}{2} \text{DIST}(41, 6) - \binom{9}{4} \binom{10}{2} \binom{8}{2} \binom{6}{2} \binom{4}{2} \text{DIST}(39, 5) \\ & + \binom{9}{5} \binom{10}{2} \binom{8}{2} \binom{6}{2} \binom{4}{2} \binom{2}{2} \text{DIST}(37, 4). \end{aligned}$$

A questo punto, facendo molta attenzione nell'eseguire i calcoli (e possibilmente avvalendoci di un software per il calcolo algebrico in alta precisione) abbiamo tutti gli elementi per calcolare la probabilità che qualche giocatore abbia chiuso il colore. Essa è

$$\Pr(\text{qualcuno ha colore}) = \frac{r}{|S|} = \frac{1728919851}{5178066751} \simeq 0.333892.$$

Si tratta di una probabilità estremamente vicina (anzi, a tutti i fini pratici del gioco, uguale) a $1/3$. Quindi, una volta su tre, se nove giocatori arrivano al river e in tavola ci sono 3 cuori, almeno uno di loro ha chiuso colore (la stessa probabilità vale anche quando al river arrivano meno di nove giocatori, ma nell'ipotesi che chiunque riceva preflop una mano di carte dello stesso colore, non passi mai e la porti fino al river). \diamond

ESERCIZIO 5.5. Si dimostrino le seguenti formule ricorsive:

$$\text{DIST}(c, g) = \frac{c}{c - 2g} \text{DIST}(c - 1, g)$$

e, per ogni $0 \leq k \leq g$,

$$\text{DIST}(c, g) = \frac{c(c-1)(c-2) \cdots (c-2k+1)}{2^k} \text{DIST}(c-2k, g-k)$$

\diamond

ESERCIZIO 5.6. Si calcoli, per $n = 2, 3, \dots, 8$, la probabilità che se n giocatori ricevono ciascuno due carte, almeno uno di loro riceva una coppia di assi. \diamond

ESERCIZIO 5.7. Si calcoli, per $n = 2, 3, \dots, 8$, la probabilità che se n giocatori ricevono ciascuno due carte, e poi vengono girate 5 carte di cui esattamente 3 sono di cuori, almeno uno di loro abbia ricevuto una coppia di carte di cuori. \diamond

Esempio. Una *stringa* sull'alfabeto $\Sigma = \{A, B\}$ è una qualsiasi parola costruita concatenando una sequenza di simboli di Σ . Ad esempio, le seguenti sono stringhe su Σ : ABAAB, ABBA, BABABABA. La *lunghezza* di una stringa corrisponde al numero di simboli di cui si compone. L'insieme di tutte stringhe della stessa lunghezza n è denotato con Σ^n . Ad esempio, le seguenti sono alcune delle 16 stringhe in Σ^4 : AABA, BBBA, BAAB. L' i -mo carattere di una stringa s è denotato con $s[i]$. Ad esempio, se $s = AABA$ si ha $s[3] = B$.

Consideriamo ora l'alfabeto $\Sigma' = \Sigma \cup \{*\}$ ottenuto aggiungendo a Σ il carattere $*$, detto *wild card*. Ogni stringa s costruita su Σ' rappresenta un insieme $C(s)$ di stringhe su Σ . In particolare, questo insieme è dato da tutte le stringhe ottenibili da s sostituendo tutte le occorrenze di una wild card con un qualsiasi simbolo di Σ . Ogni stringa in $C(s)$ è detta una stringa *compatibile* con s . Ovviamente, una stringa x su Σ è compatibile con s se e solo se x e s hanno la stessa lunghezza, e per ogni posizione i tale che $s[i] \neq *$, si ha $x[i] = s[i]$. Ad esempio, l'insieme delle stringhe compatibili con $s = A*B**$ è

$$C(A*B**) = \{AABAA, AABAB, AABBA, AABBB, ABBAA, ABBAB, ABBBA, ABBBB\}.$$

È immediato verificare che se una stringa s in $(\Sigma')^n$ contiene k wild cards, allora vi sono esattamente 2^k stringhe in Σ^n compatibili con s . Supponiamo ora che sia dato un insieme S di stringhe in $(\Sigma')^n$, che chiamiamo *queries*. Ci chiediamo quante sono le stringhe in Σ^n compatibili con almeno una delle queries in S . Chiamiamo tale numero $\sigma(S)$.

Ci sono due modi possibili di calcolare $\sigma(S)$:

1. Andando a considerare, una alla volta, ogni query $s \in S$, generando tutte le stringhe compatibili con essa, e mantenendo l'unione di tutte le stringhe via via generate.
2. Utilizzando il principio di inclusione-esclusione, come descritto nel seguito.

L'idea è quella di contare prima le stringhe compatibili con esattamente una query, poi sottrarre quelle compatibili con esattamente due queries, riaggiungere quelle compatibili con esattamente tre, ecc. Quindi, stiamo applicando il principio di inclusione-esclusione dove, per ogni stringa, la proprietà P_i è quella di essere compatibile con la query i -ma, per $i = 1, \dots, |S|$.

Dato un qualsiasi sottoinsieme $Y \subset S$, denotiamo con T_Y l'insieme delle stringhe che sono compatibili con *tutte* le queries di Y (i.e., $x \in T_Y$ se x è compatibile con s per ogni s in Y). Sia δ_Y la cardinalità di T_Y . Chiaramente, $\delta_\emptyset = 0$, mentre, nel caso generale, è facile calcolare δ_Y basandosi sulla seguente regola:

1. Se esistono due queries $s, s' \in Y$, e una posizione $i \in \{1, \dots, n\}$, tali che $s[i] \neq *$, $s'[i] \neq *$, e $s[i] \neq s'[i]$ allora $\delta_Y = 0$ (infatti, in questo caso, una stringa x compatibile sia con s che con s' dovrebbe avere $x[i] = s[i]$ e $x[i] = s'[i]$, ma ciò è impossibile).
2. Altrimenti, sia k il numero di posizioni i per le quali vale $s[i] = *$ per ogni $s \in Y$. Allora $\delta_Y = 2^k$

(si noti che, quando Y consiste di esattamente una query, il caso 1 non può verificarsi, e la regola si riduce al conteggio immediato che avevamo descritto in precedenza, i.e., una query con k “*” ha 2^k stringhe compatibili).

Dal principio di inclusione-esclusione si ottiene allora il seguente risultato:

$$\sigma(S) = \sum_{Y \subset S} (-1)^{|Y|-1} \delta_Y.$$

Ad esempio, se $a = **AA$, $b = *AA*$, $c = B**B$, e $S = \{a, b, c\}$, abbiamo: $\delta_{\{a\}} = \delta_{\{b\}} = \delta_{\{c\}} = 4$, $\delta_{\{a,b\}} = 2$, $\delta_{\{a,c\}} = 0$, $\delta_{\{b,c\}} = 1$, $\delta_{\{a,b,c\}} = 0$, da cui $\sigma(S) = (4 + 4 + 4) - (2 + 0 + 1) + 0 = 9$. L'insieme di tutte le stringhe compatibili con almeno una query è

$$\{AAAA, ABAA, BAAA, BBAA, AAAB, BAAB, BABB, BBAB, BBBB\}.$$

◇

ESERCIZIO 5.8. Quante sono le stringhe su $\{A, B\}$ compatibili con almeno una delle seguenti queries:

$$\{A***, *BAB, B**A, ***B, *AAA\}?$$

◇

Esempio. Quante sono le stringhe binarie di lunghezza 12, contenenti esattamente sei “1” e sei “0”, e tali che la stringa “010” non appare mai al loro interno? Chiamiamo *buone* le stringhe che non contengono 010 e *cattive* le altre. Chiamiamo inoltre V la stringa vietata, i.e., 010. Per contare le stringhe buone usiamo il principio di inclusione-esclusione. Sia S l'insieme di tutte le stringhe di 6 uni e 6 zeri, per cui $|S| = 12!/(6!6!) = 924$. Supponiamo che le posizioni siano numerate da 1 a 12, e chiamiamo *centro* di V ,

in una stringa cattiva, la posizione in cui si trova l'1 di V . In una stringa cattiva, il centro di V può essere qualsiasi posizione in $I = \{2, 3, \dots, 11\}$. Sull'insieme S , chiamiamo P_i la proprietà "nella stringa compare V , con centro in i ". Quindi a noi interessa sapere quante stringhe in S non godono di alcuna delle proprietà P_i , per $i = 2, \dots, 11$. Dovremo quindi enumerare quante stringhe godono di una, poi di due, ecc., proprietà, e usare il principio di inclusione-esclusione. Notiamo subito che è impossibile per una stringa cattiva di godere di sei o più delle proprietà, perchè questo implicherebbe la presenza di almeno 7 zeri nella stringa.

1. (Stringhe cattive che godono di P_i , per $i \in I$.) Sia n_1 il numero di stringhe che godono di P_i , per un dato i . Fissato $i \in I$, abbiamo

$$n_1 = 9!/(4!5!) = 126,$$

in quanto, dopo aver posizionato V con centro in i , restano da piazzare 9 simboli, di cui 4 sono zeri e 5 uni. Inoltre ci sono $M_1 = 10 = \binom{11}{1}$ modi di scegliere i .

2. (Stringhe cattive che godono di P_i e P_j , per $i, j \in I$, $i < j$.) Dobbiamo distinguere due casi:

- (2.a) I centri i e j sono "consecutivi", ossia le stringhe vietate condividono uno 0, come in "...01010...". Chiamiamo n_2^a il numero di stringhe cattive con centri in i e j consecutivi. Abbiamo

$$n_2^a = 7!/(3!4!) = 35.$$

Inoltre, due centri consecutivi possono essere presi in $M_2^a = 8$ modi in quanto la sequenza 01010 può avere 8 diversi punti di inizio.

- (2.b) I centri i e j non sono consecutivi, come in "...010...010...". Chiamiamo n_2^b il numero di stringhe cattive con centri in i e j non consecutivi. Abbiamo

$$n_2^b = 6!/(2!4!) = 15.$$

Per contare in quanti modi si possono prendere due centri non consecutivi (sia M_2^b tale numero), contiamo le soluzioni dell'equazione $x_1 + x_2 + x_3 = 6$. Infatti, detta $V(i)$ la sottostringa pari a V di centro i , e $V(j)$ la sottostringa pari a V di centro j , x_1 è il numero di bit prima di $V(i)$, x_2 sono i bit tra la fine di $V(i)$ e l'inizio di $V(j)$ e x_3 i bit tra la fine di $V(j)$ e la fine della stringa, come in

$$| \leftarrow x_1 \rightarrow |010| \leftarrow x_2 \rightarrow |010| \leftarrow x_3 \rightarrow |$$

Abbiamo quindi $M_2^b = \binom{8}{2} = 28$.

3. (Stringhe cattive che godono di P_i , P_j e P_k , per $i, j, k \in I$, $i < j < k$.) Distinguiamo 3 casi:

- (3a) I tre centri sono consecutivi, come in "...0101010...". Chiamiamo n_3^a il numero di stringhe cattive con tre centri i, j, k consecutivi. Abbiamo

$$n_3^a = 5!/(2!3!) = 10.$$

Inoltre, tre centri consecutivi possono essere presi in $M_3^a = 6$ modi in quanto la sequenza 0101010 può avere 6 diversi punti di inizio.

- (3b) Due dei centri sono consecutivi e il terzo non lo è, come in "...01010...010...". Chiamiamo n_3^b il numero di stringhe cattive con tre dati centri i, j, k di cui solo due consecutivi. Abbiamo

$$n_3^b = 4!/(1!3!) = 4.$$

Sia M_3^b il numero di modi in cui si possono prendere tre centri di cui due consecutivi. I due consecutivi possono essere i primi due o gli ultimi due. Supponiamo lo siano i primi due e in

seguito moltiplicheremo per 2 per avere il numero totale. I modi sono altrettanti che le soluzioni dell'equazione $x_1 + x_2 + x_3 = 4$, come rappresentato dalla scrittura:

$$| \leftarrow x_1 \rightarrow |01010| \leftarrow x_2 \rightarrow |010| \leftarrow x_3 \rightarrow |$$

Abbiamo perciò $M_3^b = 2 \times \binom{6}{2} = 30$, dove il fattore 2 è dovuto al fatto che, come osservato, i due centri consecutivi possono essere i primi due o gli ultimi due.

- (3c) I tre centri sono tutti non consecutivi, come in "...010...010...010...". Chiamiamo n_3^c il numero di stringhe cattive con tre centri i, j, k non consecutivi. Abbiamo

$$n_3^c = 3!/(0!3!) = 1.$$

Sia M_3^c il numero di modi in cui si possono prendere tre centri tutti non consecutivi. I modi sono altrettanti che le soluzioni dell'equazione $x_1 + x_2 + x_3 + x_4 = 3$, come rappresentato dalla scrittura:

$$| \leftarrow x_1 \rightarrow |010| \leftarrow x_2 \rightarrow |010| \leftarrow x_3 \rightarrow |010| \leftarrow x_4 \rightarrow |$$

Abbiamo perciò $M_3^c = \binom{6}{3} = 20$.

4. (Stringhe cattive che godono di P_i, P_j, P_k , e P_h per $i, j, k, h \in I, i < j < k < h$.) Distinguiamo i seguenti casi:

- (4a) I quattro centri sono consecutivi, come in "...010101010...". Chiamiamo n_4^a il numero di stringhe cattive con centri i, j, k, h consecutivi. Abbiamo

$$n_4^a = 3!/(1!2!) = 3.$$

Inoltre, quattro centri consecutivi possono essere presi in $M_4^a = 4$ modi in quanto la sequenza 010101010 può avere 4 diversi punti di inizio.

- (4b) Tre dei centri sono consecutivi e il quarto non lo è, come in "...0101010...010...". Chiamiamo n_4^b il numero di stringhe cattive con dati centri i, j, k, h di cui solo tre consecutivi. Abbiamo

$$n_4^b = 2!/(0!2!) = 1.$$

Sia M_4^b il numero di modi in cui si possono prendere quattro centri di cui tre consecutivi. I tre consecutivi possono essere i primi tre o gli ultimi tre. Supponiamo lo siano i primi tre e in seguito moltiplicheremo per 2 per avere il numero totale. I modi sono altrettanti che le soluzioni dell'equazione $x_1 + x_2 + x_3 = 2$, come rappresentato dalla scrittura:

$$| \leftarrow x_1 \rightarrow |0101010| \leftarrow x_2 \rightarrow |010| \leftarrow x_3 \rightarrow |$$

Abbiamo perciò $M_4^b = 2 \times \binom{4}{2} = 12$, dove il fattore 2 è dovuto al fatto che, come osservato, i tre centri consecutivi possono essere i primi tre o gli ultimi tre.

- (4c) I primi due e gli ultimi due centri sono consecutivi, ma il secondo e il terzo no, come in "...01010...01010...". Chiamiamo n_4^c il numero di stringhe cattive per dati centri i, j, k, h di cui solo i primi due e gli ultimi due sono consecutivi. Abbiamo

$$n_4^c = 2!/(0!2!) = 1.$$

Sia M_4^c il numero di modi in cui si possono prendere quattro centri di cui solo i primi due e gli ultimi due sono consecutivi. I modi sono altrettanti che le soluzioni dell'equazione $x_1 + x_2 + x_3 = 2$, come rappresentato dalla scrittura:

$$| \leftarrow x_1 \rightarrow |01010| \leftarrow x_2 \rightarrow |01010| \leftarrow x_3 \rightarrow |$$

Abbiamo perciò $M_4^c = \binom{4}{2} = 6$.

- (4d) Tutti e quattro i centri sono non consecutivi, come in "...010...010...010...010...". È facile rendersi conto di come questo caso non sia possibile (servirebbero almeno 8 zeri nella stringa).
5. (Stringhe cattive che godono di P_i, P_j, P_k, P_h e P_t per $i, j, k, h, t \in I, i < j < k < h < t$.) È facile rendersi conto di come questo caso sia possibile solo se tutti e cinque i centri sono consecutivi, come in "...01010101010...". Chiamiamo n_5 il numero di stringhe con centri in i, j, k, h, t . Abbiamo

$$n_5 = 1!/(0!1!) = 1.$$

Inoltre, detto M_5 il numero di modi di scegliere 5 centri consecutivi, abbiamo $M_5 = 2$.

Abbiamo ora tutti gli ingredienti per applicare il principio di inclusione esclusione e calcolare il numero di stringhe buone:

$$|S| - (M_1 \cdot n_1) + (M_2^a \cdot n_2^a + M_2^b \cdot n_2^b) - (M_3^a \cdot n_3^a + M_3^b \cdot n_3^b + M_3^c \cdot n_3^c) + (M_4^a \cdot n_4^a + M_4^b \cdot n_4^b + M_4^c \cdot n_4^c) - M_5 \cdot n_5$$

ossia

$$924 - (10 \cdot 126) + (8 \cdot 35 + 28 \cdot 15) - (6 \cdot 10 + 30 \cdot 4 + 20 \cdot 1) + (4 \cdot 3 + 12 \cdot 1 + 6 \cdot 1) - 2 \cdot 1$$

e quindi le stringhe buone sono in tutto

$$924 - 1260 + 700 - 200 + 30 - 2 = 192.$$

◇

Esempio. Sia A un insieme di n elementi e B un insieme di $k \leq n$ elementi. Quante sono le funzioni suriettive di A in B ?

Chiamiamo S l'insieme di tutte le funzioni di A in B . Si ha $|S| = k^n$ in quanto ogni elemento di A può avere una tra k immagini. Una funzione non è suriettiva se esistono h elementi di B , con $1 \leq h \leq k-1$, che non sono immagine di alcun elemento di A . Per ogni $i \in B$ sia P_i la proprietà definita su S , soddisfatta da quelle funzioni f per le quali $f(A) = B - \{i\}$, ossia per le quali tutti gli elementi di B tranne i sono immagine di qualche elemento di A . Diciamo che ogni funzione che gode di P_i "non tocca l'elemento i ". Diciamo inoltre che una funzione che non tocca h degli elementi di B , "lascia fuori" h elementi. In base al principio di inclusione-esclusione, le funzioni suriettive possono allora essere contate partendo da tutte le funzioni, sottraendo quelle che lasciano fuori un elemento, riaggiungendo quelle che ne lasciano fuori due, sottraendo quelle che ne lasciano fuori tre, ecc. Dato un insieme di $1 \leq h \leq k-1$ elementi di B , siano essi i_1, \dots, i_h , si ha

$$|A_{i_1} \cap \dots \cap A_{i_h}| = (k-h)^n$$

in quanto ogni elemento di A ha un'immagine che può essere scelta in $k-h$ modi. Inoltre, il numero complessivo di funzioni che lasciano fuori h elementi è

$$\sum_{i_1, \dots, i_h} |A_{i_1} \cap \dots \cap A_{i_h}| = \binom{k}{h} (k-h)^n$$

in quanto gli elementi da lasciare fuori possono essere scelti in $\binom{k}{h}$ modi. Abbiamo allora che il numero totale di funzioni suriettive di A in B è

$$k^n - \binom{k}{1} (k-1)^n + \binom{k}{2} (k-2)^n + \dots + (-1)^{k-1} \binom{k}{k-1} 1^n = \sum_{h=0}^{k-1} (-1)^h \binom{k}{h} (k-h)^n.$$

◇

ESERCIZIO 5.9. Quante funzioni suriettive esistono dall'insieme $\{5, 6, \dots, 11\}$ nell'insieme $\{A, C, G, T\}$? ◇

5.2 Spiazziamenti

Un gruppo di amici, in occasione del Natale, decide di scambiarsi i regali in modo anomalo. Ogni persona, anzichè fare un regalo a tutte le altre (troppo costoso) scrive il suo nome su un foglio di carta e lo mette in un vaso. Il vaso viene poi mescolato ed ognuno estrae un biglietto. Ogni persona dovrà fare un solo regalo, alla persona il cui nome è scritto sul biglietto che ha estratto. Sfortunatamente, qualcuno può estrarre il suo stesso nome, nel qual caso non avrà regali (a meno che non se lo compri da solo, ma allora, addio sorpresa). Ci chiediamo qual è la probabilità che ciò non accada.

Una permutazione $\pi = (\pi_1, \dots, \pi_n)$ si dice *spiazzamento** se $\pi_i \neq i$ per $i = 1, \dots, n$. Ad esempio, $(2, 1, 4, 5, 3)$ e $(3, 4, 1, 5, 2)$ sono spiazzamenti, mentre $(5, 2, 1, 3, 4)$ e $(4, 1, 3, 2, 5)$ non lo sono. Il problema degli amici corrisponde a determinare quanti sono gli spiazzamenti di n elementi. Chiamiamo questo numero Z_n .

TEOREMA 29: Per $n \geq 1$ si ha

$$Z_n = n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots + (-1)^n \frac{1}{n!} \right) \quad (5.12)$$

Dim: Sia S l'insieme di tutte le permutazioni di $\{1, \dots, n\}$. Per $i = 1, \dots, n$ sia P_i la proprietà che, in una permutazione, i è nella sua posizione originale (ossia, $\pi_i = i$). Quindi, una permutazione è uno spiazzamento se non ha alcuna delle proprietà P_1, \dots, P_n . Se A_i è l'insieme di permutazioni che hanno la proprietà P_i , abbiamo

$$Z_n = |\bar{A}_1 \cap \bar{A}_2 \cap \dots \cap \bar{A}_n|.$$

Usiamo il principio di inclusione-esclusione. Le permutazioni in A_1 sono tutte quelle che cominciano per “1”, da cui $|A_1| = (n-1)!$. Allo stesso modo, $|A_i| = (n-1)!$ per ogni i , in quanto, una volta piazzato i nella posizione i , restano $(n-1)!$ modi di piazzare i rimanenti $n-1$ elementi nelle $n-1$ rimanenti posizioni. Le permutazioni in $A_1 \cap A_2$ sono quelle in cui 1 è al primo posto e 2 è al secondo. I rimanenti $n-2$ elementi possono essere ordinati in tutti i modi. Si ottiene $|A_1 \cap A_2| = (n-2)!$, e, similmente, $|A_i \cap A_j| = (n-2)!$, per ogni $1 \leq i < j \leq n$. Proseguendo allo stesso modo, si ha, in generale,

$$|A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_k}| = (n-k)!$$

per ogni $1 \leq i_1 < i_2 < \dots < i_k \leq n$. Siccome ci sono $\binom{n}{k}$ scelte di k indici $1 \leq i_1 < i_2 < \dots < i_k \leq n$, dal principio di inclusione-esclusione abbiamo

$$Z_n = n! - \binom{n}{1}(n-1)! + \binom{n}{2}(n-2)! - \binom{n}{3}(n-3)! + \dots + (-1)^n \binom{n}{n}(n-n)!$$

*In Inglese, *derangement*.

Dalla definizione di coefficiente binomiale segue che, per ogni $1 \leq k \leq n$, $\binom{n}{k}(n-k)! = \frac{n!}{k!}$, per cui si ottiene

$$Z_n = n! - \frac{n!}{1!} + \frac{n!}{2!} - \frac{n!}{3!} + \cdots + (-1)^n \frac{n!}{n!}$$

Raggruppando $n!$ si ha

$$Z_n = n! \left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n \frac{1}{n!} \right).$$



Ricordando dall'analisi che lo sviluppo in serie di e^{-1} è

$$e^{-1} = 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} + \cdots \quad (5.13)$$

abbiamo che

$$Z_n \simeq \frac{n!}{e}. \quad (5.14)$$

Questo risultato è tanto più accurato quanto più grande è n , ma non è necessario che n sia molto grande per avere già una buona approssimazione. Infatti, troncando lo sviluppo di $\frac{1}{e}$ in (5.13) al termine n , si ottiene un'approssimazione di $\frac{1}{e}$ molto vicina al valore corretto (corretta in almeno 3 cifre decimali) già per $n = 7$. Da un punto di vista pratico, possiamo concludere che la frazione di permutazioni che sono spiazzeamenti è $\frac{1}{e}$ del totale. Quindi la probabilità che nessuno degli amici dell'esempio estragga il suo stesso nome è (circa) $\frac{1}{e}$. È curioso il fatto che questa probabilità non dipenda da n e resti sostanzialmente la stessa sia che gli amici siano 10, sia che siano 100000.

ESERCIZIO 5.10. Ad una festa ci sono 10 uomini e 10 donne. In quanti modi gli uomini possono scegliere una compagna per il primo ballo? In quanti modi per il secondo ballo, nell'ipotesi che ognuno debba cambiare partner? \diamond

ESERCIZIO 5.11. Uno studente viene a sapere che in un test a scelta multipla, la risposta esatta ad ogni domanda ha un numero sempre diverso. Ci sono 6 domande, ognuna con 6 risposte a scelta, e lo studente non ha studiato nulla, per cui risponde sostanzialmente a caso. Qual è la sua strategia migliore (che massimizza il numero di risposte esatte) tra (i) rispondere sempre "1" (ii) tirare un dado ad ogni domanda e dare la risposta corrispondente al numero che esce (iii) scegliere a caso una permutazione dei numeri $\{1, \dots, 6\}$ e rispondere seguendo tale permutazione. Si generalizzi tale problema al caso generico di n domande, con n scelte per risposta. \diamond

Per gli spiazzeamenti valgono le seguenti due formule ricorsive:

$$Z_n = (n-1)(Z_{n-2} + Z_{n-1}) \quad (5.15)$$

$$Z_n = nZ_{n-1} + (-1)^n. \quad (5.16)$$

Dimostriamo la (5.15). Sia $n \geq 3$ e consideriamo gli spiazamenti di n elementi. Questi possono essere partizionati in $n - 1$ classi, a seconda che il numero $2, 3, \dots, n$ occupi il primo posto della permutazione. Sia z_n il numero di spiazamenti che cominciano con l'elemento "2" (che è poi lo stesso del numero di spiazamenti che cominciano per $i = 3, 4, \dots, n$). Si ha perciò:

$$Z_n = (n - 1)z_n. \quad (5.17)$$

Ora, gli spiazamenti che cominciano per "2" possono a loro volta essere divisi in due gruppi: quelli che hanno "1" come secondo elemento, e quelli che hanno un numero $\pi_2 \neq 1$ come secondo elemento. I primi sono del tipo

$$2 \ 1 \ \pi_3 \ \pi_4 \ \dots \ \pi_n$$

con $p_i \neq i$ per $i = 3, 4, \dots, n$, e ce ne sono in tutto Z_{n-2} (vengono "spiazzati" $n - 2$ elementi). Gli altri sono del tipo

$$2 \ \pi_2 \ \pi_3 \ \pi_4 \ \dots \ \pi_n$$

con $p_2 \neq 1$, $p_i \neq i$ per $i = 3, 4, \dots, n$, e ce ne sono in tutto Z_{n-1} . Quindi, $z_n = Z_{n-2} + Z_{n-1}$. Sostituendo nella (5.17), si ottiene la (5.15).

Dimostriamo ora la (5.16). Sviluppando la (5.15) e riarrangiando i termini, si ha

$$Z_n - nZ_{n-1} = -(Z_{n-1} - (n - 1)Z_{n-2}).$$

Si noti che, a destra dell'uguale, c'è un'espressione analoga a quella che appare a sinistra, solo che $(n - 1)$ ha preso il posto di n . Ripetendo il passaggio, questa volta per l'espressione a destra, si ottiene

$$Z_n - nZ_{n-1} = -(-(Z_{n-2} - (n - 2)Z_{n-3})).$$

Proseguendo fino all'apparire del caso base (ossia $Z_2 = 1$ e $Z_1 = 0$), si ricava che

$$Z_n - nZ_{n-1} = (-1)^{n-2}(Z_2 - 2Z_1) = (-1)^{n-2}.$$

Quindi, segue che $Z_n = nZ_{n-1} + (-1)^{n-2}$, che è esattamente la formula (5.16), in quanto $(-1)^{n-2} = (-1)^n$.

Le formule (5.15) e (5.16) dimostrano ancora una volta lo strettissimo legame tra gli spiazamenti e le permutazioni in generale. Infatti, esistono formule analoghe relative al numero di permutazioni, che qui riportiamo:

$$\begin{aligned} n! &= (n - 1)((n - 2)! + (n - 1)!) \\ n! &= n(n - 1)! \end{aligned}$$

ESERCIZIO 5.12. Si dimostri che

$$n! = (n - 1)((n - 2)! + (n - 1)!)$$

◇

Chapter 6

Procedure combinatoriche

6.1 Matrimoni stabili

Consideriamo la seguente situazione. È dato un insieme di n uomini ed un insieme di n donne. Ogni uomo esprime il suo ordine di preferenza per le n donne, rappresentato da una permutazione delle stesse, e viceversa. Si tratta di trovare un *matching (accoppiamento) stabile*, consistente in n matrimoni mutualmente “solidi”. La condizione di solidità dei matrimoni è la seguente: non devono esistere un uomo e una donna, non sposati fra loro, che si preferiscano a vicenda rispetto ai loro attuali consorti (in tale caso, ci sarebbe il rischio che scappino insieme).

Ad esempio, indicando gli uomini con lettere minuscole e le donne con lettere maiuscole, le liste di preferenze potrebbero essere le seguenti:

$$\begin{array}{lll} a : & A & B & C \\ b : & B & A & C \\ c : & A & C & B \end{array} \qquad \begin{array}{lll} A : & b & a & c \\ B : & c & b & a \\ C : & a & c & b \end{array}$$

Supponiamo che si sposino le coppie $\{aB, bC, cA\}$. Questo matching non sarebbe stabile, in quanto i matrimoni di a e A sono a rischio. Infatti, a preferisce A a B e A preferisce a a c . Quindi a e A scapperebbero insieme. Il matching $\{aA, bB, cC\}$ è invece stabile, ed è facile convincersene. Infatti, a e b non potrebbero sperare in una sposa migliore, mentre c potrebbe aspirare alla mano di A , la quale però non sarebbe disposta allo scambio.

Il principale risultato di questa sezione è quello di dimostrare che, date le liste di preferenze, un matching stabile *esiste sempre*. Lo dimostreremo in maniera costruttiva, tramite un algoritmo che crea un matching stabile.

ALGORITMO DEL MATCHING STABILE (AMS)

1. Ad ogni persona si associ la lista delle sue preferenze. Inizialmente, nessuno è *cancellato* da tale lista, ma, man mano che l'algoritmo procede, dalle liste vengono cancellate persone.

2. Per ciascun uomo m , si esegua **PROPONI**(m), definita sotto.

PROPONI(m):

Sia W la *prima* donna non ancora cancellata dalla lista delle preferenze di m .

Si esegua **DECIDI**(W, m), definita sotto

DECIDI(W, m):

Sia m' il partner attuale di W (ammesso che esista). Se W preferisce m' a m , allora lei rifiuta m , nel qual caso:

(a) si cancelli m dalla lista di W e W dalla lista di m ;

(b) Si esegua **PROPONI**(m) (si noti che ora m si proporrà a qualcun'altra.)

Altrimenti, W accetta l'offerta di m e si mette con lui, mandando a spasso, se c'era, m' . In questo caso

(a) si cancelli m' dalla lista di W e W dalla lista di m' ;

(b) Si esegua **PROPONI**(m') (si noti che ora m' si proporrà a qualcun'altra.)

Si noti che, abbastanza realisticamente, sono le donne a scegliere e gli uomini a doversi dar da fare nel proporsi. La vendetta degli uomini viene però consumata dal fatto che, come dimostreremo fra poco, la soluzione trovata è *maschio-ottima* e *femmina-pessima*. Vale a dire, l'algoritmo determina per ogni uomo la sposa migliore a cui potesse aspirare in qualsiasi matching stabile, e per ogni donna lo sposo peggiore che si potesse aspettare in qualsiasi matching stabile.

Consideriamo un esempio di esecuzione dell'algoritmo sulla seguente lista di preferenze:

$a:$	D	A	C	B	$A:$	a	c	d	b
$b:$	A	C	D	B	$B:$	d	a	b	c
$c:$	C	D	B	A	$C:$	c	b	d	a
$d:$	D	A	C	B	$D:$	b	d	c	a

Inizialmente, a si propone a D , che accetta. Poi b si propone a A , che accetta, e c si propone a C , che accetta. A questo punto, d si propone a D e scoppia il pandemonio. D accetta la proposta di d e molla a . a allora prova a proporsi ad A , che accetta e molla b . b si propone a C , ma C lo rifiuta, sicchè b si propone a D . D ci sta e molla d che prova a proporsi ad A . A non accetta, e d prova a proporsi a C che pure non accetta. Infine, d si propone a B , che accetta. Il matching determinato è quindi $\{aA, bD, cC, dB\}$. Si noti che può succedere che qualcuno venga accoppiato alla sua ultima scelta (ad esempio, d), e nonostante questo, il matching sia stabile.

Dimostriamo ora che la procedura AMS termina sempre e che, alla terminazione, ha determinato un matching stabile. Per il primo punto, si noti che nessun uomo può proporsi mai due volte alla stessa donna, mentre, se l'algoritmo proseguisse all'infinito, questo necessariamente dovrebbe accadere. Inoltre, non è possibile che al termine dell'algoritmo un uomo x e una donna Y restino senza partner. Infatti, ogni uomo scandisce la sua lista e quindi x si sarebbe proposto, prima o poi, a Y , la quale avrebbe accettato (e, da allora in poi, Y non sarebbe più potuta tornare "single").

Ora, veniamo al punto interessante e dimostriamo che il matching è stabile. Supponiamo per assurdo che non lo sia. Allora, dovrebbe esistere una coppia aB , non sposati fra loro, tali che sia a che B si preferiscono a vicenda rispetto ai loro attuali sposi. Supponiamo che questi siano A e b rispettivamente (ossia che l'algoritmo

abbia creato i matrimoni aA e bB). Siccome a preferisce B ad A , ma è finito con lo sposarsi A , vuol dire che c'è stato un momento in cui a si è proposto a B , ma è stato rifiutato. Questo vorrebbe dire che, in quel momento, B era fidanzata con qualcuno, diciamo c , per lei meglio di a . Per come funziona l'algoritmo, B non accetta mai un fidanzato peggiore e quindi alla fine B dovrebbe essere sposata con qualcuno non peggiore di c . Ma lo sposo trovato dall'algoritmo, b , è peggiore di a e quindi anche di c . Assurdo.

Dimostriamo ora che l'algoritmo AMS è *maschio-ottimo*: vale a dire che, per ogni coppia xY creata dall'algoritmo, non esiste alcun matching stabile in cui x è sposato a una donna che lui preferisce a Y . Siccome nel corso dell'algoritmo ogni uomo scandisce la sua lista in ordine di preferenza decrescente, l'affermazione di cui sopra è equivalente a questa: se una donna W viene cancellata dalla lista di un uomo m , non esiste alcun matching stabile che contenga la coppia mW . Dimostriamo questa affermazione per assurdo, facendo vedere che, se così non fosse, esisterebbe un matching stabile con un numero infinito di coppie.

Supponiamo allora che W venga cancellata dalla lista di m nel corso dell'algoritmo AMS, ma che lo stesso esista un matching stabile \mathcal{S} che contiene la coppia mW . Al tempo t , subito dopo la cancellazione di W dalla lista di m (e di m da quella di W), si aveva che W doveva essere fidanzata con un uomo m' per lei preferibile a m . Sia W' la sposa di m' nel matching \mathcal{S} . Siccome \mathcal{S} è stabile, m' deve preferire W' a W (altrimenti m' e W scapperebbero insieme). Però l'algoritmo AMS aveva creato il fidanzamento $m'W$ e quindi, in quel momento, W' era già stata cancellata dalla lista di m' . Questo implica che, in aggiunta alla coppia mW , cancellata da AMS ma presente in \mathcal{S} , abbiamo ora trovato anche la coppia $m'W'$ cancellata da AMS ma presente in \mathcal{S} . Inoltre la cancellazione di $m'W'$ è avvenuta a un tempo $t' < t$. Ma allora lo stesso ragionamento potrebbe essere ripetuto con $m'W'$ al posto di mW , dando luogo a una nuova coppia $m''W''$ cancellata da AMS, ad un tempo $t'' < t' < t$, ma presente in \mathcal{S} . Siccome gli istanti di cancellazione delle coppie così create sono tutti diversi fra loro, tutte queste coppie dovrebbero essere diverse. Ma allora \mathcal{S} conterrebbe un numero infinito di coppie. Assurdo.

Dimostriamo ora che la soluzione trovata è *femmina-pessima*, in quanto non c'è alcun matching stabile in cui una donna possa essere sposata a qualcuno per lei peggiore del partner assegnatole da AMS. Supponiamo per assurdo che W possa essere sposata, in un matching stabile \mathcal{S} , con m' che per lei è peggiore di m , il partner assegnatole da AMS. Siccome AMS è maschio-ottimo, m preferisce W a qualsiasi altra donna in un matching stabile. Quindi m e W scapperebbero insieme in \mathcal{S} che non potrebbe essere stabile.

Consideriamo ora il caso di *liste di preferenze parziali*. In questo caso, può succedere che una persona decida di non volere sposarsi a tutti i costi, ma preferisca rimanere single piuttosto che sposare determinate altre persone. Si tratta tutto sommato di un'ipotesi verosimile. Si noti che in caso di liste parziali potrebbe non esistere alcun matching stabile, ed anzi, non esistere neppure alcun matching completo (si pensi ad esempio a una persona che non voglia sposare nessun altro). Descriviamo allora un metodo per determinare, se esiste, un matching stabile per un insieme di liste parziali, o per affermare con certezza che un tale matching stabile non è possibile. L'idea è quella di introdurre due “fantocci”, uno maschio \hat{m} e una femmina, \hat{W} , che fungeranno da separatori fra le persone con cui ci si vuole oppure no sposare. Faremo in modo di riportarci a una situazione di liste complete, aggiungendo i fantocci alla fine delle liste parziali che vengono poi completate arbitrariamente, e creando delle liste di preferenza anche per i fantocci. Tali liste possono essere arbitrarie, a patto che \hat{W} sia l'*ultima* preferenza di \hat{m} e \hat{m} sia l'*ultima* preferenza di \hat{W} . Per esempio, date le seguenti liste parziali:

$$\begin{array}{ll}
a: & D \quad A \\
b: & A \quad C \quad D \\
c: & C \\
d: & D \quad A \quad C \quad B
\end{array}
\qquad
\begin{array}{ll}
A: & a \quad c \\
B: & d \quad a \quad b \\
C: & c \\
D: & b \quad d \quad c \quad a
\end{array}$$

un completamento possibile è il seguente:

$$\begin{array}{ll}
a: & D \quad A \quad \hat{W} \quad C \quad B \\
b: & A \quad C \quad D \quad \hat{W} \quad B \\
c: & C \quad \hat{W} \quad A \quad B \quad D \\
d: & D \quad A \quad C \quad B \quad \hat{W} \\
\hat{m}: & A \quad B \quad C \quad D \quad \hat{W}
\end{array}
\qquad
\begin{array}{ll}
A: & a \quad c \quad \hat{m} \quad d \quad b \\
B: & d \quad a \quad b \quad \hat{m} \quad c \\
C: & c \quad \hat{m} \quad b \quad d \quad a \\
D: & b \quad d \quad c \quad a \quad \hat{m} \\
\hat{W}: & a \quad b \quad c \quad d \quad \hat{m}
\end{array}$$

Passiamo ora a dimostrare che le liste parziali ammettono un matching stabile se e solo se esiste un matching stabile delle liste complete in cui \hat{m} è sposato a \hat{W} .

(\Rightarrow) Dato un matching stabile sulle liste parziali, lo si può completare aggiungendo la coppia $\hat{m}\hat{W}$. Si noti che la coppia aggiunta non può rendere il matching non stabile, in quanto ognuno preferisce il suo sposo vero a uno sposo fantoccio.

(\Leftarrow) Consideriamo ora un matching delle liste totali, che comprenda la coppia $\hat{m}\hat{W}$. Rimuovendo tale coppia si ottiene un matching sui rimanenti elementi. Vogliamo vedere che in tale matching ognuno è accoppiato con qualcuno con cui voleva veramente sposarsi. Supponiamo ad esempio di considerare una coppia xY del matching. Se x avesse preferito \hat{W} a Y (ossia se Y fosse una delle donne con cui x non era disposto a sposarsi) allora il matching non sarebbe stato stabile, perchè x sarebbe scappato con il fantoccio \hat{W} in quanto anche \hat{W} preferisce \hat{x} a \hat{m} . (Un discorso perfettamente analogo vale per il caso in cui x fosse stato un uomo con cui Y non era disposta a sposarsi).

Concludiamo la sezione considerando il caso generale, in cui le preferenze non sono espresse tra maschi e femmine, ma all'interno di un unico gruppo di persone il cui genere non ha importanza. In questo caso, dati n elementi, ad ognuno associamo la lista delle preferenze sui rimanenti $n - 1$. Ad esempio, dato un gruppo di n persone e dovendo accoppiarle per un torneo di doppio a tennis, ognuno esprime le sue preferenze per il potenziale partner. Ci chiediamo ancora se esista un matching stabile.

Consideriamo, per esempio, il caso

$$\begin{array}{ll}
A: & B \quad C \quad D \\
B: & A \quad C \quad D \\
C: & A \quad D \quad B \\
D: & C \quad A \quad B
\end{array}$$

che ammette il matching stabile $\{AB, CD\}$. Sfortunatamente, per il caso generale in cui ognuno esprime le preferenze rispetto a tutti gli altri, non esiste una procedura tipo AMS. In effetti, non è noto alcun modo efficiente per verificare se esista un matching stabile, visto che il metodo di provare tutti i possibili matching, pur funzionando, non può senz'altro essere considerato efficiente. Per esercizio, si trovino delle liste di preferenze per 4 persone tali che non esista alcun matching stabile.

6.2 Generazione di strutture random

In questa sezione consideriamo il problema di generare un oggetto combinatorio (quale un sottoinsieme, o una disposizione, ecc.) secondo una distribuzione uniforme. Ossia, se esistono N di tali oggetti, la probabilità di selezionarne uno in particolare deve risultare $1/N$. Nel descrivere gli algoritmi useremo uno pseudo-linguaggio di programmazione. Assumiamo che la procedura

`rndint(a, b)`

sia disponibile nel linguaggio e che, dati due numeri interi a e b , restituisca un intero casuale x , con $a \leq x \leq b$ (ossia distribuito uniformemente fra a e b).

6.2.1 Insiemi

Dato l'insieme $S = \{1, 2, \dots, n\}$, consideriamo il problema di generare un sottoinsieme casuale A di S . Questo può essere ottenuto lanciando in aria una moneta n volte, e, ad ogni lancio i in cui esce “testa”, includendo i nel sottoinsieme casuale (Algoritmo 2).

Algorithm 2 RANDOMSUBSET

```

1.  $A := \emptyset$ ;
2. for  $i := 1$  to  $n$  do
3.   if rndint(0,1) = 1 then
4.      $A := A \cup \{i\}$ ;
5. endfor
```

Per dimostrare che A è effettivamente casuale, consideriamo un qualsiasi sottoinsieme B di S e facciamo vedere che la probabilità che $A = B$ è $1/2^n$. Sia ad esempio $B = \{3, 5, 6\}$ (per esercizio lo studente generalizzi l'esempio ad un caso qualsiasi). Allora $A = B$ se il lancio della moneta ha dato “testa” ai tentativi 3, 5 e 6, e “croce” ai rimanenti $n - 3$ tentativi. Siccome ogni lancio è indipendente dagli altri, la probabilità che ciò avvenga è

$$Prob(\text{testa})^3 \times Prob(\text{croce})^{n-3}$$

che, essendo $Prob(\text{testa}) = Prob(\text{croce}) = 1/2$, è pari a $1/2^n$.

Consideriamo ora il problema di generare un sottoinsieme di una data cardinalità k prefissata. Analizziamo prima una soluzione errata. L'idea potrebbe essere quella di procedere come nell'esempio precedente, ossia lanciando la moneta (virtuale) e interrompendo il processo non appena siano state ottenute k “teste”. Esiste anche la possibilità che al termine di un ciclo sugli n elementi non siano state ottenute k teste, nel qual caso bisognerà ritentare l'intero processo una nuova volta (si veda l'algoritmo 3).

È facile riconoscere il problema dell'algoritmo 3: i sottoinsiemi generati non seguono la distribuzione uniforme. Per accorgersene, basta considerare il caso $k = 1$ e chiedersi qual'è la probabilità di generare il sottoinsieme $\{n\}$. Questa probabilità è pari a $1/2^n$ (e quindi bassissima), in quanto tale sottoinsieme viene creato solo quando i primi $n - 1$ lanci della moneta forniscono “croce” e l'ultimo fornisce “testa”. D'altro canto, la probabilità di generare il sottoinsieme $\{1\}$ è $1/2$. Si vede quindi che questi insiemi non sono generati con la stessa probabilità come invece dovrebbe avvenire. Non solo: entrambe le probabilità sono

Algorithm 3 RANDOM k -SUBSETWRONG

```

1. repeat
2.    $A := \emptyset$ ;
3.   for  $i := 1$  to  $n$  do
4.     if  $\text{rndint}(0,1) = 1$  then
5.        $A := A \cup \{i\}$ ;
6.       if  $|A| = k$  then exit for loop
7.     endif;
8.   endfor;
9. until  $|A| = k$ .

```

sbagliate, in quanto la probabilità di ogni siffatto sottoinsieme dovrebbe risultare pari a $1/n$. Nella sezione 6.2.2 descriveremo il modo corretto di generare un k -sottoinsieme con distribuzione uniforme.

ESERCIZIO 6.1. Si consideri un numero in base 2 di n bit come rappresentante un insieme (l'insieme delle posizioni in cui i bit valgono "1"). Si discuta pertanto un modo di generare sottoinsiemi casuali di $\{1, \dots, n\}$ tramite la generazione di numeri casuali da interpretarsi poi in base 2. \diamond

6.2.2 Permutazioni e disposizioni

Consideriamo il problema di generare una k -disposizione, ossia un ordinamento di k numeri diversi presi fra 1 e n , in modo casuale. L'idea è quella di cominciare generando un numero casuale d_1 , compreso tra 1 e n . Poi, si genera un numero casuale d_2 , compreso tra 1 e n , ma diverso da d_1 . Al generico passo i -esimo, si genera un numero d_i con $1 \leq d_i \leq n$ e $d_i \neq d_1, d_2, \dots, d_{i-1}$. Per essere sicuri di non generare un numero già generato in precedenza, utilizziamo un vettore $v[]$ e un contatore **left**, facendo in modo che gli elementi $v[1], v[2], \dots, v[\text{left}]$ siano, in ogni momento, tutti e soli i numeri che non sono ancora stati utilizzati, e quindi sono disponibili. Chiamiamo poi $p[1, \dots, k]$ il vettore che costruiamo, e che, al termine, conterrà la disposizione casuale.

Algorithm 4 RANDOM k -PERM

```

1. for  $i:=1$  to  $n$  do  $v[i] := i$ ; /* inizializzazione */
2. left :=  $n$ ;
3. for  $i:=1$  to  $k$  do
4.    $\text{pos} := \text{rndint}(1, \text{left})$ ;
5.    $p[i] := v[\text{pos}]$ ;
6.    $v[\text{pos}] := v[\text{left}]$ ;
7.    $\text{left} := \text{left} - 1$ ;
8. endfor

```

Al passo 4 viene generata la posizione di un elemento di $v[]$ compreso tra 1 e **left**. Siccome questi elementi sono tutti e soli i numeri disponibili, viene in pratica generato un numero casuale (vale a dire $v[\text{pos}]$) tra quelli disponibili. Tale numero viene copiato in $p[]$ al passo 5. Ai passi 6 e 7 si fa poi in modo da mantenere in $v[1..left]$ sempre e soli i numeri ancora disponibili, sovrascrivendo $v[\text{pos}]$ (già usato) con

`v[left]` e decrementando `left`.

Per quel che riguarda la distribuzione di probabilità, consideriamo una specifica disposizione, ad esempio (b_1, b_2, \dots, b_k) e chiediamoci qual è la probabilità di generarla. Si avrà $p[1] = b_1$ con probabilità $1/n$. Una volta posto $p[1] := b_1$, la probabilità che $p[2] = b_2$ è $1/(n-1)$ in quanto $p[2]$ viene scelto fra $n-1$ elementi, che comprendono b_2 . Continuando, la probabilità che $p[3] = b_3$, dati $p[1] = b_1$ e $p[2] = b_2$ è $1/(n-2)$. Dal prodotto di queste probabilità si ottiene

$$Prob(\text{generare } (b_1, b_2, \dots, b_k)) = \frac{1}{n} \times \frac{1}{n-1} \times \dots \times \frac{1}{n-k+1} = \frac{1}{D(n, k)}$$

e quindi la distribuzione è uniforme.

Rispondiamo ora al quesito su come generare un sottoinsieme di cardinalità k in maniera uniforme. Per fare ciò basta utilizzare l'algoritmo 4, e considerare l'insieme dei k elementi nella disposizione generata (ossia, prendere la disposizione, ma ignorando l'ordine). Ad esempio, se la disposizione casuale generata risulta $(3, 1, 5)$, questa verrà interpretata come l'insieme $\{1, 3, 5\}$. Lo stesso insieme si avrebbe anche nel caso fosse stata generata la disposizione $(5, 3, 1)$, eccetera. Per vedere che gli insiemi vengono generati con distribuzione uniforme, chiediamoci qual è la probabilità di generare uno specifico k -insieme $\{b_1, b_2, \dots, b_k\}$. Questo insieme viene indotto dalle $k!$ permutazioni possibili dei suoi elementi, ossia da $k!$ disposizioni, ognuna di probabilità $1/D(n, k)$. Otteniamo che

$$Prob(\text{generare } \{b_1, b_2, \dots, b_k\}) = k! \times \frac{1}{D(n, k)} = \frac{1}{\binom{n}{k}}$$

e quindi la distribuzione è uniforme.

Infine, consideriamo il problema di generare una permutazione casuale, in maniera uniforme. Banalmente, essendo ogni permutazione anche una n -disposizione, basterà utilizzare l'algoritmo 4 con $k = n$.

6.3 Enumerazione completa

Consideriamo ora il problema di enumerare tutte le strutture combinatorie di un certo tipo (ad esempio sottoinsiemi e permutazioni). Per questo problema esistono tipicamente due soluzioni, la soluzione *ricorsiva* e la soluzione *iterativa*. La soluzione ricorsiva genera tutte le strutture di dimensione n a partire da tutte le strutture di dimensione $n-1$. Se realizzato con un programma su un calcolatore, questo modo di procedere implica la necessità di una enorme quantità di memoria, in quanto tutte le strutture devono essere memorizzate contemporaneamente. Quindi, servirà una memoria proporzionale a 2^n per contenere tutti i sottoinsiemi di un insieme di n elementi, e proporzionale a $n!$ per contenerne tutte le permutazioni. Anche per valori modesti di n , queste quantità risultano proibitive.

Nella soluzione iterativa, invece, le strutture vengono implicitamente ordinate, sicchè ne esiste una *prima* e una *ultima*. Se siamo in grado, data l' i -esima struttura dell'ordine, di creare a partire da essa la $(i+1)$ -esima, la i -esima può poi essere cancellata. Pertanto, la memoria necessaria è solo quella che basta per contenere due strutture (quella corrente e la successiva) e quindi è proporzionale a n .

6.3.1 Generare tutti i sottoinsiemi

Sia $S = \{1, \dots, n\}$. Vogliamo elencare tutti i suoi sottoinsiemi. Consideriamo prima la soluzione ricorsiva:

1. Si generino tutti i sottoinsiemi di $\{1, \dots, n-1\}$. Sia A l'insieme di questi sottoinsiemi.
2. Si crei un insieme A' di sottoinsiemi, ottenuti aggiungendo l'elemento n a ogni insieme di A (ossia, $A' := \{B \cup \{n\} \mid B \in A\}$).
3. I sottoinsiemi di S sono allora dati da $A \cup A'$.

Il passo 1 può essere eseguito ricorsivamente, e corrisponde al passaggio induttivo nelle dimostrazioni per induzione. Se $n-1 > 0$ il passo implica che si deve utilizzare lo stesso procedimento per calcolare A . Se invece $n-1 = 0$, allora basta porre $A = \emptyset$.

Consideriamo ora la soluzione iterativa. Si identifichi un sottoinsieme B di S con una sequenza di valori booleani:

$$(b_1, b_2, \dots, b_n)$$

dove $b_i = \text{VERO}$ se $i \in B$ e $b_i = \text{FALSO}$ altrimenti.

Definiamo $b_\alpha = (\text{FALSO}, \text{FALSO}, \dots, \text{FALSO})$ come il primo sottoinsieme, e $b_\omega = (\text{VERO}, \text{VERO}, \dots, \text{VERO})$ come l'ultimo. Dato un sottoinsieme (b_1, b_2, \dots, b_n) che non sia l'ultimo, per calcolarne il successivo, chiamiamolo $(b'_1, b'_2, \dots, b'_n)$, si proceda come segue:

1. Si trovi $1 \leq j \leq n$ tale che $b_j = \text{FALSO}$ e $b_i = \text{VERO}$ per $i = j+1, \dots, n$.
2. Si ponga $b'_k := b_k$ per $k = 1, \dots, j-1$ e $b'_k := \neg b_k$ per $k = j, \dots, n$.

ESERCIZIO 6.2. Si rifletta sul fatto che il procedimento iterativo descritto corrisponde a generare i numeri da 0 a $2^n - 1$ in base 2. \diamond

6.3.2 Generare tutte le permutazioni

Sia $S = \{1, \dots, n\}$. Vogliamo elencare tutte le permutazioni dei suoi elementi. Consideriamo prima la soluzione ricorsiva:

1. Si generino tutte le permutazioni di $\{1, \dots, n-1\}$. Sia A l'insieme di queste permutazioni.
2. Per ogni permutazione $\pi = (\pi_1, \pi_2, \dots, \pi_{n-1}) \in A$ si crei un insieme $A(\pi)$, contenente n permutazioni dei numeri $\{1, \dots, n\}$, in questo modo: si introduce n in tutte le posizioni possibili fra gli elementi di π , ossia $A(\pi) =$

$$\{(n, \pi_1, \pi_2, \dots, \pi_{n-1}), (\pi_1, n, \pi_2, \dots, \pi_{n-1}), (\pi_1, \pi_2, \dots, n, \pi_{n-1}), (\pi_1, \pi_2, \dots, \pi_{n-1}, n)\}$$

3. Tutte le permutazioni di S sono allora date dall'unione degli $A(\pi)$ per tutti i $\pi \in A$.

Il passo 1 può essere eseguito ricorsivamente. Se $n - 1 > 1$ il passo implica che si deve utilizzare lo stesso procedimento per calcolare A . Se invece $n - 1 = 1$, allora basta porre $A = \{(1)\}$.

Consideriamo ora la soluzione iterativa. Questa soluzione è basata sull'ordine degli elementi. Se ad esempio S fosse $\{A, B, C\}$, le permutazioni in ordine alfabetico sarebbero

$$\{(A, B, C), (A, C, B), (B, A, C), (B, C, A), (C, A, B), (C, B, A)\}.$$

Siccome le permutazioni possono riguardare oggetti generici (nel nostro caso i numeri $1, \dots, n$) l'ordine alfabetico non è necessariamente definito, e al suo posto usiamo l'ordine lessicografico, in base al quale, ad esempio, $(3, 5, 1, 6, 4)$ precede $(3, 5, 11, 0)$ e (B, C, F) precede (B, F, A, A) . Le permutazioni di $\{1, 2, 3\}$, in ordine lessicografico sono

$$(1, 2, 3), (1, 3, 2), (2, 1, 3), (2, 3, 1), (3, 1, 2), (3, 2, 1).$$

Siano $\pi_\alpha = (1, 2, \dots, n)$ la prima permutazione, e $\pi_\omega = (n, n - 1, \dots, 2, 1)$ l'ultima. Data una permutazione $(\pi_1, \pi_2, \dots, \pi_n)$ che non sia l'ultima, per calcolarne la successiva, chiamiamola $(\pi'_1, \pi'_2, \dots, \pi'_n)$, si proceda come segue:

1. Si trovi $1 \leq r \leq n$ tale che $\pi_{r+1} > \pi_{r+2} > \dots > \pi_n$ e $\pi_r < \pi_{r+1}$ (i.e., si determini la sequenza massimale decrescente al termine della permutazione)
2. Si determini un indice l , con $r + 1 \leq l \leq n$, tale che $\pi_l > \pi_r$ e $\pi_{l+1} < \pi_r$ (i.e., π_l è il più piccolo numero maggiore di π_r all'interno della sequenza decrescente)
3. Si scambino fra loro, nella permutazione π , gli elementi π_l e π_r : $\pi_l \leftrightarrow \pi_r$.
4. Per $i = 1, \dots, r$, si ponga $\pi'_i := \pi_i$, mentre per $i = r + 1, \dots, n$, si ponga $\pi'_i = \pi_{n+(r+1-i)}$ (in pratica, si "rovescia" la striscia di elementi tra l' $(r + 1)$ -mo e l'ultimo, ottenendo così che ora siano in ordine crescente).

Ad esempio, la permutazione immediatamente successiva a

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

è

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

In questo esempio, $r = 5$ ($\pi_r = 4$) e $l = 8$ ($\pi_l = 6$).

ESERCIZIO 6.3. Si dimostri formalmente che π' ottenuta con il procedimento descritto è la permutazione che immediatamente segue π nell'ordine lessicografico, ossia che non esiste una permutazione σ che segue π ma precede π' . \diamond

Chapter 7

Teoria dei grafi

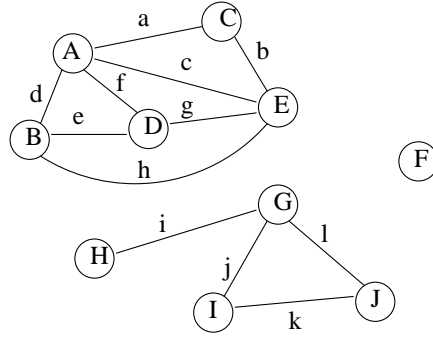
Un *grafo* è un oggetto matematico con cui si può rappresentare una relazione binaria su un insieme di elementi. Tale relazione può essere simmetrica (dando origine a un grafo *non orientato*), o asimmetrica (dando origine a un grafo *orientato*). Come esempio del primo caso, si pensi alla relazione “ i ha un genitore in comune con j ”, definita su un insieme di persone, oppure “ i è amico di j ” (anche se quest’ultima, più realisticamente, non è necessariamente una relazione simmetrica). Nel secondo caso, gli elementi possono essere alcuni incroci di una città, e la relazione del tipo “esiste una strada percorribile nel senso che va dall’incrocio a all’incrocio b ”. Oppure, su un insieme di persone, la relazione “ a è figlio di b ”. La *Teoria dei Grafi* è la disciplina che studia i grafi e loro proprietà fondamentali. Grazie ad essa, si conoscono algoritmi e teoremi che ci permettono di rispondere a domande quali “esiste un percorso (sequenza di vie) per andare da un incrocio x a un incrocio y in una città senza mai violare un senso unico?” o “la persona x è un antenato della persona y ?” o “in un gruppo di n persone, esistono k persone tali che ciascuno di loro conosce gli altri $k - 1$?” ed altre simili.

7.1 Grafi non orientati

Un *grafo non orientato* (o semplicemente *grafo*, qualora non ci sia pericolo di confusione) è definito da una coppia $G = (V, E)$ di insiemi finiti, dove V è detto l’insieme dei *vertici* (o *nodì*) e E l’insieme dei *lati* (o *archi*). Le iniziali sono dovute ai termini inglesi **V**ertex e **E**dge. Un lato è una coppia non ordinata di vertici, che indicheremo con ij ($= ji$), dove i e j appartengono a V e $i \neq j$.

Due vertici $i, j \in V$ si dicono *adiacenti* se il lato $e = ij$ appartiene ad E . In tal caso si dice che e è *incidente* in i e in j (o che e *collega* i e j), e questi ultimi si dicono anche gli *estremi* di e . Due lati si dicono *adiacenti* se sono incidenti in un medesimo vertice.

Il *grado* di un vertice v di G , denotato con $d_G(v)$ (o, più semplicemente con $d(v)$ qualora non ci sia pericolo di confusione) è il numero di archi incidenti in v . Un grafo si dice *regolare* se $d(i) = d(j)$ per ogni $i, j \in V$. In particolare, il grafo si dice k -regolare se $d(i) = d(j) = k$ per ogni $i, j \in V$. Un vertice di grado 0 si dice *isolato*. In figura 7.1 vediamo rappresentato un grafo che chiameremo G^* e che useremo nel resto del capitolo per illustrare alcuni dei concetti introdotti. In G^* il vertice F è isolato, il vertice E ha grado 4, e i

Figure 7.1: Il grafo G^* , con 10 vertici e 12 lati.

	a	b	c	d	e	f	g	h	i	j	k	l
A	1	0	1	1	0	1	0	0	0	0	0	0
B	0	0	0	1	1	0	0	1	0	0	0	0
C	1	1	0	0	0	0	0	0	0	0	0	0
D	0	0	0	0	1	1	1	0	0	0	0	0
E	0	1	1	0	0	0	1	1	0	0	0	0
F	0	0	0	0	0	0	0	0	0	0	0	0
G	0	0	0	0	0	0	0	0	1	1	0	1
H	0	0	0	0	0	0	0	0	1	0	0	0
I	0	0	0	0	0	0	0	0	0	1	1	0
J	0	0	0	0	0	0	0	0	0	0	1	1

Figure 7.2: La matrice di incidenza nodi-archi di G^* .

lati a e b sono adiacenti.

La *matrice di incidenza nodi-archi* di un grafo è una matrice M con $|V|$ righe e $|E|$ colonne. Ogni riga corrisponde a un vertice $v \in V$ e ogni colonna corrisponde a un lato $e = vw \in E$. Il generico elemento M_{ve} della matrice vale 1 se $e \in E$ è incidente in $v \in V$, altrimenti vale 0. In figura 7.2, è visualizzata la matrice di incidenza nodi-archi del grafo G^* . Si noti che nella matrice M ci sono esattamente due “1” in ogni colonna, e che la somma degli elementi di una qualsiasi riga v è pari a $d(v)$. Abbiamo il seguente

TEOREMA 30: Sia $G = (V, E)$ un grafo. Allora $\sum_{v \in V} d(v) = 2|E|$.

Dim: Sommando gli elementi di M riga per riga, otteniamo $\sum_{v \in V} d(v)$. Sommandoli colonna per colonna, otteniamo $|E| \times 2$. Siccome i due modi devono dare lo stesso risultato, il teorema è dimostrato. ♣

Il precedente teorema implica che, in ogni grafo, la somma dei gradi dei vertici è un numero pari. Da questo fatto consegue un importante risultato:

TEOREMA 31: In ogni grafo c'è un numero pari di vertici di grado dispari.

Dim: Sia $D \subseteq V$ l'insieme dei vertici di grado dispari e $P = V - D$ l'insieme dei vertici di grado pari. Abbiamo

$$\sum_v d(v) = \sum_{v \in D} d(v) + \sum_{v \in P} d(v) = 2|E|$$

da cui, essendo sia $\sum_{v \in P} d(v)$ che $2|E|$ dei numeri pari, consegue che $\sum_{v \in D} d(v)$ deve anch'esso essere un numero pari. Ma allora $|D|$ è pari, in quanto sommando una quantità dispari di numeri dispari, il risultato è un numero dispari. ♣

Una sequenza (d_1, \dots, d_n) di numeri naturali si dice *grafica* se esiste un grafo G di n vertici tale che la sequenza corrisponde ai gradi dei vertici di G . Non tutte le sequenze sono grafiche, come è facile vedere. Ad esempio, le seguenti sono alcune condizioni necessarie perchè una sequenza risulti grafica:

- una sequenza grafica non può contenere alcun numero $\geq n$
- se una sequenza contiene sia il numero 0 che il numero $n-1$, non può essere grafica, perchè implicherebbe che esiste un nodo che non è adiacente ad alcun altro nodo, ed uno che è adiacente a tutti gli altri
- la sequenza deve contenere un numero pari di numeri dispari. Ad es. la sequenza $(2, 3, 0, 1, 1)$ non è grafica.

ESERCIZIO 7.1. Dimostrare che, dato un gruppo di n persone, ve ne sono sempre almeno due con lo stesso numero di amici (supponendo che l'amicizia sia una relazione simmetrica). ◇

ESERCIZIO 7.2. Dimostrare che non può esistere un grafo $G = (V, E)$ in cui $|E| = 1000$ e $d(v) \in \{3, 6, 9\}$ per ogni $v \in V$. ◇

Due grafi $G = (V, E)$ e $G' = (V', E')$ si dicono *isomorfi* se esiste una funzione $f : V \mapsto V'$ tale che $f(v)f(w) \in E'$ se e solo se $vw \in E$. In pratica, due grafi sono isomorfi se è possibile rinominare i nodi del primo usando i nomi dei nodi del secondo, e ottenere esattamente il secondo grafo. Si noti che in un grafo non è importante il modo in cui il grafo è disegnato, ma solo quali sono le relazioni tra i nodi.

Dato un grafo $G = (V, E)$, un grafo $G' = (V', E')$ si dice *sottografo* di G se $V' \subseteq V$ e $E' \subseteq E$. Se inoltre $V' = V$, allora G' si dice un sottografo *di supporto* (*spanning*) di G . Dato un sottoinsieme di vertici $S \subseteq V$, si dice sottografo *indotto* da S , indicato con $G[S]$ il grafo che ha S come insieme di vertici e come lati ha tutti i lati $ij \in E$ tali che $i \in S$ e $j \in S$.

Un grafo si dice *completo* se ogni coppia di vertici è collegata da un lato. Il generico grafo completo di n nodi (unico, a meno di isomorfismi) si indica con K_n . In K_n ci sono n vertici e $n(n-1)/2$ lati. Un sottografo completo di un grafo è detto una *clique* (o anche *cricca*). Se in un grafo i lati indicano relazioni di compatibilità fra gli elementi, una clique è un insieme di elementi tutti mutualmente compatibili. Ad esempio, il sottografo indotto da $\{G, I, J\}$ in G^* è una clique di 3 nodi, detta anche un *triangolo*.

Dato un grafo $G = (V, E)$ si definisce grafo *complementare* di G il grafo $\bar{G} = (V, \bar{E})$ definito da $\bar{E} = \{vw \mid v, w \in V, vw \notin E\}$. Se G è un grafo completo, il suo complementare è un grafo di soli nodi isolati. Un insieme di vertici $S \subseteq V$ è detto un *insieme indipendente* o *stabile*, se $ij \notin E$ per ogni $i, j \in S$. Si noti che S è un insieme indipendente se e solo se il grafo indotto da S in \bar{G} è una clique.

ESERCIZIO 7.3. Dato un insieme V di 20 elementi, quanti grafi diversi (non necessariamente non isomorfi) esistono, che abbiano V come insieme di vertici? \diamond

7.2 Cammini e cicli

Un *cammino* dal vertice v_0 al vertice v_k in un grafo $G = (V, E)$ è una sequenza di vertici $v_0, v_1, \dots, v_{k-1}, v_k$ tali che, per $0 \leq i \leq k-1$, si ha $v_i v_{i+1} \in E$. Si dice anche che il cammino *usa* (o *attraversa*) i k lati $v_i v_{i+1}$, per $0 \leq i \leq k-1$, e che *visita* (o *attraversa*) i $k+1$ vertici v_0, \dots, v_k . Si dice anche che un tale cammino ha *lunghezza* k (la lunghezza è pari al numero di lati usati) e che *connette* (o *collega*) v_0 e v_k . Un cammino si dice *semplice* se non usa mai lo stesso arco più di una volta, ed *elementare* se non visita mai lo stesso vertice più di una volta (con l'eccezione del primo vertice del cammino, che può coincidere con l'ultimo). Nell'esempio di figura 7.1 i seguenti cammini collegano C ad A:

$$P_1 : C, E, D, B, E, D, A$$

$$P_2 : C, E, B, D, E, A$$

$$P_3 : C, E, D, A$$

P_1 non è un cammino semplice. P_2 è semplice ma non elementare. P_3 è un cammino elementare. Nel seguito, qualora non specificato diversamente, per “cammino” intenderemo sempre, implicitamente, cammino elementare.

Dati due vertici u e v , la loro *distanza* in G , denotata con $d_G(u, v)$, è definita come la lunghezza del cammino più corto che li congiunge. Il *diametro* di un grafo è la distanza massima fra una qualsiasi coppia di vertici (ad esempio, in $G^*[\{H, G, I, J\}]$ il diametro è 2).

Un *ciclo*, o *circuito*, è un cammino chiuso, ossia un cammino in cui $v_0 = v_k$. Ad esempio, A,B,D,E,C,A e G,I,J,G sono circuiti in G^* . Un grafo G si dice *aciclico* se non contiene alcun ciclo elementare (i.e., senza vertici ripetuti, a parte il primo e l'ultimo). Un circuito elementare che attraversa tutti i nodi di G si chiama *circuito hamiltoniano*. Un circuito semplice (i.e., senza lati ripetuti) che attraversa tutti i lati di G si chiama *circuito euleriano*. Circuiti hamiltoniani ed euleriani saranno trattati nella prossima sezione.

Un grafo G si dice *connesso* se ogni coppia di vertici è collegata da almeno un cammino in G . Dato un grafo $G = (V, E)$, i vertici possono essere partizionati in k sottoinsiemi V_1, \dots, V_k tali che $G[V_i]$ è un grafo connesso per ogni i , mentre non lo è il grafo $G[V_i \cup \{v\}]$ per alcun $v \notin V_i$. I sottografi $G[V_i]$ si chiamano le *componenti connesse* di G . Un grafo è connesso se e solo se ha un'unica componente connessa. Il grafo G^* ha tre componenti connesse.

Un insieme $E' \subseteq E$ di lati si dice un *taglio* se la sua rimozione da E aumenta il numero di componenti connesse. In particolare, a partire da un insieme S di vertici si può definire il seguente insieme $\delta(S)$ di lati

$$\delta(S) := \{ij : i \in S, j \in V - S\}$$

che risulta un taglio non appena esista almeno una coppia di nodi (uno in S e l'altro in $V - S$) adiacenti

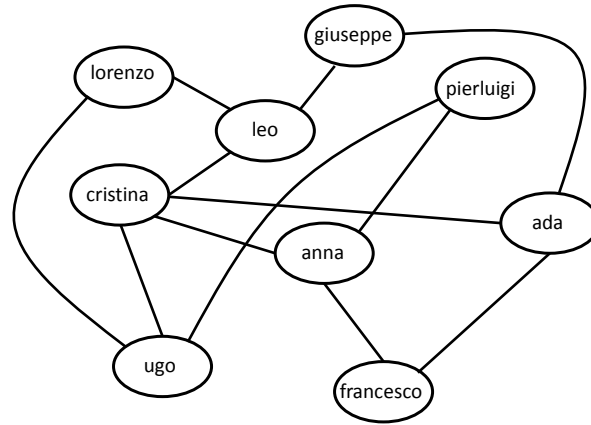


Figure 7.3: Un gruppo di amici invitati a cena

in G (in caso contrario, $\delta(S) = \emptyset$).

ESERCIZIO 7.4. Dimostrare che un grafo con sequenza grafica $(3, 3, 3, 3, 3, 3, 4, 4)$ è necessariamente connesso
 \diamond

ESERCIZIO 7.5. Dimostrare che in un grafo G aciclico, esiste sempre almeno un vertice v con $d_G(v) \leq 1$. \diamond

ESERCIZIO 7.6. Dimostrare che, dato un grafo $G = (V, E)$, si ha che $\{e\}$ è un taglio per ogni $e \in E$ se e solo se G è aciclico. \diamond

ESERCIZIO 7.7. Dimostrare che un grafo con n nodi e $(n-1)(n-2)/2 + 1$ lati è necessariamente connesso.
 \diamond

ESERCIZIO 7.8. Sia G un grafo (non completo) tale che, per ogni coppia di vertici x e y non adiacenti si ha $d(x) + d(y) \geq n - 1$. Dimostrare che $\text{diam}(G) = 2$. \diamond

7.3 Grafi bipartiti, hamiltoniani e euleriani

Un gruppo di persone si trovano per una cena a casa di uno di loro. Le relazioni di amicizia fra gli stessi sono rappresentate, in modo ovvio, dal grafo in Figura 7.3. Il padrone di casa desidera farli sedere in modo tale che ognuno abbia come due immediati commensali, a destra e sinistra, degli amici. È possibile una tale disposizione? Un modo per verificarlo, sarebbe quello di andare per tentativi, provando tutte le possibili permutazioni circolari (sono $(n-1)!/2$ per n elementi) e vedendo se ce ne è una del tipo desiderato. Abbiamo

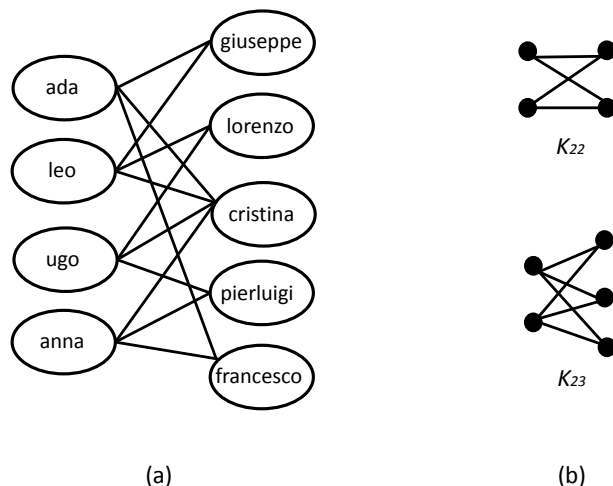


Figure 7.4: (a) Un grafo bipartito. (b) Grafi bipartiti completi

già visto fin dagli esempi introduttivi del primo capitolo come questa sia, in generale, una strategia da evitare. Basti notare che, per soli 9 elementi, si dovrebbero esaminare potenzialmente ben 20160 disposizioni!

Dato un grafo G , una permutazione circolare dei vertici in cui ogni nodo è preceduto e seguito da un nodo che gli è adiacente in G , è detta *circuito* (o *ciclo*) *hamiltoniano*. Detto altrimenti, un ciclo hamiltoniano è un ciclo che passa per ogni nodo, una e una sola volta. Un grafo si dice *hamiltoniano* se contiene un circuito hamiltoniano. Quindi, il nostro problema, corrisponde a verificare se il grafo di Figura 7.3 è hamiltoniano. Questo problema è un problema che può risultare molto difficile, e per il quale non esistono condizioni necessarie e sufficienti che siano facili da verificare. Da un punto di vista algoritmico, il problema è dei più difficili in assoluto, e non sono note procedure più efficienti che –implicitamente o esplicitamente– provare tutte le possibilità. Nel nostro esempio però (a parte la piccola dimensione del problema) possiamo sfruttare una caratteristica del problema per rispondere immediatamente che no, non ci sono soluzioni possibili. Infatti, si noti che ogni persona ha un nome corto (una o due sillabe) o lungo (tre o più sillabe) e accade che chi ha il nome corto ha solo amici con il nome lungo, mentre chi ha il nome lungo ha solo amici con il nome corto. Quindi, una disposizione accettabile dovrebbe alternare persone dal nome lungo e persone dal nome corto, sicché dovrebbero esserci esattamente altrettanti nomi lunghi che nomi corti (e, in particolare, dovrebbe esserci un numero *pari* di persone). Ma ci sono 9 invitati e perciò una tale disposizione è impossibile.

Un grafo in cui i nodi possono essere ripartiti in due insiemi, V_1 e V_2 tale che ogni arco collega un estremo in V_1 e uno in V_2 si dice *bipartito*. In figura 7.4(a) si è ridisegnato il grafo iniziale, mettendo in evidenza la bi-partizione. Il ragionamento di poco fa si ritrova in questo teorema, che caratterizza i grafi bipartiti:

TEOREMA 32: G è un grafo bipartito se e solo se ogni ciclo in G ha un numero pari di nodi.

Dim: La necessità è molto semplice: Un qualsiasi ciclo che parta, ad esempio, da un nodo in V_1 , deve alternare nodi di V_1 e V_2 e terminare in un nodo di V_1 . Quindi, deve attraversare un numero pari di lati, o finirebbe in un nodo di V_2 .

Per la sufficienza, ragioniamo così. Intanto, supponiamo il grafo connesso (in caso contrario, si ripeta questo procedimento sulle varie componenti connesse). Si fissi un nodo v , e si definisca V_1 come l'insieme dei nodi per i quali esiste un cammino di lunghezza pari da v , e $V_2 = V - V_1$. Se, per assurdo, esistesse un arco ij con i e j entrambi in V_1 (o entrambi in V_2), allora ci sarebbe anche un ciclo dispari, contenuto nell'unione del cammino da v a i col cammino da v a j e con l'arco ij . Siccome abbiamo supposto che non ci siano cicli dispari, V_1 e V_2 sono una partizione di V . ♣

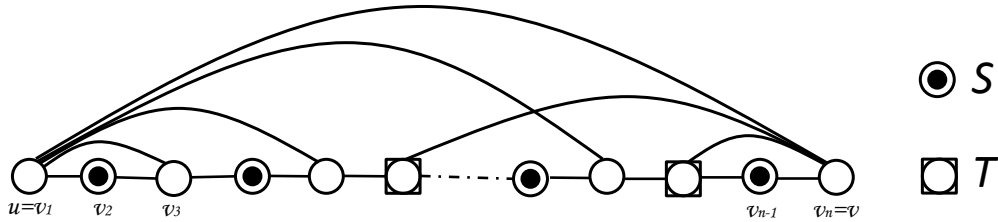
Un grafo bipartito si denota anche con $G = (V_1, V_2, E)$. Un grafo si dice *bipartito completo* se è tale che $ij \in E$ per ogni $i \in V_1$ e $j \in V_2$. Un tale grafo si indica anche con $K_{n,m}$ (dove $n = |V_1|$ e $m = |V_2|$) ed ha $n + m$ vertici e nm lati.

Esempio. Il processo detto *sequenziamento* del genoma consiste in (1) replicare (clonare) il DNA in oggetto in molte copie (almeno una decina); (2) spezzare, casualmente, ogni copia in frammenti di circa 1000 basi l'uno; (3) con un'apposita macchina (detta sequenziatore) ricavare la sequenza di basi di ognuno di questi frammenti; (4) con un computer, determinare la sovrapposizione dei frammenti in modo da poter ricostruire la sequenza originale.

Al termine del processo, si ha una sequenza s ricostruita, che contiene la sequenza f_i di ogni frammento i . Inoltre, ogni frammento ha anche associata una posizione p_i , che specifica il suo inizio all'interno della sequenza s . Uno dei maggiori problemi in questo processo è dato dal fatto che di ogni cromosoma esistono, in realtà due copie (una paterna e una materna) e quindi il processo dovrebbe ricostruire non una, ma due sequenze (s_p e s_m) e per ogni frammento, oltre alla posizione d'inizio, dovrebbe anche determinare l'appartenenza a_i (con, ad esempio, $a_i = 1$ se il frammento proviene dalla copia paterna e $a_i = 0$ se il frammento proviene dalla copia materna). Sia F l'insieme di tutti i frammenti. Dati due frammenti i e j con sovrapposizione non nulla (ossia tale che $p_i \leq p_j < p_i + \text{lung}(f_i)$), diciamo che i due frammenti sono *in conflitto* se, nelle posizioni coperte da entrambi, esiste almeno una posizione k tale che il nucleotide $f_i[k]$ è diverso dal nucleotide $f_j[k]$. Chiaramente, due tali frammenti non possono provenire entrambi dalla copia paterna o dalla copia materna. Sia E l'insieme delle coppie di frammenti in conflitto. Allora, il grafo $G = (F, E)$ deve essere un grafo bipartito (se così non fosse, vuol dire che ci sono stati errori di sequenziamento e/o di piazzamento dei frammenti). Se G è bipartito, i nodi F possono partizionarsi in nodi F_p (provenienti dalla copia paterna) e F_m , provenienti dalla copia materna. ♦

Come corollario del teorema 32 abbiamo che *un grafo bipartito con un numero dispari di nodi non può essere hamiltoniano*. Dal punto di vista algoritmico, è nota una procedura molto efficiente per determinare se un grafo è bipartito. Applicandola al nostro caso, si può risolvere il problema iniziale in modo molto più rapido rispetto all'enumerazione completa di tutte le disposizioni degli invitati. Si noti però che la condizione di essere bipartito con n dispari è solo una condizione sufficiente, e molto debole, per verificare che un grafo *non* è hamiltoniano. Il problema di verificare se un grafo è hamiltoniano o meno è difficile e non esistono semplici condizioni necessarie e sufficienti perchè un grafo risulti essere hamiltoniano. Una condizione sufficiente non-elementare è la seguente:

TEOREMA 33: Un grafo di almeno 3 vertici $G = (V, E)$, in cui $d(v) \geq |V|/2$ per ogni $v \in V$ è hamiltoniano.

Figure 7.5: Il cammino hamiltoniano in G .

Dim: Sia, per assurdo, G un controesempio massimale (ossia, in G si ha $d(v) \geq |V|/2$ per ogni v , G non è hamiltoniano, ma aggiungendo un qualsiasi arco lo diventa). Sia ora uv un lato mancante in G (ce ne devono essere, o G sarebbe completo, e quindi hamiltoniano). Siccome $G \cup uv$ è hamiltoniano, ogni circuito hamiltoniano in $G \cup uv$ usa il lato uv (o sarebbe già stato presente in G). Quindi, un tale circuito individua un *cammino* hamiltoniano tra u e v in G . Sia questo cammino

$$u = v_1, v_2, \dots, v_n = v.$$

Definiamo ora due insiemi di vertici, $S = \{v_i | uv_{i+1} \in E\}$ e $T = \{v_i | v_i v \in E\}$ (si veda la Figura 7.5). Si ha $T \cap S = \emptyset$, o altrimenti ci sarebbe un ciclo hamiltoniano in G . Infatti, se $x = v_k \in S \cap T$, il ciclo

$$u, v_{k+1}, v_{k+2}, \dots, v, x, v_{k-1}, \dots, v_2, u$$

sarebbe tutto contenuto in G . Inoltre $S \cup T \neq V$. Infatti, ad esempio, $v \notin S \cup T$. Quindi

$$|S \cup T| = |S| + |T| < |V|$$

e ne consegue che $d(u) = |S| < |V|/2$ oppure $d(v) = |T| < |V|/2$ portandoci a contraddire l'ipotesi sul grado dei nodi del grafo. ♣

ESERCIZIO 7.9. In un'aula ci sono 5 file di 5 banchi ciascuna. L'insegnante richiede agli alunni di cambiare posto, in modo tale che ogni alunno passi dal suo banco a un banco che sia immediatamente a sinistra o a destra, o di fronte o dietro al suo (chiaramente, non tutte le scelte sono possibili per tutti gli studenti. Ad esempio, chi è già seduto in un banco all'estrema destra non può spostarsi ancora più a destra). Si determini se esiste o no almeno un modo di spostarsi che permetta a tutti gli studenti di cambiare banco. ◇

ESERCIZIO 7.10. Nel gioco degli scacchi, il cavallo compie la caratteristica mossa a "L" (ossia, passa dalla casella (x, y) alla casella $(x + \delta, y + \Delta)$ dove $\delta, \Delta \in \{-2, -1, 1, 2\}$ e $|\delta| \neq |\Delta|$). Un "giro del cavallo" di una scacchiera consiste nel partire da una casella (x, y) e, effettuando sempre mosse valide, toccare ogni altra casella una e una sola volta, fino a tornare alla casella (x, y) . Si determini se esiste una posizione di partenza da cui è possibile il giro del cavallo su una scacchiera 5×5 . La stessa domanda per una scacchiera 4×4 . ◇

Un grafo si dice *planare* se può essere disegnato in modo che due archi non si incrocino mai in alcun punto. Un grafo G' si dice un *minore* di G se G' può essere ottenuto da G tramite una sequenza di ripetizioni della seguente operazione:

- *Contrazione di un arco*: Si rimuove un arco $e = ij$ (inclusi i vertici i e j) e al suo posto si inserisce un nuovo nodo, e' . Ogni lato che incideva in i o in j diventa ora un lato che incide in e' (si cancellano eventuali lati duplicati).

Abbiamo il seguente teorema, la cui dimostrazione è troppo complessa per essere riportata qui:

TEOREMA 34: Un grafo G è planare se e solo se non ha nè K_5 nè $K_{3,3}$ fra i suoi minori.

Analogamente al problema di determinare se un grafo abbia o meno un circuito che attraversa tutti i vertici una e una sola volta, possiamo chiederci se esista un circuito che attraversi tutti i lati una e una sola volta. Un tale circuito si dice *euleriano* ed un grafo che possiede un circuito euleriano si dice *grafo euleriano*. Il nome deriva da quello di Eulero, il famoso matematico che può considerarsi il padre della teoria dei grafi. La teoria dei grafi è infatti nata, almeno storicamente, con il problema dei ponti della città di Königsberg: ci si chiedeva se fosse possibile partire da un punto della città, attraversare i suoi 7 ponti una e una sola volta, e ritornare al punto di partenza. Eulero dimostrò come questo non fosse possibile, e diede condizioni necessarie e sufficienti all'esistenza di un circuito del tipo desiderato nel caso generale.

TEOREMA 35: Un grafo $G = (V, E)$ connesso è euleriano se e solo se $d(v)$ è pari per ogni $v \in V$.

Dim: Che la condizione sia necessaria è banale. Sia C un circuito euleriano. Seguendo C , rimuoviamo gli archi dal grafo. Ogni volta che entriamo in un nodo, e poi ne usciamo, diminuiamo di 2 il grado del nodo. Alla fine il grado di ogni nodo deve essere 0, e quindi, all'inizio, doveva essere un numero pari.

Per la sufficienza, facciamo vedere che la seguente procedura determina un circuito euleriano C :

1. $C := \{u\}$ /* u è un qualsiasi nodo di G */
2. **while** $E \neq \emptyset$
 - 2a. Sia v un nodo di C di grado > 0
 - 2b. Partendo da v , si determini un circuito semplice C' che attraversa alcuni archi (siano essi F') e torna a v
 - 2c. Si fondano C e C' , ottenendo il circuito che va da u a v lungo C , poi attraversa tutto C' e poi torna a u lungo C . Si rinomini C il circuito risultante
 - 2d. $E := E - F'$ /* si tolgano gli archi appena visitati */
3. **endwhile**

Ad ogni iterazione del ciclo 2a-2d, deve esistere almeno un nodo di C di grado positivo. Infatti, noi abbiamo supposto che il grafo sia connesso, e quindi da almeno un nodo di C deve uscire qualche arco con un estremo al di fuori di C . Il grado di ogni nodo rimane sempre pari, in quanto ad ogni iterazione viene rimosso un circuito (passo 2d). In virtù di ciò, nel passo 2b siamo sicuri di poter partire da v e, costruendo un qualsiasi cammino semplice, tornare prima o poi a v , in quanto ogni volta che entriamo in un nodo diverso da v , possiamo anche uscire dallo stesso. Al termine della procedura, il grado di tutti i nodi del grafo deve essere diventato 0, e il circuito C finale è un circuito euleriano. ♣

Un *cammino euleriano* è un cammino che attraversa tutti gli archi, una e una sola volta. Dal teorema 35 segue il

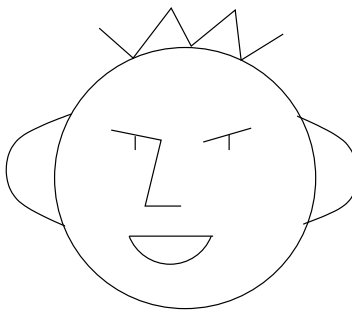


Figure 7.6: Quante volte va staccata la penna dal foglio per disegnare questa figura senza mai ripassare la stessa linea?

COROLLARIO 36: Un grafo connesso ha un cammino euleriano se e solo se ha al più due vertici di grado dispari.

Infatti, se non ci sono vertici di grado dispari il grafo è euleriano e quindi c'è un circuito (che è anche un cammino) euleriano. Altrimenti, detti a e b i vertici di grado dispari, l'algoritmo precedente inizializzato con $v_0 = a$ determina un cammino euleriano da a a b . Si noti che il famoso gioco di disegnare una certa figura geometrica senza mai staccare la penna dal foglio nè ripassare due volte su una stessa linea può essere interpretato come il problema di determinare se un certo grafo ha un cammino euleriano o meno.

ESERCIZIO 7.11. Quante volte, come minimo, bisogna staccare la penna dal foglio per disegnare (senza mai passare due volte su una stessa linea) la figura 7.6? \diamond

ESERCIZIO 7.12. Sia $G = (V, E)$ un grafo con esattamente due vertici, a e b di grado dispari. Sia G' il grafo ottenuto da G aggiungendo a V un nodo $c \notin V$ e ad E i due lati ac e bc . Dimostrare che G è connesso se e solo se G' è connesso. \diamond

ESERCIZIO 7.13. Sia $V = \{1, 2, \dots, 20\}$ e $G = (V, E)$ un grafo in cui E è definito dalle regole seguenti. Si dica, per ogni caso, se (i) G è connesso, (ii) G è bipartito, (iii) Ogni componente connessa di G è euleriana, (iv) Ogni componente connessa di G è hamiltoniana:

1. $ab \in E$ se $a + b$ è pari.
2. $ab \in E$ se $a + b$ è dispari.
3. $ab \in E$ se $a \times b$ è pari.
4. $ab \in E$ se $a \times b$ è dispari.
5. $ab \in E$ se $a \times b$ è un quadrato.
6. $ab \in E$ se $a - b$ è un multiplo 3.

\diamond

7.4 Alberi

Un grafo che sia

- (i) aciclico; (ii) connesso

è detto un *albero*. L'albero è il grafo minimale (rispetto al numero di lati) necessario e sufficiente per connettere un insieme di nodi. Infatti, in un albero l'aggiunta di un qualsiasi lato non aumenta il numero di coppie di nodi connesse, mentre si può dimostrare che la rimozione di un qualsiasi lato riduce il numero di coppie connesse. Un generico grafo aciclico si chiama anche una *foresta*, perchè ogni sua componente connessa è un albero.

Un albero di n nodi ha sempre esattamente $n - 1$ archi. Per vedere ciò dimostriamo che

1. Un grafo con $n \geq 3$ nodi e $|E| \geq n$ non può essere aciclico.
2. Un grafo con $n \geq 2$ nodi e $|E| < n - 1$ non può essere connesso.

Dim: Entrambi i punti possono essere dimostrati, ad esempio, per induzione. Per quel che riguarda il punto 1, l'asserzione è sicuramente vera per $n = 3$. Consideriamo ora il caso di $n > 3$. Se ogni nodo ha grado ≥ 2 il grafo ha sicuramente almeno un ciclo (vedi anche esercizio in sezione 7.2). Altrimenti, sia v un nodo di grado ≤ 1 . Togliendo v e l'eventuale arco incidente in v , otteniamo un grafo con $n - 1$ nodi e almeno $n - 1$ archi, che, per induzione, deve avere almeno un ciclo.

Per quel che riguarda il punto 2, il caso base $n = 2$, è certamente vero. Per $n > 2$, se esiste un nodo di grado 0, il grafo non è connesso. Altrimenti, sia v un nodo di grado 1 (deve esistere, perchè, diversamente, si avrebbe $\sum_{u \in V} d(u) \geq 2n$. Ma $2n > 2|E|$, mentre la somma dei gradi deve dare $2|E|$). Come prima, togliendo v e l'arco incidente in v , otteniamo un grafo G' con $n - 1$ nodi e al più $n - 2$ archi, che, per induzione, non può essere connesso. Siccome una qualsiasi coppia di vertici non connessa in G' non è connessa neppure in G (perchè il nodo v non può essere usato in nessun cammino –se non come nodo iniziale/finale del cammino), anche G non è connesso. ♣

Le seguenti proprietà caratterizzano gli alberi, ossia sono tutte definizioni alternative di un albero $G = (V, E)$:

1. G è connesso e aciclico
2. G è connesso e $|E| = |V| - 1$
3. G è aciclico e $|E| = |V| - 1$
4. G è connesso e, per ogni coppia di nodi i e j esiste un unico cammino fra i e j
5. G è connesso e la rimozione di un qualsiasi arco disconnette G .
6. G è aciclico e, per ogni coppia di nodi i e j tali che $ij \notin E$, aggiungendo l'arco ij , G conterrebbe esattamente un ciclo.

Per esercizio, si dimostri l'equivalenza di almeno alcune delle definizioni alternative citate (cioè si scelgano arbitrariamente alcune coppie $x, y \in \{1, \dots, 6\}$ e si dimostri che x implica y).

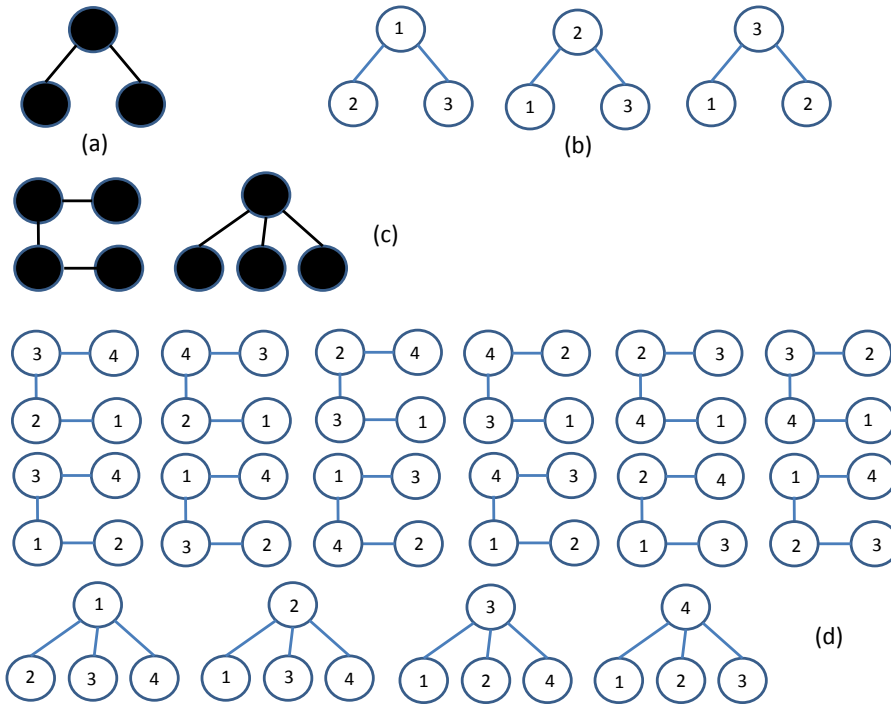


Figure 7.7: (a) e (c) Alberi di 3 e 4 nodi (a meno di isomorfismi). (b) Alberi sui nodi $\{1, 2, 3\}$. (d) Alberi sui nodi $\{1, 2, 3, 4\}$.

Un nodo di grado 1 in un albero si chiama una *foglia*. In ogni albero con $n \geq 2$ ci sono almeno due foglie (per esercizio, lo si dimostri). Un nodo non foglia di un albero si chiama anche *nodo interno*. Si noti che un cammino di lunghezza l rappresenta un caso estremo di albero (con esattamente 2 foglie e $l - 1$ nodi interni). Il cammino è l'albero di diametro massimo tra tutti gli alberi su un certo insieme di nodi. All'altro estremo abbiamo la *stella*, ossia un albero in cui c'è un nodo interno e tutti gli altri nodi sono foglie. La stella è l'albero di diametro minimo.

Sia $T = (V, E_T)$ un albero di supporto in un grafo $G = (V, E)$. La rimozione da T di un qualsiasi arco $e = ij$ disconnette l'albero. In particolare, l'arco individua una partizione dei nodi in due insiemi: V_i (i nodi raggiungibili da i in $(V, E_T - \{e\})$) e $V_j = V - V_i$ (i nodi raggiungibili da j in $(V, E_T - \{e\})$). Il taglio $\delta(V_i)$ è anche detto *taglio fondamentale* associato all'arco e nell'albero T .

Similmente, l'aggiunta a T di un qualsiasi arco $a = ij \in E - E_T$ definisce univocamente un circuito C in G passante per i e j . Il circuito, consistente dell'unico cammino tra i e j in T più l'arco a , è detto *circuito fondamentale* associato ad a nell'albero T .

Concludiamo questa sezione con un teorema riguardo al numero di alberi possibili su un insieme di n nodi.

TEOREMA 37: (Cayley) Il numero di alberi diversi su un insieme di n nodi è n^{n-2} .

In questo teorema, alberi isomorfi ma non identici vengono considerati diversi. Ad esempio, per $n = 3$ risultano 3 alberi diversi, mentre, se contassimo solo gli alberi non isomorfi fra loro, ci sarebbe un unico albero possibile. In figura 7.7 (a) e (c) rispettivamente, sono illustrati gli alberi non isomorfi di 3 e 4 nodi. In figura 7.7 (b) e (d) sono illustrati invece tutti i possibili alberi sugli insiemi di vertici $\{1, 2, 3\}$ e $\{1, 2, 3, 4\}$.

Non è nota alcuna formula semplice (del tipo della formula di Cayley) che fornisca il numero T_n di alberi non isomorfi di n nodi. Possiamo però dare dei limiti inferiori e superiori quali

$$\frac{n^{n-2}}{n!} \leq T_n \leq 4^{n-1}. \quad (7.1)$$

ESERCIZIO 7.14. In un albero T , il grado medio dei nodi è 1.99. Quanti archi ha T ? ◇

ESERCIZIO 7.15. In un albero T tutti i nodi hanno grado 3 o 1 e ci sono esattamente 10 nodi di grado 3. Quanti sono i nodi di grado 1? ◇

ESERCIZIO 7.16. In un albero T ci sono : esattamente un nodo di grado 5; esattamente un nodo di grado 4; esattamente un nodo di grado 3; esattamente un nodo di grado 2; nessun nodo di grado ≥ 6 . Quante foglie ha T ? ◇

ESERCIZIO 7.17. Quanti alberi (a due a due non isomorfi) esistono di diametro 3 e con 103 archi ciascuno? ◇

Indici di Wiener

Un *indice* per una famiglia di grafi è una funzione che a ogni grafo associa un numero. Ad esempio, il grado massimo dei nodi di un grafo è un indice, così come lo è il suo diametro. In chimica combinatoria, dove i grafi sono utilizzati per rappresentare molecole (con i nodi associati agli atomi e i lati ai legami atomici), molti indici vengono adottati per discriminare, ad esempio, il livello di completezza, di connettività, ecc., dei grafi in questione. Uno tra i più famosi di tali indici è l'*indice di Wiener*.

Dato un grafo $G = (V, E)$, l'indice di Wiener di G è così definito:

$$W(G) = \sum_{i,j \in V} d_G(i, j).$$

Semplificandone il significato, ad un indice basso corrispondono grafi “compatti” mentre ad un indice alto corrispondono grafi “sparsi”, con cammini lunghi.

Dato un grafo, determinarne l'indice di Wiener è un problema semplice. Il problema inverso, consistente nel verificare se, per un certo numero t esiste un grafo G tale che $W(G) = t$, è anch'esso di facile soluzione, come descritto dal seguente teorema:

TEOREMA 38: Per ogni $t \neq 2, 5$ esiste un grafo G tale che $W(G) = t$.

Per dimostrare il teorema, partiamo con la dimostrazione di un utile lemma:

Lemma 39: Per ogni grafo $G = (V, E)$ di diametro 2, il grafo $G' = (V, E \cup \{e\})$ per $e \notin E$ ha indice di Wiener $W(G') = W(G) - 1$.

Dim: Sia $e = (v_1, v_2)$ un lato mancante in G . Chiaramente $d_G(v_1, v_2) = 2$ e $d_{G'}(v_1, v_2) = 1$. Siccome la distanza di ogni altra coppia di nodi non è alterata dall'aggiunta di e , l'indice di Wiener cala esattamente di un'unità. ♣

Siamo ora pronti a dimostrare il teorema 38.

Dim: Sia $G_0 = S_n$, la stella di dimensione n (un albero con al più un nodo interno). Si ha $W(G_0) = (n-1)^2$ e il diametro di G_0 è 2. Sia G_1 il grafo ottenuto aggiungendo a G_0 un lato mancante. Se G_1 non è un grafo completo, allora ha diametro 2, e per il lemma precedente $W(G_1) = W(G_0) - 1$. Si può ripetere questo procedimento finché il grafo ottenuto è completo, e si ha $W(K_n) = n(n-1)/2$. Ad ogni passo, il lemma garantisce che $W(G_k) = W(G_{k-1}) - 1$. Quindi, ogni numero nell'intervallo $I_n = [n(n-1)/2, (n-1)^2]$ è l'indice di Wiener di G_k per qualche k . Per $n = 4$ si ha $I_4 = [6, 9]$ mentre $I_5 = [10, 16]$ e gli intervalli I_n e I_{n+1} si sovrappongono per $n \geq 5$. Quindi, per ogni $t \geq 6$ c'è un grafo G tale che $W(G) = t$. Per i rimanenti casi, si noti che il grafo (connesso) di due nodi ha indice di Wiener pari a 1, mentre con 3 nodi si hanno due possibili grafi, di indici, rispettivamente 3 e 4. Siccome con 4 o più nodi l'indice di Wiener è almeno 6 (ci sono almeno 6 coppie) si vede che i valori 2 e 5 restano esclusi. ♣

Il calcolo dell'indice di Wiener per gli alberi può essere semplificato dalla seguente formula. Dato un albero $T = (V, E)$, si definisca, per un lato $e = uv \in E$, il *carico* del lato e

$$\lambda(e) = n_u \times n_v$$

dove n_u e $n_v = |V| - n_u$ sono il numero di nodi nelle due componenti connesse indotte dalla rimozione di e da T . Si noti che $\lambda(e)$ rappresenta il numero di coppie di nodi che sono collegate da un cammino che usa il lato e . Siccome per ogni coppia di vertici c'è un unico cammino che li collega in T , l'indice di Wiener è la somma delle lunghezze di tali cammini, e questo corrisponde alla somma, per tutti i lati dell'albero, del numero di cammini che utilizzano i lati:

$$W(T) = \sum_{e \in E} \lambda(e).$$

Si ha il seguente semplice risultato che lega la parità del numero di nodi a quella dell'indice:

Lemma 40: Ogni albero con un numero n dispari di nodi ha indice di Wiener pari.

Dim: Se n è dispari, il carico di ogni arco risulta pari (il prodotto di un numero pari e uno dispari) e quindi la somma dei carichi è anch'essa pari. ♣

Il problema inverso nel caso degli alberi è il seguente: dato un numero t , esiste un albero con indice di Wiener t ? Tale problema risulta molto più complesso del caso generale. Esistono svariati valori che non possono essere indice di alcun albero, ma, per t sufficientemente grande, ogni t è ottenibile da qualche albero:

TEOREMA 41: Ogni valore di t diverso da 2, 3, 5, 6, 7, 8, 11, 12, 13, 14, 15, 17, 19, 21, 22, 23, 24, 26, 27, 30, 33, 34, 37, 38, 39, 41, 43, 45, 47, 51, 53, 55, 60, 61, 69, 73, 77, 78, 83, 85, 87, 89, 91, 99, 101, 106, 113, 147, 159, è ottenibile come indice di Wiener di qualche albero.

ESERCIZIO 7.18. Fissato un numero n di nodi, quali sono gli alberi di indice di Wiener minimo e quanto vale tale indice? Quali sono gli alberi di indice massimo e quanto vale tale indice? \diamond

7.5 Grafi orientati

Un *grafo orientato* (o *grafo diretto* o *digrafo*) è una coppia $G = (N, A)$ dove N è detto l'insieme dei *nod*i e A l'insieme degli *archi*. Ogni arco è una coppia (i, j) ordinata di nodi, con $i \neq j$. Graficamente, l'arco (i, j) viene rappresentato con una freccia uscente dal nodo i ed entrante nel nodo j . Si dice anche che j è la *testa* dell'arco (i, j) e i ne è la *coda*.

Gli archi orientati rappresentano una relazione binaria non necessariamente simmetrica (per cui $(i, j) \neq (j, i)$). Si noti che però gli archi (i, j) e (j, i) possono esistere entrambi). Esempi di tale relazione possono essere

- “sul lavoro, i prende ordini da j ”,
- “una strada tra i e j è percorribile nel senso che va da i a j ”,
- “la squadra i ha battuto la squadra j in almeno un'occasione”,
- ecc.

Per un insieme di nodi $S \subseteq N$, restano definiti i due insiemi di archi $\delta^+(S)$ (archi *usc*enti da S) e $\delta^-(S)$ (archi *entr*anti in S) in questo modo:

$$\delta^+(S) := \{(i, j) \in A \mid i \in S, j \in N - S\} \quad (7.2)$$

$$\delta^-(S) := \{(i, j) \in A \mid i \in N - S, j \in S\}. \quad (7.3)$$

In un digrafo si distinguono due tipi di gradi per i nodi, un *grado d'uscita*, $d^+(v) := |\delta^+(\{v\})|$ pari al numero di archi di cui v è la coda, e un *grado d'entrata*, $d^-(v) := |\delta^-(\{v\})|$ pari al numero di archi di cui v è la testa.

Un cammino in un grafo orientato $G = (N, A)$ è una sequenza di vertici $v_0, v_1, \dots, v_{k-1}, v_k$ tali che, per $0 \leq i \leq k-1$, si ha $(v_i, v_{i+1}) \in A$. Si dice anche che un siffatto cammino *va da* v_0 *a* v_k (o *parte da* v_0 *e arriva a* v_k). Se $v_0 = v_k$ il cammino si dice circuito o ciclo. Circuiti e cammini semplici, elementari, euleriani e hamiltoniani, sono definiti in maniera analoga al caso non orientato.

Dato un digrafo $G = (N, A)$, resta definito un grafo non orientato, $G' = (N, E)$, detto il grafo non orientato *sottostante*, ottenuto “rimuovendo la direzione” dagli archi di A (più formalmente, $ij \in E$ se $(i, j) \in A \vee (j, i) \in A$).

Un digrafo si dice *debolmente connesso* se il grafo non orientato sottostante è connesso. Il digrafo si dice *fortemente connesso* se per ogni coppia $i, j \in N$ esiste un cammino che va da i a j . Un digrafo risulta

fortemente connesso se e solo se ogni coppia di nodi è contenuta in un circuito. Dato un digrafo $G = (N, A)$ i nodi possono essere partizionati in sottoinsiemi massimali N_1, \dots, N_k tali che i sottografi indotti $G[N_i]$ sono fortemente connessi (e sono detti le componenti fortemente connesse di G). Si noti che, a differenza del caso dei grafi non orientati, non è necessariamente vero che ogni arco in A appartenga a qualche componente fortemente connessa. Infatti (esercizio) un arco $a \in A$ appartiene a qualche componente fortemente connessa se e solo se a è contenuto in almeno un circuito di G .

ESERCIZIO 7.19. Vero o Falso: Esiste un grafo orientato $G = (N, A)$ in cui (i) $d^+(v) \neq d^+(w)$ per ogni $v \neq w \in N$ e (ii) per ogni $v \in N$ esiste $u \in N$ con $d^-(u) = d^+(v) - 1$. \diamond

Un *albero orientato* anche detto (*arborescenza*) di radice r , è un grafo orientato aciclico in cui esiste un cammino da r a ogni altro nodo. In un tale albero, si ha $d^-(r) = 0$ e $d^-(v) = 1$ per ogni nodo $v \neq r$. Un nodo di un albero orientato in cui $d^+(v) = 0$ si dice una *foglia*. Dato un nodo v in un'arborescenza, l'insieme di tutti i cammini che cominciano in v è detto il *sottoalbero* di radice v . Ogni nodo in tale sottoalbero si dice anche *discendente* di v . Un nodo v è *antenato* di tutti i suoi discendenti. In particolare, se esiste l'arco (v, w) , si dice che v è *padre* di w , e w è *figlio* di v . Si noti che il sottografo sottostante un'arborescenza è un albero.

Un albero orientato si dice *binario* se $d^+(v) = 2$ per ogni nodo v non foglia; si dice *ternario* se $d^+(v) = 3$ per ogni nodo v non foglia; più in generale, si dice *k-ario* se $d^+(v) = k$ per ogni nodo v non foglia. Dato un nodo u in un albero orientato di radice r , si dice *livello* di u la lunghezza del cammino da r a u . In un albero *k-ario* ci sono al più k^l nodi di livello l . L'*altezza* di un albero è il livello massimo di uno qualsiasi dei suoi nodi.

ESERCIZIO 7.20. Sia $T = (N, A)$ un albero orientato binario di altezza h . Dimostrare che T ha al più 2^h foglie. \diamond

ESERCIZIO 7.21. Sia K_n il grafo completo non orientato di n nodi. Sia D_n un grafo ottenuto da K_n orientando ciascuno dei lati di K_n in esattamente uno dei due modi possibili. Dimostrare che in D_n esiste sempre un cammino hamiltoniano (diretto). \diamond

7.6 Grafi pesati

Talvolta, per modellare una situazione del mondo reale mediante un grafo, può risultare necessario introdurre dei *pesi* (costi o profitti) da associare ai nodi e/o agli archi. Ad esempio, un grafo non orientato può servire a rappresentare le connessioni tra coppie di città mediante linee ferroviarie, ma non da' alcuna indicazione sulle distanze fra tali città. Per ottenere ciò sarebbe necessario associare un peso, pari alla distanza chilometrica tra la città i e la città j , per ogni coppia ij di città collegate. Un altro esempio si può applicare al caso in cui, dati n uomini e n donne, vogliamo creare n coppie per un ballo. In questo caso, si potrebbe associare ad ogni possibile coppia un peso dato dal "valore di compatibilità" dei due elementi, ossia una stima di quanto questa coppia desideri ballare insieme. In questo caso, l'obiettivo nello scegliere le coppie che balleranno, dovrebbe essere quello di ottenere un'elevata compatibilità media. Infine, supponiamo di avere alcune vie cittadine nelle quali collocare dei cassonetti per l'immondizia. Ogni coppia di vie si incontra in un incrocio e vogliamo posizionare i cassonetti negli incroci, in maniera tale che gli abitanti di ogni via trovino un cassonetto ad almeno uno dei due estremi in cui la loro via termina. A complicare il problema c'è il fatto che ci sono

incroci in cui un cassonetto è preferibile che in altri. Ad esempio, se un incrocio è una piazza storica, o c'è un monumento, sarebbe meglio evitare di mettere lì il cassonetto (tuttavia questo potrebbe essere inevitabile: ad esempio se una strada termina da entrambi i lati in piazze storiche). Per modellare questo problema, bisogna associare un peso $p(v)$ ad ogni incrocio v (ossia, ad ogni nodo del grafo che modella, in modo ovvio, il problema), e si vuole selezionare un sottoinsieme di nodi tale che: (i) di ogni lato è stato selezionato almeno un estremo, (ii) il costo medio degli estremi selezionati è minimo.

Un *grafo pesato* è una tripla $G = (V, E, p)$, dove (V, E) è un grafo e p è una funzione $p : E \mapsto \mathbb{R}$ (nel caso di pesi dei lati) o $p : V \mapsto \mathbb{R}$ (nel caso di pesi dei vertici). La definizione di *grafo orientato pesato* è perfettamente analoga. Supponiamo p sia la funzione di peso dei lati (concetti analoghi valgono per il peso dei vertici). Il numero $p(e)$, denotato anche spesso con p_e , si dice peso (o costo, o profitto) del lato $e \in E$. Dato un insieme F di lati (o di vertici), si definisce peso dell'insieme, e lo si denota con $p(F)$, il numero $p(F) := \sum_{e \in F} p(e)$.

Gli esempi di cui sopra, necessari ad introdurre i grafi pesati, verranno ripresi nelle prossime sezioni, dedicate all'*ottimizzazione combinatoria*. L'ottimizzazione combinatoria si occupa della soluzione dei problemi citati e di molti altri, di natura simile, definiti su grafi pesati o meno, o su altri oggetti matematici propri della matematica discreta.

Chapter 8

Problemi su grafi

In questo capitolo descriveremo alcuni importanti problemi di ottimizzazione (in particolare, si tratterà di esempi di *ottimizzazione combinatoria*). Questi problemi consistono, in generale, nel determinare un elemento *ottimo* all'interno di un insieme finito –ma di cardinalità tipicamente molto grande– di elementi. Ad ogni elemento si suppone associato un costo (o un profitto) e l'elemento ottimo è quello che minimizza il costo (rispettivamente, che massimizza il profitto). L'aggettivo “combinatoria” è dovuto al fatto che gli elementi dei problemi di ottimizzazione che descriveremo sono tipicamente oggetti combinatorici discreti (quali insiemi, permutazioni, grafi,...) anzichè enti “continui” (quali numeri reali irrazionali, curve, figure geometriche, ecc.).

L'importanza dei problemi che descriveremo è data dal fatto che si possono presentare in contesti diversissimi, per quanto possa non risultare immediatamente evidente che si ha a che fare proprio con uno di questi problemi. A questo proposito, è fondamentale una fase preliminare di astrazione, detta *modellizzazione*, in cui i dati di un problema reale vengono trasformati in oggetti matematici (ad esempio, nodi e lati di un grafo) e si riconosce che la soluzione ottima del problema reale può essere ottenuta tramite la risoluzione di un noto problema di ottimizzazione sull'oggetto matematico del nostro modello. Ad esempio, l'assegnazione di aule ad un insieme di corsi, il confronto di strutture proteiche, la selezione di un gruppo numeroso di persone compatibili da assegnare a un medesimo progetto, sono tutti problemi che possono essere ricondotti, più o meno facilmente, al problema di ottimizzazione della *massima clique* (trovare la clique di cardinalità massima in un grafo). È importante conoscere quanti più problemi di ottimizzazione “classici” possibile, in modo da poter essere in grado di riconoscere se un dato problema reale è riconducibile ad uno di essi. Si noti però che non sempre (anzi, raramente) i problemi di ottimizzazione “classici” risultano di facile soluzione (esiste una loro classificazione, dovuta alla *Teoria della Complessità*, che permette di affermare che un problema è “facile” o “difficile”). Lo studio della complessità dei problemi esula dal contesto di stretta pertinenza della Matematica Discreta, e pertanto non sarà qui affrontato. Tuttavia, cercheremo, quando possibile, di accennare alla complessità dei problemi introdotti, in modo che la fase di modellizzazione possa anche portare a concludere che il problema reale di partenza è facile o difficile, a seconda della complessità del corrispondente problema di ottimizzazione individuato.

8.1 Il minimo albero di supporto

Dato un grafo pesato $G = (V, E, c)$, con $c(e) \geq 0$ per ogni $e \in E$, vogliamo determinare un albero di supporto di costo minimo. Il costo di un albero di supporto $T = (V, E_T)$ è definito come

$$c(T) := \sum_{e \in E_T} c(e).$$

Il grafo G (che supponiamo connesso) può essere completo o meno. Non c'è perdita di generalità ad assumere che G sia completo, in quanto, se non lo fosse, potremmo aggiungere i lati mancanti e dare a loro un costo "infinito" (i.e., un costo sufficientemente alto da garantire che ciascuna soluzione che usa uno di questi archi sia peggiore di quelle che non li usano). È facile verificare che ogni soluzione ottima necessariamente userà solo gli archi originali.

Per il problema del minimo albero di supporto (detto anche MST, dall'inglese Minimum Spanning Tree) è possibile l'utilizzo di un algoritmo *greedy* (avido, ingordo). L'approccio greedy a un problema consiste nel fare scelte che massimizzano il profitto immediato, senza preoccuparsi del fatto che queste scelte possano portare a dei problemi in futuro. L'approccio greedy in generale non porta alla soluzione ottima di un problema. Ad esempio, supponendo di avere 100 euro con i quali vogliamo comprare un paio di scarpe e un paio di jeans, l'approccio greedy porterebbe ad acquistare il primo paio di scarpe che ci piace (anche se costasse 99 euro!), salvo poi renderci conto che non abbiamo più abbastanza soldi per i jeans. L'approccio corretto, in questo esempio, consisterebbe nel raccogliere i prezzi di tutte le scarpe e tutti i jeans che ci piacciono, e scegliere la coppia che più ci piace tra quelle che possiamo effettivamente permetterci. Nel caso del MST l'approccio greedy consiste nello scegliere i lati da mettere nella soluzione ottima (l'albero che stiamo costruendo) cercando sempre di aggiungere il lato di costo minimo tra quelli ancora disponibili. Faremo ora vedere come una tale strategia produce sempre, per questo problema, una soluzione ottima.

Dato un insieme A di lati, diciamo che A è un *insieme estendibile* se esiste almeno un albero $T^* = (V, E_{T^*})$ di costo minimo tale che $A \subseteq E_{T^*}$. Se A è un insieme estendibile, ed $e \in E - A$ è tale che $A \cup \{e\}$ è ancora un insieme estendibile, allora e si dice un *lato sicuro per A* . Chiaramente, una condizione perchè un insieme di lati sia estendibile è che sia aciclico. Inoltre, l'insieme vuoto è sicuramente estendibile.

La seguente procedura rappresenta uno schema generico per la costruzione di un MST:

Algorithm 5 GENERICMST

1. $A := \emptyset$;
 2. **for** $i := 1$ **to** $|V| - 1$ **do**
 3. Trova un lato $e \in E - A$ sicuro per A ;
 4. $A := A \cup \{e\}$;
 5. **endfor**
-

Si noti che al termine della procedura siamo sicuri di aver selezionato esattamente i lati di un albero. Infatti un albero ha $|V| - 1$ lati. Inoltre, l'albero ha costo minimo, come è immediato verificare. La procedura data non può però ancora dirsi un algoritmo, in quanto il passo 3. è descritto troppo genericamente, e non è chiaro in che modo si possa determinare un lato sicuro. Diamo ora una condizione sufficiente (ma non necessaria) perchè un lato e sia sicuro per un insieme estendibile A .

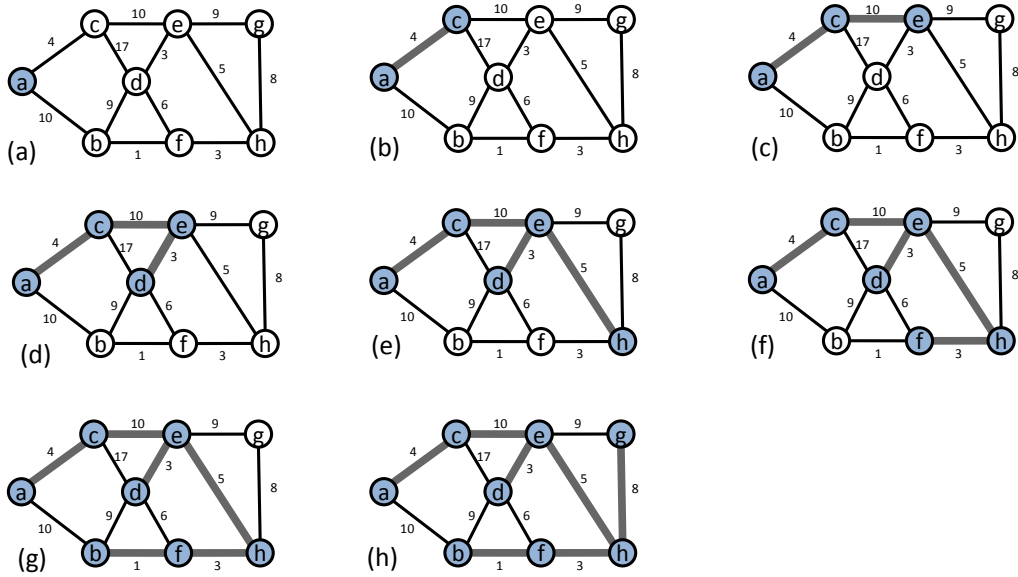


Figure 8.1: Esecuzione dell'algoritmo di Prim. I nodi ombreggiati indicano il sottoalbero del MST fino all'iterazione corrente. A questo sottoalbero, viene aggiunto ogni volta un lato di costo minimo tra quelli appartenenti al taglio definito dal sottoalbero corrente. I lati entranti nel MST sono indicati con una linea più spessa.

TEOREMA 42: Sia A un insieme estendibile e sia V' l'insieme dei vertici di una qualsiasi componente connessa di $G[A]$ (il grafo indotto da A). Sia e un lato in $\delta(V')$. Se avviene che $c(e) \leq c(a)$ per ogni $a \in \delta(V')$, allora e è sicuro per A .

Dim: Sia $e = ij$, con $i \in V'$ e $j \notin V'$ e sia $T^* = (V, E_{T^*})$ un albero di supporto di costo minimo tale che $A \subseteq E_{T^*}$. Se $e \in E_{T^*}$ allora e è sicuro. In caso contrario, esiste in T^* un cammino tra i e j , che non comprende l'arco e . Tale cammino contiene, necessariamente, un lato f in $\delta(V')$. Sostituendo f con e si ottiene un nuovo albero di supporto, sia esso T' , di costo non-maggiore del precedente (in quanto $c(e) \leq c(f)$). In particolare, visto che T^* aveva costo minimo, anche T' ha costo minimo. Siccome tra gli archi di T' c'è anche e , e è un lato sicuro per A . ♣

Si noti che la condizione non è necessaria. Ad esempio, se G stesso è un albero, ogni lato è sicuro.

Strategie di Prim e Kruskal

La scelta di un lato sicuro può essere fatta seguendo una tra due strategie popolari, chiamate la strategia di Prim e quella di Kruskal. Entrambe le strategie partono da un insieme estendibile vuoto, e quindi tale da indurre una foresta di n componenti connesse, ognuna consistente di un solo nodo. Inoltre, in entrambe le

strategie, ad ogni passo vengono collegate due componenti connesse, diciamo a e b , finchè alla fine rimane una sola componente connessa. Le differenze tra i due metodi sono le seguenti:

- **Prim:** Nella strategia di Prim, la componente a è sempre la componente che contiene un ben determinato nodo (per convenzione, diciamo il nodo v_1). Quindi, la componente b consiste di un singolo nodo, e possiamo vedere il processo come la crescita di un albero a (inizialmente dato dal nodo v_1) che ad ogni passo si “mangia” un nuovo nodo. Ad ogni iterazione, il lato sicuro che viene aggiunto è il lato di costo minimo tra quelli in $\delta(a)$. Si veda la figura 8.1 per un esempio di applicazione dell’algoritmo di Prim.
- **Kruskal:** nella strategia di Kruskal, a e b possono essere due qualsiasi componenti connesse della foresta corrente. Il processo può essere visto come un passaggio progressivo da una foresta ad un albero, ed ad ogni passo due generici alberi della foresta vengono fusi fra loro. La scelta delle componenti a e b da fondere è data dal seguente criterio: si trova il lato di costo minimo tra quelli i cui estremi non sono entrambi in una stessa componente connessa e si fondono le due componenti a cui tali estremi appartengono. Si veda la figura 8.2 per un esempio di applicazione dell’algoritmo di Kruskal.

Sia nella strategia di Prim che in quella di Kruskal, se ad un passo ci sono più lati possibili da utilizzare (ossia tutti hanno costo minimo in $\delta(a)$), se ne può scegliere uno arbitrariamente.

La strategia di Kruskal può essere realizzata efficacemente come segue. Si ordinino i lati di E in ordine di costo non-decrescente, ossia in modo tale che $c(e_1) \leq c(e_2) \leq \dots \leq c(e_{|E|})$. Partendo con $|V|$ componenti connesse, consistenti ciascuna di un solo nodo, si scandisca poi questa lista per $k = 1, \dots, |E|$. Se l’arco e_k collega estremi nella stessa componente connessa, lo si scarti. Se invece collega estremi in due componenti distinte, si fondano le due componenti e si inserisca l’arco nella soluzione.

Casi speciali di MST

Il problema del MST è stato presentato assumendo che tutti i lati abbiano costi non-negativi. Facciamo ora vedere come la presenza di eventuali costi negativi non altera la complessità del problema. Infatti, supponiamo che i costi c non siano necessariamente non-negativi, e sia $C = \min_e c(e)$. Ridefinendo i costi dei lati come $c'(e) := c(e) - C$, abbiamo che $c'(e) \geq 0$ per ogni $e \in E$. Inoltre, per ogni albero di supporto T si ha $c'(T) = c(T) - (n-1)C$ (in quanto ogni albero ha esattamente $n-1$ lati). Pertanto, dati due alberi T_1 e T_2 si avrà $c'(T_1) \leq c'(T_2)$ se e solo se $c(T_1) \leq c(T_2)$. Quindi, per trovare l’albero di costo minimo per i costi originali, $c(\cdot)$, basta trovare l’albero di costo minimo per i nuovi costi $c'(\cdot)$, i quali sono tutti non-negativi.

Da questo risultato consegue anche che il problema di trovare l’albero di supporto di costo *massimo* può essere risolto allo stesso modo che per il costo minimo. Siccome per ogni funzione f si ha $\min f(x) = -\max(-f(x))$, basta definire $w(e) = -c(e)$ per ogni $e \in E$, in modo tale che T ha costo minimo per $w(\cdot)$ se e solo se ha costo massimo per $c(\cdot)$.

ESERCIZIO 8.1. Si applichino le procedure di Prim e Kruskal al seguente problema di MST. Sia $V = \{1, 2, 3, 4, 5, 6\}$, $E = \{12, 13, 23, 34, 35, 45, 46, 56\}$, $c(12) = 5$, $c(13) = 4$, $c(23) = 2$, $c(34) = 8$, $c(35) = 7$, $c(45) = 1$, $c(46) = 3$, $c(56) = 4$. \diamond

ESERCIZIO 8.2. Negli esempi di procedure di Prim e Kruskal riportate in figura 8.1 e figura 8.2, esistono dei passaggi in cui la scelta su quale arco inserire nel MST non è univoca. Si riesegnano le procedure su tali

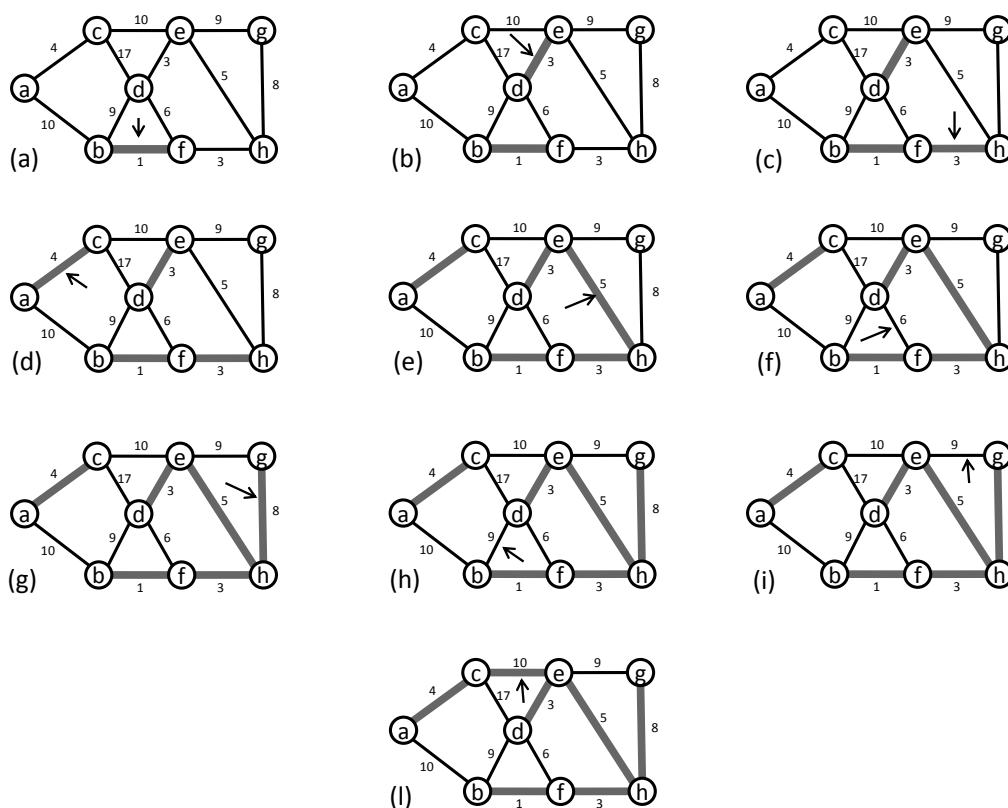


Figure 8.2: Esecuzione dell'algoritmo di Kruskal. I lati più spessi sono quelli selezionati nella foresta che viene fatta crescere. Ad ogni iterazione, la freccia punta al lato che viene preso in considerazione per essere inserito nel MST. Se il lato collega due componenti distinte, esso viene aggiunto al MST, mentre se entrambi i suoi estremi sono nella stessa componente, esso viene scartato.

esempi prendendo una strada alternativa a quella riportata nelle figure. \diamond

ESERCIZIO 8.3. Vero o falso: (i) L'albero di supporto di costo minimo è unico se e solo se tutti i costi degli archi sono diversi fra loro. (ii) Sia e un arco di costo minimo in G . Allora e è in ogni albero di supporto di costo minimo. \diamond

8.2 Accoppiamenti e coperture

Un *accoppiamento* (o *matching*) in un grafo $G = (V, E)$ è un insieme di lati M a due a due non adiacenti, ossia tali che non hanno alcun estremo in comune. Un modo alternativo per esprimere il medesimo concetto è che M è un matching se nel grafo $G[M] = (V, M)$ ogni nodo ha grado al più 1.

Un matching si dice *perfetto* se in $G[M]$ ogni nodo ha grado esattamente 1. Chiaramente, una condizione

necessaria per l'esistenza di un matching perfetto è che $|V|$ sia pari.

ESERCIZIO 8.4. Quanti sono i matching perfetti possibili nel grafo completo K_{2n} ? \diamond

Dato un matching M , un *cammino alternante* è un cammino fatto di lati di M alternati a lati di $E - M$ (può cominciare, indifferentemente, con un lato di M o di $E - M$). Un nodo si dice *esposto* se non c'è un lato di M ad esso incidente, mentre in caso contrario si dice *saturo* o *coperto* da M . Un cammino alternante fra due nodi esposti si dice *cammino aumentante* per M .

Un importante problema di ottimizzazione consiste nel trovare un matching di cardinalità massima (detto anche un *matching massimo*) in un grafo assegnato. Il seguente teorema caratterizza i matching massimi:

TEOREMA 43: Un matching M è massimo se e solo se non ci sono cammini aumentanti per M .

Dim: Una direzione è ovvia: se M ammette un cammino aumentante $v_1, v_2, v_3, \dots, v_k$ il matching può essere migliorato come segue: si rimuovano da M i lati v_2v_3, v_4v_5, \dots e si inseriscano in M i lati $v_1v_2, v_3v_4, \dots, v_{k-1}v_k$. Quello che si ottiene è ancora un matching, di cardinalità maggiore (di un'unità) rispetto al precedente.

Per la direzione opposta, si assuma che M non sia massimo, e sia M^* un matching massimo. Sia $E' := M^* \Delta M$. Nel grafo $G[E']$ ogni nodo ha grado ≤ 2 , e quindi $G[E']$ consiste di cicli disgiunti e cammini. Sia i cicli che i cammini alternano lati di M^* e M . I cicli (che hanno necessariamente lunghezza pari) e i cammini di lunghezza pari contengono lo stesso numero di lati di M^* che di M . I rimanenti cammini, di lunghezza dispari, possono (i) cominciare e finire con un lato di M o (ii) cominciare e finire con un lato di M^* . Siccome $|M^*| > |M|$, ci deve essere almeno un cammino di tipo (ii). Ma un tale cammino è un cammino aumentante per M . \clubsuit

Dal teorema 43 si ricava una procedura per trovare il matching massimo in grafi generici. La procedura, descritta nell'algoritmo GENERIC-MAXMATCHING, consiste nell'iterare un ciclo di ricerca di cammini aumentanti, partendo con un matching arbitrario M (al limite, il matching vuoto).

Algorithm 6 GENERIC-MAXMATCHING

1. **while**(esistono cammini aumentanti in M)
2. Si trovi un cammino aumentante $p = v_1, v_2, \dots, v_k$;
3. /* aumento */ Si ponga

$$M := M - \{v_2v_3, v_4v_5, \dots, v_{k-2}v_{k-1}\} \cup \{v_1v_2, v_3v_4, \dots, v_{k-1}v_k\}$$

9. **endwhile**.
-

Per poter risultare efficace, la procedura illustrata deve essere in grado di risolvere il passo 2 in maniera “veloce” (ossia, sensibilmente migliore dell'enumerazione di tutti i possibili cammini aumentanti). Inoltre bisogna che la procedura che cerca i cammini aumentanti sia tale da non trovarne se e solo se non ce ne sono, e quindi anche il test del passo 1 viene risolto in maniera “veloce”. La ricerca veloce di cammini aumentanti è possibile (per quanto assolutamente non banale) sia sui grafi generici che su quelli bipartiti. Il caso bipartito risulta molto più facile da illustrare, e pertanto ci concentreremo su quest'ultimo nel seguito.

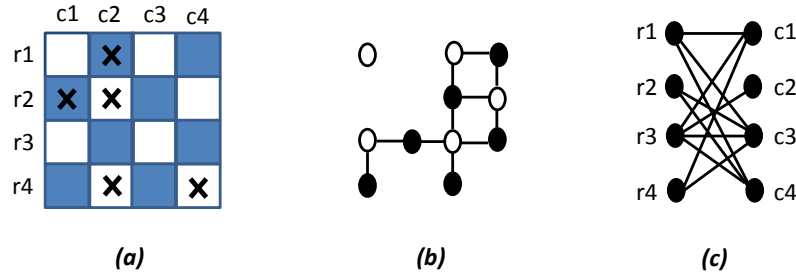


Figure 8.3: (a) La scacchiera. (b) Grafo bipartito per il domino. (c) Grafo bipartito per le torri.

Accoppiamenti massimi in grafi bipartiti

Esempio. È data una scacchiera $n \times n$, in cui k posizioni sono state marcate come “vietate” (si veda la Figura 8.3(a) per un esempio con $n = 4$ e $k = 5$). Consideriamo i seguenti problemi:

1. Avendo a disposizione dei pezzi del domino, ognuno dei quali è in grado di coprire due caselle della scacchiera, vogliamo piazzarne quanti più possibile in maniera che ogni casella sia coperta da al più un tassello del domino, e nessuna casella vietata sia coperta.
2. Vogliamo piazzare, su caselle non vietate, quante più torri possibile in maniera che non si attacchino a vicenda. Ricordiamo che, in base alle regole del gioco degli scacchi, ogni torre attacca un'altra torre piazzata sulla stessa riga o sulla stessa colonna.

Nel primo esempio, costruiamo un grafo bipartito $G_1 = (B, N, E)$, con $n^2 - k$ nodi come segue. Abbiamo un nodo per ogni casella non vietata della scacchiera. Inoltre, essendo le caselle della scacchiera bianche e nere, la ripartizione dei nodi è data dagli insiemi B (tutte le caselle bianche non vietate) e N (quelle nere non vietate). Abbiamo poi un lato tra due caselle se e solo se le stesse sono consecutive, in orizzontale o in verticale, sulla scacchiera. Siccome caselle consecutive hanno colore diverso, il grafo risulta bipartito (si veda la figura 8.3(b)). Ogni lato di G_1 individua una coppia di caselle che possono essere coperte da un pezzo del domino. Un matching corrisponde a un insieme di pezzi del domino in cui due pezzi non coprono mai la stessa casella e nessun pezzo copre una casella vietata. Quindi, il matching massimo in G_1 individua il piazzamento di un insieme massimo di pezzi del domino che rispetta le regole stabilite.

Veniamo ora al secondo problema. Anche in questo caso definiamo un opportuno grafo bipartito $G_2 = (R, C, E')$ che ha ora $n^2 - k$ lati anziché nodi. Il primo sottoinsieme di nodi, R , corrisponde alle righe della scacchiera, ed ha n elementi. Il secondo sottoinsieme, C , corrisponde alle colonne, ed ha anch'esso n elementi. Infine, c'è un lato in E' per ogni posizione non vietata della scacchiera (si veda la figura 8.3(c)). Ogni lato del grafo G_2 corrisponde al possibile piazzamento di una torre su una casella non vietata, e ogni matching individua un insieme di torri mutualmente compatibili. Quindi, il matching massimo in G_2 individua il piazzamento di un insieme massimo di torri che non si attaccano a vicenda.

◇

Nel caso di grafi bipartiti esiste una procedura efficiente per determinare un matching massimo, detta la *procedura di etichettatura*, che ora descriveremo. Sia $G = (X, Y, E)$ un grafo bipartito, con $X = \{x_1, \dots, x_n\}$ e $Y = \{y_1, \dots, y_m\}$ e sia inoltre M un matching in G . Nella corso procedura ogni nodo può avere lo status di *etichettato* o meno e di *esplorato* o meno. L'algoritmo riportato di seguito identifica, se esiste, un cammino aumentante in G , oppure affermare che non esistono cammini aumentanti:

- (1) Si etichetti ogni nodo esposto di X con l'etichetta $\langle * \rangle$.
- (2) Se al passo precedente nessun nuovo nodo in X è stato etichettato, **STOP**.
- (3) Si considerino tutti i nodi di X che risultino etichettati ma mai esplorati. Per ogni tale nodo x_i si proceda come segue:
 - (a) Si considerino tutti i nodi di Y non etichettati e collegati a x_i con lati non in M .
 - (b) Si etichetti ogni tale nodo con l'etichetta $\langle x_i \rangle$.
 - (c) Si dichiari il nodo x_i come *esplorato*.
- (4) Se al passo precedente nessun nuovo nodo in Y è stato etichettato, **STOP**.
- (5) Si considerino tutti i nodi di Y che risultino etichettati ma mai esplorati. Per ogni tale nodo y_j si proceda come segue:
 - (a) Si consideri un nodo di X non etichettato e collegato a y_j con un lato in M .
 - (b) Si etichetti tale nodo con l'etichetta $\langle y_j \rangle$.
 - (c) Si dichiari il nodo y_j come *esplorato*.
- (6) **GOTO 2**.

Si noti che la procedura deve sempre terminare. Infatti, ad ogni iterazione in cui non termina almeno un nuovo nodo viene etichettato, e nessun nodo può essere etichettato più di una volta. Inoltre, è facile convincersi del fatto che, per ogni nodo v che viene etichettato, esiste un cammino alternante da un nodo esposto a v .

Al termine della procedura, siano $L(Y)$ i nodi di Y che sono stati etichettati. Possono verificarsi due condizioni:

1. Esiste un nodo $y \in L(Y)$ esposto. Per quanto appena detto, vuol dire che c'è un cammino alternante tra un nodo esposto di X e y . Ma tale cammino risulta allora un cammino aumentante, che può essere usato per migliorare il matching corrente.
2. Non esiste alcun nodo esposto in $L(Y)$. Vogliamo allora dimostrare che questo implica che non esistono neppure cammini aumentanti. Per assurdo, sia $x_{i_1}, y_{j_1}, x_{i_2}, y_{j_2}, \dots, x_{i_k}, y_{j_k}$ un cammino aumentante, con y_{j_k} non etichettato. Questo implica che anche x_{i_k} non è stato etichettato, o sarebbe stato usato dalla procedura per etichettare y_{j_k} . A sua volta, neppure $y_{j_{k-1}}$ può essere stato etichettato, o la procedura lo avrebbe usato per etichettare x_{i_k} . Proseguendo, si arriva a concludere che neppure x_{i_1} può essere stato etichettato. Ma questo è impossibile, perchè x_{i_1} è un nodo esposto e quindi ha certamente ricevuto l'etichetta $\langle * \rangle$.

Esempio. Consideriamo il grafo bipartito $G = (X, Y, E)$ con $X = \{x_1, \dots, x_6\}$ e $Y = \{y_1, \dots, y_6\}$ riportato in figura 8.4(a). Prendiamo il matching iniziale $M = \{x_2y_2, x_3y_3, x_4y_4\}$ e applichiamo ad esso la procedura di etichettatura per cercare un cammino aumentante:



Figure 8.4: (a) Matching iniziale ed etichettatura. (b) Matching finale massimo.

- (i) (Passo 1) I vertici x_1, x_5 ed x_6 sono esposti e vengono etichettati con $\langle * \rangle$.
- (ii) (Passo 3) Esaminiamo, uno alla volta, i vertici x_1, x_5 e x_6 ed etichettiamo y_3 con $\langle x_1 \rangle$ ed y_4 con $\langle x_5 \rangle$. Siccome tutti i vertici adiacenti a x_6 sono già etichettati, nessun vertice di Y riceve l'etichetta $\langle x_6 \rangle$.
- (iii) (Passo 5) Esaminiamo, uno alla volta, i vertici y_3 ed y_4 che erano stati etichettati in (ii) ed etichettiamo x_3 con $\langle y_3 \rangle$ ed x_4 con $\langle y_4 \rangle$.
- (iv) (Passo 3) Esaminiamo, uno alla volta, i vertici x_3 ed x_4 che erano stati etichettati in (iii) ed etichettiamo y_2 con $\langle x_3 \rangle$.
- (v) (Passo 5) Esaminiamo il vertice y_2 etichettato in (iv) ed etichettiamo x_2 con $\langle y_2 \rangle$.
- (vi) (Passo 3) Esaminiamo il vertice x_2 etichettato in (v) ed etichettiamo y_1, y_5 ed y_6 con $\langle x_2 \rangle$.
- (vii) (Passo 5) Esaminiamo, uno alla volta, i vertici y_1, y_5 ed y_4 che erano stati etichettati in (vi) e scopriamo che non è più possibile etichettare alcun nodo.

L'algoritmo è terminato, e siccome alla fine un nodo esposto di Y è stato etichettato (in effetti, più d'uno, i.e., i vertici y_1, y_5 e y_6) abbiamo trovato un cammino aumentante. Tracciando il cammino all'indietro, a partire dal nodo y_1 ed usando le etichette per trovare i nodi successivi, ricostruiamo il seguente cammino aumentante:

$$C = y_1, x_2, y_2, x_3, y_3, x_1.$$

Rimuoviamo da M i lati $\{x_2y_2, x_3y_3\}$ ed inseriamo in M i lati $\{x_1y_3, x_3y_2, x_2y_1\}$ ottenendo il nuovo matching descritto in figura 8.4(b). Se applichiamo al nuovo matching l'algoritmo delle etichette, notiamo che, alla terminazione, nessun nodo esposto di Y risulta etichettato e quindi il matching M è massimo. \diamond

Minima copertura di vertici

Una *copertura di vertici* in un grafo $G = (V, E)$ è un insieme $C \subseteq V$ tale che ogni lato di E è incidente in almeno un nodo di C . Un noto problema di ottimizzazione richiede di determinare una copertura C^* la cui cardinalità sia minima rispetto a tutte le possibili coperture. Questo problema è noto come il problema della *minima copertura di vertici* e C^* viene detta una *copertura ottima*. Ad esempio, supponiamo che i lati di un grafo rappresentino un insieme di strade, e i nodi rappresentino degli incroci in cui alcune strade si incontrano. Un poliziotto piazzato ad un incrocio è in grado di controllare tutte le strade che confluiscono in quell'incrocio. L'obiettivo è quello di controllare tutte le strade utilizzando il minor numero possibile di poliziotti.

Esiste anche una versione pesata del problema della copertura minima. In questo caso ad ogni nodo $v \in V$ è associato un peso p_v , rappresentante il costo in cui si incorre per coprire il nodo v , e il problema consiste nel minimizzare il costo complessivo di una copertura C , definito come $p(C) = \sum_{v \in C} p_v$. Si tratta di un problema computazionalmente difficile (NP-hard) in generale, anche nel caso non pesato. Se però il grafo G è bipartito, allora il problema può essere risolto in modo efficace, come vedremo fra breve, utilizzando l'algoritmo per la ricerca di un matching massimo ed alcuni risultati che legano accoppiamenti e coperture. Il primo e fondamentale risultato di tale natura è il seguente:

TEOREMA 44: Dato un grafo G , per ogni matching M e copertura C in G si ha $|M| \leq |C|$.

Dim: Ogni lato di M deve essere coperto da almeno un nodo di C , e nessun nodo di C può coprire più di un lato di M . ♣

Dal teorema 44 segue che, detto M^* un matching massimo e C^* una copertura minima, si ha

$$|M^*| \leq |C^*|. \quad (8.1)$$

Tutte le volte in cui, per un matching M e una copertura C si ha $|M| = |C|$ si può concludere che M è un matching massimo e C una copertura minima. Tuttavia non è necessariamente vero che, confrontando gli ottimi dei due problemi, l'uguaglianza valga sempre: ad esempio, se G è il triangolo K_3 , il matching massimo contiene un solo lato, ma la copertura minima richiede due vertici. Come vedremo nella prossima sezione, questa discrepanza tra i valori ottimi dei due problemi si ha in effetti solo quando G non è un grafo bipartito.

Il caso bipartito

Cominciamo la sezione dimostrando il seguente teorema.

TEOREMA 45: Sia $G = (V_1, V_2, E)$ un grafo bipartito, e sia M un matching di cardinalità massima. Allora esiste una copertura di vertici C tale che

$$|M| = |C| \quad (8.2)$$

(chiaramente, C è una copertura minima di G).

Dim: Dimostriamo il teorema per induzione su $|E|$. Se $|E| = 1$, chiaramente il matching massimo ha valore 1, ed inoltre un solo nodo è sufficiente per coprire tutti i lati. Supponiamo ora $|E| = k > 1$ e che il

teorema valga per $|E| = 1, 2, \dots, k-1$. Se non c'è alcun nodo esposto in G , allora il matching è perfetto, e, necessariamente, $|M| = |V_1| = |V_2|$. Ma, in questo caso, la copertura C consistente in tutti vertici di V_1 , ha la stessa cardinalità di M , e quindi è ottima. Altrimenti, sia $uv \in E$ tale che $u \in V_1$ è un nodo esposto (un ragionamento analogo vale nel caso u sia un nodo esposto di V_2). Siccome M è massimo, v non può essere esposto, e quindi esiste un arco $iv \in M$. Si rimuova dal grafo il nodo v nonchè tutti gli archi a lui incidenti. Sia G' il grafo risultante e $M' = M - \{iv\}$ il matching rimanente. Facciamo vedere che non esistono cammini aumentanti per M' in G' (e quindi M' è massimo per G'). Per assurdo, sia x, \dots, y un tale cammino aumentante, con $x \in V_1$ e $y \in V_2$, nodi esposti. Siccome x non poteva essere esposto in G (altrimenti si sarebbe avuto un cammino aumentante in G), deve essere $x = i$. Ma allora $u, v, i = x, \dots, y$ sarebbe un cammino aumentante in G , assurdo.

Quindi M' è un matching ottimo in G' e, per induzione, esiste una copertura C' di G' con $|C'| = |M'|$. Ma allora $C := C' \cup \{v\}$ è una copertura di G con

$$|C| = |M'| + 1 = |M|.$$



Si noti che la dimostrazione del teorema suggerisce la seguente procedura iterativa per determinare una copertura di vertici C ottima a partire da un matching M ottimo. Si costruisce C (partendo con $C := \emptyset$), prendendo esattamente un estremo da ogni arco di M , in questo modo:

1. Se non ci sono nodi esposti in V_1 nè in V_2 , si ponga $C := C \cup V_1$ e si termini la procedura.
2. Altrimenti, sia $ij \in M$ con $i \in V_1$ collegato a un nodo esposto di V_2 (nel qual caso si ponga $v := i$), oppure $j \in V_2$ collegato a un nodo esposto di V_1 (nel qual caso si ponga $v := j$).
3. Si aggiorni il grafo togliendo il nodo v , tutti gli archi incidenti in v , e gli eventuali nodi isolati (si noti che l'aggiornamento può rendere esposto un nodo che prima non lo era), si aggiunga v a C ($C := C \cup \{v\}$) e si torni al passo 1.

Dal teorema 45 si può ricavare un'importante condizione, necessaria e sufficiente, per l'esistenza di matching perfetti in grafi bipartiti. Dato un grafo bipartito $G = (V_1, V_2, E)$ e un sottoinsieme W di nodi dello stesso colore (ossia $W \subseteq V_1$ o $W \subseteq V_2$), denotiamo con $N(W)$ l'insieme dei nodi adiacenti a nodi di W . Abbiamo il

TEOREMA 46: (Condizione di Hall) Un grafo G bipartito ha un matching perfetto se e solo se per ogni sottoinsieme W di nodi dello stesso colore si ha $|W| \leq |N(W)|$.

Dim: Una direzione è ovvia: se per un sottoinsieme W si avesse $|W| > |N(W)|$, sarebbe impossibile accoppiare tutti nodi di W (il principio della piccionaia porterebbe ad avere due o più archi del matching incidenti in uno stesso nodo di $N(W)$). Per quel che riguarda la direzione opposta, supponiamo la condizione di Hall verificata da ogni W . Questo implica che $|V_1| = |V_2|$ (basta prendere, a turno, $W = V_1$ e $W = V_2$). Sia $n = |V_1|$ e supponiamo che esista una copertura $C = C_1 \cup C_2$, con $C_1 \subseteq V_1$ e $C_2 \subseteq V_2$, tale che $|C| < n$. Definiamo $W_i = V_i - C_i$; siccome C è una copertura, non ci sono lati tra W_1 e W_2 e quindi $N(W_1) = C_2$ e $N(W_2) = C_1$. Abbiamo allora

$$|W_1| = n - |C_1| > |C_1| + |C_2| - |C_1| = |C_2| = |N(W_1)|$$

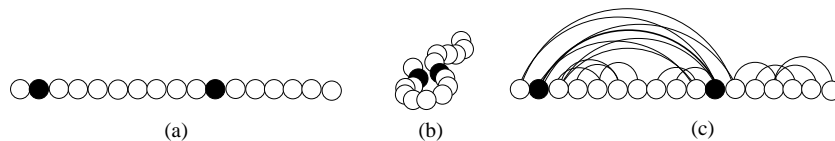


Figure 8.5: (a) Una proteina non ripiegata. (b) La sua struttura 3-D. (c) Il grafo della mappa dei contatti.

e la condizione di Hall risulta, assurdamamente, violata. Pertanto, la copertura minima non può avere meno di n nodi, e, siccome V_1 è una copertura, la copertura minima ha esattamente n nodi. Quindi, dal Teorema 45, si deduce che il matching massimo ha n nodi, ed è perciò un matching perfetto. ♣

Dal precedente teorema possiamo ricavare un interessante corollario.

TEOREMA 47: Sia $G = (V_1, V_2, E)$ un grafo bipartito d -regolare, con $d \geq 1$. Allora in G esiste un matching perfetto.

Dim: Consideriamo un qualsiasi sottoinsieme W di V_1 (o, equivalentemente, di V_2). Da W escono esattamente $d \cdot |W|$ lati, che entrano in $N(W)$. Se $|W| > |N(W)|$, per il principio della piccionaia esisterebbe almeno un nodo di $N(W)$ in cui entrerebbero più di d lati, ma questo è impossibile perchè il grafo è d -regolare. Quindi le condizioni di Hall sono soddisfatte e si conclude che esiste un matching perfetto. ♣

8.3 Clique e insieme indipendente

Dato un grafo $G = (V, E)$, un insieme Q di nodi a due a due adiacenti è detto una *clique*. Un insieme S di nodi a due a due non adiacenti è detto un *insieme indipendente* o *insieme stabile*. Il problema di ottimizzazione (in entrambi i casi) consiste nel determinare l'insieme di cardinalità massima. Si noti che i due problemi sostanzialmente si equivalgono, nel senso che si può passare dall'uno all'altro semplicemente rimpiazzando un grafo con il grafo complementare: A è una clique in G se e solo se A è un insieme indipendente in \bar{G} . Il problema di determinare la massima clique in un grafo rientra nella categoria dei problemi computazionalmente difficili (i.e., NP-hard), per i quali non sono note procedure efficienti. Si noti inoltre che C è una copertura di vertici se e solo se il suo complementare $V - C$ è un insieme indipendente. Pertanto trovare insiemi indipendenti grandi è altrettanto difficile che trovare coperture di vertici di bassa cardinalità.

Sia della clique che dell'insieme indipendente esistono delle versioni pesate, in cui ogni nodo i ha associato un profitto w_i , e si vuole trovare l'insieme S che massimizza il profitto complessivo, definito da $w(S) := \sum_{v \in S} w_v$.

Esempio. Una *mappa dei contatti* è una rappresentazione bi-dimensionale di una struttura proteica tri-dimensionale. Quando una proteina si ripiega, due residui che non erano vicini nella sequenza lineare della proteina, possono terminare vicini l'un l'altro nello spazio tridimensionale (si veda la figura 8.5 (a) e (b)).

La mappa dei contatti di una proteina con n residui è una lista delle coppie di residui che si trovano a una “piccola” distanza (tipicamente, non più di 5\AA) l'uno dall'altro nella ripiegatura della proteina. Ogni

tale coppia di residui si dice anche essere *in contatto*. La mappa dei contatti può anche essere interpretata come un grafo, in cui ogni residuo è un vertice, e ogni lato collega una coppia di residui in contatto (si veda la figura 8.5 (c), dove sono evidenziati solo contatti tra residui non consecutivi).

Uno dei problemi più importanti della proteomica è la determinazione della funzione svolta da una proteina. A tal fine, siccome la funzione di una proteina dipende in massima parte dalla sua struttura tridimensionale, è importante essere in grado di confrontare una struttura nuova con altre strutture note (in modo che, per analogia, se le due strutture si somigliano anche la funzionalità delle proteine sarà presumibilmente simile). Un modo per valutare la somiglianza di due strutture proteiche è quello di valutare la somiglianza delle loro mappe di contatto. L'obiettivo è quello di determinare se ci sono numerose coppie di residui nelle due proteine che “si comportano allo stesso modo” (ossia, che sono in contatto in entrambe le proteine). Tali residui vengono considerati *equivalenti*.

Supponiamo allora date due mappe di contatto (che, per quanto si è detto prima, sono sostanzialmente due grafi): $G_1 = (V_1, E_1)$ e $G_2 = (V_2, E_2)$. Numeriamo i residui secondo il loro ordine nella sequenza lineare della proteina, in modo che $V_1 = \{1, 2, \dots, n_1\}$ e $V_2 = \{1, 2, \dots, n_2\}$ (si noti che non è richiesto che le due proteine abbiano la stessa lunghezza). Per determinare un insieme di residui equivalenti, bisogna scegliere due sottoinsiemi $A \subseteq V_1$ e $B \subseteq V_2$ con $|A| = |B|$. Sia $A = \{a_1, \dots, a_k\}$ e $B = \{b_1, \dots, b_k\}$, con $a_1 < \dots < a_k$ e $b_1 < \dots < b_k$. Allora, si dice che a_i è equivalente a (o *allineato con*) b_i , per ogni $1 \leq i \leq k$. Si noti che l'allineamento rispetta l'ordine dei residui: se a è allineato a b , un residuo che segue a nella prima proteina può solo essere allineato a un residuo che segua b nella seconda. Il valore di un allineamento è dato dal numero di coppie in contatto nella prima proteina che sono allineate con coppie in contatto nella seconda. Tanto maggiore è questo valore, tanto più simili sono le proteine. Per trovare il numero massimo di tali coppie, costruiamo un nuovo grafo G_C (il grafo dei conflitti per i contatti). In G_C inseriamo un nodo (denominato N_{lg}) per ogni $l \in E_1$ e $g \in E_2$. Siano $e = ij \in E_1$, $e' = i'j' \in E_1$, ed $f = uv \in E_1$, $f' = u'v' \in E_2$. I due nodi N_{ef} e $N_{e'f'}$ sono collegati da un lato in G_C se è *impossibile* che i sia equivalente a u e j sia equivalente a v e, *contemporaneamente*, i' sia equivalente a u' e j' sia equivalente a v' . Quindi, ogni equivalenza corretta (i.e., ogni allineamento ammissibile), deve scegliere se allineare i con u e j con v oppure i' con u' e j' con v' (quindi uno dei contatti comuni (e, f) ed (e', f') deve essere perso).

Sia $R = \{i, j, i', j'\}$ e $S = \{u, v, u', v'\}$. Nel piano cartesiano, si considerino i $|R|$ punti di coordinate $(r, 0)$ con $r \in R$, e i $|S|$ punti di coordinate $(s, 1)$, con $s \in S$. Per vedere se esiste il lato tra N_{ef} e $N_{e'f'}$, si colleghino i punti $(i, 0)$ con $(u, 1)$, $(j, 0)$ con $(v, 1)$, $(i', 0)$ con $(u', 1)$ e $(j', 0)$ con $(v', 1)$ determinando (al più) 4 segmenti diversi. Allora (e, f) ed (e', f') sono compatibili (cioè *non* esiste il lato tra N_{ef} e $N_{e'f'}$ in G_C) se e solo se questi segmenti hanno, a due a due, intersezione vuota.

Una volta calcolato G_C , un insieme di coppie equivalenti che siano in contatto in entrambi i grafi, coincide con un insieme indipendente in G_C . Pertanto, il problema di determinare la somiglianza delle mappe dei contatti si può risolvere trovando *il più grande* insieme indipendente di G_C . \diamond

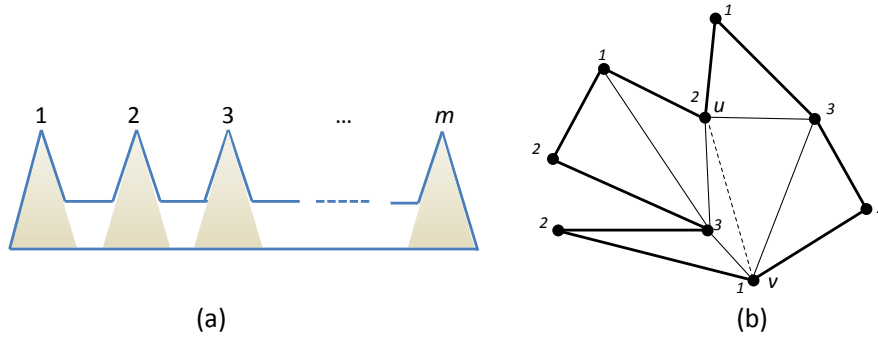


Figure 8.6: (a) Un museo "problematico". (b) Il caso generale.

8.4 Colorazione di grafi

Colorazione di vertici.

Dato un grafo $G = (V, E)$, una sua *colorazione di vertici* (o, più semplicemente, una *colorazione* qualora non ci sia pericolo di fraintendimento con la colorazione degli archi) *con k colori* è una funzione $c : V \mapsto \{1, 2, \dots, k\}$. Il numero $c(i)$ è detto il colore del vertice i . Si dice che la colorazione è *ammissibile* (o *valida*) se

$$c(i) \neq c(j) \quad \forall ij \in E. \quad (8.3)$$

Dato un numero r , un grafo si dice *r -colorabile* se esiste una sua colorazione ammissibile che usa al più r colori. Si noti che un grafo è bipartito se e solo se è 2-colorabile. Si noti inoltre che colorare un grafo con k colori corrisponde a partizionarne i vertici in k insiemi indipendenti.

Il seguente problema è detto problema della *vertice-colorazione dei grafi*: "Dato un grafo G determinare il numero minimo di colori per il quale esiste una colorazione ammissibile di G ." Tale numero è detto il *numero cromatico* di G , ed è indicato con $\chi(G)$.

Sia $\omega(G)$ il *numero della clique* di G , definito come la dimensione della massima clique in G . Allora è facile verificare che vale la relazione

$$\chi(G) \geq \omega(G).$$

Per un esempio di caso in cui la disuguaglianza vale in senso stretto si consideri K_3 , per il quale $\chi(K_3) = 3$ e $\omega(K_3) = 2$.

Il problema di riconoscere se un grafo è bipartito è facile (ossia, esiste una procedura efficiente per verificare se un grafo è bicolore). Tuttavia, per ogni $r > 2$, il problema di riconoscere se un grafo è r -colorabile è difficile, altrettanto difficile che determinare la dimensione di una clique massima nel grafo.

Le guardie del museo. Supponiamo di voler sorvegliare un museo, in cui i quadri sono appesi alle varie pareti, utilizzando il numero minimo possibile di guardiani. Visto dall'alto, il museo ha una forma poligonale chiusa, e supponiamo che un guardiano non possa spostarsi, ma solo ruotare (un po' come un faro) e osservare

tutti i punti nel suo campo visivo. Vogliamo essere sicuri che ogni punto del museo sia sotto controllo da parte di uno dei guardiani utilizzati nella soluzione.

Una figura poligonale si dice *convessa* se, presi due qualsiasi punti al suo interno, il segmento che li congiunge è interamente contenuto nella figura. In caso contrario, la figura si dice non-convessa. Chiaramente, se il museo ha forma convessa, un solo guardiano è sufficiente a sorvegliarlo. Se invece il museo ha una forma poligonale non convessa, il numero di guardiani necessario dipenderà dal numero di pareti da sorvegliare. Indichiamo con n il numero di pareti del museo. La figura 8.6(a) illustra un caso in cui almeno $\lfloor n/3 \rfloor$ guardiani sono necessari per la sorveglianza. In questo esempio, $n = 3m$ ed esistono m triangoli disgiunti tali che, per poter osservare i punti al loro interno, dobbiamo piazzare un guardiano in ognuno di essi. La soluzione richiede quindi almeno $m = \lfloor n/3 \rfloor$ guardiani (in effetti, esattamente m).

Facciamo ora vedere come di fatto questo sia il caso peggiore possibile, ossia come $\lfloor n/3 \rfloor$ siano sempre sufficienti. La dimostrazione, molto elegante, si articola in tre passi:

1. *Triangolazione.* Il poligono P definito dalla forma del museo viene scomposto in un'unione di triangoli, congiungendo via via le coppie dei suoi vertici con dei segmenti interamente contenuti nel poligono. Esistono diverse triangolazioni ed è facile convincersi (anche se un po' fastidioso da dimostrare) che una triangolazione è sempre possibile per qualsiasi figura poligonale chiusa. Si veda la figura 8.6(b) per un esempio.
2. *Colorazione.* Si considera il grafo $G = (V, E)$ in cui i vertici V sono i vertici di P (i.e., gli angoli del museo) e i lati E sono tutte le pareti del museo e tutti i segmenti introdotti dalla triangolazione. Dimostriamo ora che il grafo G è 3-colorabile. La dimostrazione procede per induzione su n . Per $n = 3$ il poligono è un triangolo e quindi 3-colorabile. Per $n > 3$ si consideri uno dei segmenti introdotti dalla triangolazione. Sia uv tale segmento. Il segmento uv divide P in due poligoni che chiamiamo P' e P'' . Per induzione, sia P' che P'' sono 3-colorabili, e siano c' e c'' delle 3-colorazioni dei loro vertici. È sempre possibile permutare i colori usati in c'' in modo tale che risulti $c'(u) = c''(u)$ e $c'(v) = c''(v)$. In questo modo si ottiene una 3-colorazione di tutti i vertici di P , in cui i vertici in P' sono colorati come in c' e quelli in P'' come in c'' . Nella figura 8.6(b) è riportata una tale colorazione accanto ai vertici del grafo.
3. *Valor medio.* Sia $\bar{c} \in \{1, 2, 3\}$ il colore meno usato nella colorazione (nel nostro esempio, $\bar{c} = 3$). Il numero medio di volte in cui un colore è usato è $n/3$ per cui il colore meno usato è usato al massimo $n/3$ volte. Siccome il numero di volte in cui è utilizzato è sempre intero, ciò significa che al più $\lfloor n/3 \rfloor$ vertici usano il colore \bar{c} . Per risolvere il problema originale, basterà allora piazzare le guardie nei vertici colorati con \bar{c} .

Colorazione di lati

Dato un grafo $G = (V, E)$, una sua *colorazione dei lati con k colori* è una funzione $c : E \mapsto \{1, 2, \dots, k\}$. Il numero $c(e)$ è detto il colore del lato $e \in E$. Si dice che la colorazione è *ammissibile* (o *valida*) se

$$c(iv) \neq c(iu) \quad \forall i, j, iu \in \delta(i) \text{ con } ij \neq iu. \quad (8.4)$$

Dato un numero r , un grafo si dice *r -lato-colorabile* se esiste una sua colorazione dei lati ammissibile che usa al più r colori. Si noti che una colorazione dei lati con r colori corrisponde ad una partizione di E in r accoppiamenti.

Il seguente problema è detto problema della *lato-colorazione dei grafi*: “Dato un grafo G determinare il numero minimo di colori per il quale esiste una colorazione dei lati ammissibile.” Tale numero è detto l’*indice cromatico* (o il *numero lato-cromatico*) di G , ed è indicato con $\chi'(G)$. Sia $\Delta(G)$ il grado massimo di un nodo in G . Allora è facile verificare che vale la relazione

$$\chi'(G) \geq \Delta(G).$$

Per un esempio di caso in cui la disuguaglianza vale in senso stretto si consideri K_3 , per il quale $\chi'(K_3) = 3$ e $\Delta(K_3) = 2$.

Il problema di determinare l’indice cromatico di un grafo è difficile, ma risulta facile determinare una r -colorazione in cui $r \leq \chi'(G) + 1$ (ossia, se non è ottima, questa colorazione usa un solo colore in più rispetto al minimo possibile). Si tratta di un risultato molto forte, che solitamente non è possibile ottenere per la maggior parte dei problemi computazionalmente difficili dell’ottimizzazione combinatoria. Questo risultato è conseguenza di un importante teorema, del quale omettiamo la dimostrazione e riportiamo l’enunciato:

TEOREMA 48: (Vizing). Per ogni grafo G , si ha $\Delta(G) \leq \chi'(G) \leq \Delta(G) + 1$.

I numeri di Ramsey Consideriamo la seguente affermazione: *in ogni gruppo di 6 persone esistono sempre almeno 3 persone che si conoscono tutte fra loro, o almeno 3 di cui nessuno conosce gli altri due.*

Supponiamo di rappresentare la situazione precedente con un grafo di 6 nodi, in cui gli archi rappresentano le relazioni di amicizia. L’affermazione precedente diventa allora: *in ogni grafo di 6 nodi esiste sempre almeno una clique di 3 o più nodi, o almeno un insieme indipendente di 3 o più nodi.* Analogamente, se immaginiamo di colorare blu gli archi presenti nel grafo, e di aggiungere gli archi mancanti, colorandoli di rosso, l’affermazione precedente si potrebbe riformulare così: *per ogni colorazione degli archi di K_6 con i colori blu e rosso, esiste sempre almeno un triangolo blu, o almeno un triangolo rosso.*

Dimostriamo l’affermazione come segue. Supponiamo data una colorazione di K_6 e consideriamo un nodo v . Siccome il grado di v è 5 e si sono usati due colori, per il principio della piccionaia esisteranno almeno tre lati incidenti in v colorati con lo stesso colore (senza perdita di generalità, diciamo con il blu). Supponiamo che tali lati siano vx , vy e vz . Ora, se uno qualsiasi dei lati tra x , y e z fosse blu, questo lato insieme ai lati tra i suoi estremi e il nodo v darebbe un triangolo blu. Se invece nessuno dei lati tra x , y e z fosse blu, allora x , y e z individuerrebbero i vertici di un triangolo rosso.

Definiamo ora un insieme di numeri $R(n, m)$, con $n, m \geq 2$, detti i *numeri di Ramsey*:

- $R(n, m) =$ minimo numero di nodi tali che, in una qualsiasi colorazione in blu e rosso degli archi di un grafo completo con $R(n, m)$ nodi, esiste sempre almeno una clique blu di n nodi, o almeno una clique rossa di m nodi.

Ramsey ha dimostrato che tali numeri esistono per ogni $n, m \geq 2$. In base al ragionamento precedente, si ha $R(3, 3) \leq 6$. Inoltre, consideriamo il grafo K_5 colorato come segue: gli archi del ciclo $(v_1, v_2, v_3, v_4, v_5, v_1)$ rossi; gli archi del ciclo $(v_1, v_3, v_5, v_2, v_4, v_1)$ blu. Questa colorazione considera tutti gli archi di K_5 , ma non ci sono triangoli blu nè rossi, e dunque $R(3, 3) > 5$. Pertanto, $R(3, 3) = 6$.

I numeri di Ramsey risultano estremamente difficili da calcolare e solo pochissimi di tali numeri sono noti. Un caso molto facile si ha per i numeri di tipo $R(2, m)$. Infatti

$$R(2, m) = m \quad \forall m \geq 2.$$

La dimostrazione di ciò è semplice: in un grafo di m nodi colorato con due colori, basta un arco blu per avere una clique blu di 2 nodi, mentre se non ci sono archi blu, l'intero grafo è una clique rossa di m nodi. Quindi, $R(2, m) \leq m$. Ma K_{m-1} colorato interamente di rosso non ha clique blu di 2 nodi nè rosse di m nodi e quindi $R(2, m) > m - 1$.

Chiaramente, i numeri di Ramsey sono simmetrici: $R(n, m) = R(m, n)$. Questo segue dal fatto che a ogni colorazione di archi rossi e blu, ne corrisponde una a colori invertiti, in cui le clique rosse diventano blu e viceversa.

Alcuni fra i pochi numeri di Ramsey a tutt'oggi noti sono i seguenti:

$$\begin{aligned} R(3, 3) &= 6 \\ R(3, 4) &= 9 \\ R(3, 5) &= 14 \\ R(3, 6) &= 18 \\ R(3, 7) &= 23 \\ R(3, 8) &= 28 \\ R(3, 9) &= 36 \\ R(4, 4) &= 18 \\ R(5, 5) &\in \{43, \dots, 49\}. \end{aligned}$$

Ispirandosi ai numeri di Ramsey, sono stati sviluppati alcuni giochi in cui due giocatori alternativamente colorano gli archi di un grafo, ed il primo a completare un triangolo monocromatico perde. Ad esempio, nel gioco *sim*, due giocatori colorano gli archi di K_6 . Il primo giocatore usa sempre il colore rosso, e il secondo il blu. Dalla teoria dei numeri di Ramsey, sappiamo che il gioco non può mai terminare in parità. In effetti, è stato dimostrato che esiste una strategia vincente per il giocatore che muove per secondo, anche se non si tratta di una strategia di facile implementazione "a mente". In un altro gioco, due giocatori usano 3 colori per colorare gli archi di K_{17} . Ad ogni turno, il giocatore che deve muovere seleziona uno dei tre colori e colora un nuovo arco. È stato dimostrato che una colorazione degli archi di K_{17} con tre colori contiene sempre almeno un triangolo monocromatico, per cui il gioco non può terminare in parità. Non è ancora noto però se esista una strategia vincente per il primo giocatore o per il secondo.

8.5 Il commesso viaggiatore

Un commesso viaggiatore deve visitare un insieme di clienti, ciascuno dei quali risiede in una città diversa, e fare poi ritorno alla sua città di residenza. Nel suo giro (chiamato genericamente un *tour*) vuole attraversare ogni città una e una sola volta. Il suo obiettivo è quello di minimizzare la lunghezza complessiva del tour, i.e., di determinare un *tour ottimo*. Il problema può essere formulato nel seguente modo. È data una matrice quadrata $n \times n$, sia essa $C = (c_{ij})$. Il numero c_{ij} rappresenta il costo in cui si incorre per andare dalla città i alla città j . Supponendo che il tour abbia origine nella città 1, si vuole determinare una permutazione

$\pi = (\pi(1), \pi(2), \dots, \pi(n))$ dei numeri $\{1, 2, \dots, n\}$ tale che $\pi_1 = 1$ e

$$c(\pi) := \left(\sum_{i=1}^{n-1} c_{\pi(i), \pi(i+1)} \right) + c_{\pi(n), \pi(1)}$$

sia minimo possibile. Si tratta di un problema molto famoso (probabilmente il più famoso problema di ottimizzazione combinatoria) noto con la sigla TSP, dall'Inglese *Traveling Salesman Problem*. Vi sono varie applicazioni di questo problema, tra cui:

- Perforazione di schede nella produzione di circuiti integrati
- Instradamento di veicoli su rotte prefissate per visitare un insieme di clienti in modo ottimale
- Ottimizzazione di schedulazione in macchine con tempi set-up (ad es. telai nella produzione di tessuti)
- Costruzione di mappe fisiche relative all'ordine di marcatori genomici.

I dati del problema possono essere rappresentati in maniera naturale da un grafo completo definito sull'insieme di vertici $\{1, \dots, n\}$ e pesato sugli archi. Il problema consiste nel determinare un circuito hamiltoniano di lunghezza minima. Se la matrice dei costi è simmetrica (ossia, $c_{ij} = c_{ji}$ per ogni i e j) il grafo risultante sarà non orientato, e il problema corrispondente prende il nome di *TSP simmetrico (STSP)*. Se la matrice dei costi non è simmetrica, il grafo risultante sarà orientato, e il problema corrispondente prende il nome di *TSP asimmetrico (ATSP)*. Si noti infine che certe volte il problema del TSP viene presentato a partire direttamente da un grafo pesato anzichè dalla matrice delle distanze fra coppie di città. La differenza tra le due situazioni è che, nel primo caso, il grafo potrebbe risultare non completo. Tuttavia, è sempre possibile, senza perdita di generalità ricondursi a un caso di grafo pesato completo. Infatti, basta introdurre i lati mancanti, con costo "infinito" (i.e., pari a un qualsiasi numero sufficientemente grande da essere sicuri che la soluzione ottima non userà mai un arco di tale costo).

Dato il grafo completo $K_n = (V, E, c)$ pesato sui lati, sia H^* un circuito hamiltoniano di costo minimo in K_n , e sia T^* l'albero di supporto di costo minimo. Un limite inferiore alla lunghezza del tour ottimo è allora il seguente:

$$c(T^*) \leq c(H^*).$$

La dimostrazione, molto semplice, è la seguente. Togliendo un lato qualsiasi da H^* si ottiene un albero di supporto (in particolare, un cammino hamiltoniano) T tale che $c(T) \leq c(H^*)$. Ma T^* è il minimo albero di supporto, per cui $c(T^*) \leq c(T)$.

Come esempio di limitazione superiore alla lunghezza del tour ottimo abbiamo il seguente risultato:

$$c(H^*) \leq \frac{2}{n-1} c(K_n).$$

Per dimostrare questo risultato, facciamo vedere come il termine a destra della disuguaglianza rappresenta la lunghezza media di un circuito hamiltoniano in K_n , e quindi il risultato segue dal fatto che H^* è il circuito di lunghezza minima

Sia $c(C)$ la lunghezza di un generico circuito hamiltoniano C , e sia \mathcal{C} l'insieme di tutti i circuiti hamiltoniani in K_n . Siccome i circuiti sono non orientati, il loro numero è

$$|\mathcal{C}| = \frac{(n-1)!}{2}.$$

La somma delle lunghezze di tutti i tour è

$$\sum_{C \in \mathcal{C}} c(C) = \sum_{C \in \mathcal{C}} \sum_{e \in C} c_e = \sum_{e \in E} c_e |\{C : e \in C\}|.$$

Essendo il grafo completo, per ogni $e \in E$ si ha $|\{C : e \in C\}| = (n-2)!$, da cui otteniamo che la lunghezza media di un circuito è

$$\frac{\sum_{C \in \mathcal{C}} c(C)}{|\mathcal{C}|} = \frac{2(n-2)! \sum_{e \in E} c_e}{(n-1)!} = \frac{2}{n-1} \left(\sum_{e \in E} c_e \right).$$

Il problema di determinare un circuito hamiltoniano di lunghezza minima in un grafo è computazionalmente difficile (i.e., NP-hard). La sua difficoltà deriva dal fatto che persino il problema di decidere se un grafo abbia o meno un circuito hamiltoniano è difficile. Chiamiamo HC il problema di determinare se un grafo è hamiltoniano, e, a titolo di esempio, dimostriamo che la difficoltà di HC implica la difficoltà di TSP. Sia allora $G = (V, E)$ un generico grafo su cui ci chiediamo se esiste un circuito hamiltoniano. Consideriamo un problema di TSP ottenuto dando lunghezza unitaria a tutti i lati di G e completando poi G aggiungendogli i lati mancanti, ognuno con lunghezza L (dove L è un qualsiasi numero $> |V|$). Sia G' il grafo completo risultante. È chiaro che G ha un circuito hamiltoniano se e solo se la soluzione ottima del TSP in G' ha valore $< L$. Quindi, trovare la soluzione ottima del TSP deve essere difficile.

Menzioniamo infine un caso speciale del problema del TSP, il caso *metrico*. Un'istanza del TSP metrico è caratterizzata dal fatto che, per ogni terna di città i, j e k , si ha

$$c_{ij} \leq c_{ik} + c_{kj}. \quad (8.5)$$

La disuguaglianza (8.5) è detta *disuguaglianza triangolare*. Per quanto più vincolato rispetto al TSP generale, il TSP metrico risulta ancora NP-hard.

Esempio. Consideriamo n marcatori e m cloni, provenienti tutti da uno stesso cromosoma. I marcatori sono sequenze corte di DNA, mentre i cloni sono sequenze più lunghe (fino a qualche decina di migliaia di basi). Per ogni marcatore p_j e clone C_i , un esperimento detto *ibridizzazione* determina se il marcatore p_j proviene dal (si trova sul) clone C_i o meno. L'insieme dei risultati di tutti i possibili esperimenti di ibridizzazione può essere rappresentato da una matrice A di dimensioni $m \times n$, con $a_{ij} = 1$ se il marcatore p_j proviene dal clone C_i , e $a_{ij} = 0$ altrimenti. Supponiamo che le colonne di A siano ordinate secondo l'ordine reale con cui i marcatori si trovano sul cromosoma. Un clone che contiene due marcatori a e b , deve contenere anche tutti i marcatori che si trovano compresi tra a e b . Questo significa che, se le colonne sono ordinate correttamente, in ogni riga di A tutti gli elementi compresi tra due elementi che valgono 1, devono valere anch'essi 1. Quindi, gli 1 in ogni riga appaiono in un unico blocco, eventualmente preceduto e/o seguito da un blocco di zeri. Si dice che una matrice le cui colonne possono essere ordinate in modo da posizionare gli 1 in blocchi soddisfa la *proprietà degli 1 consecutivi* (o, in breve, che è C1P). Non tutte le matrici binarie sono C1P.

Siccome l'ordine dei marcatori non è noto, una disposizione casuale delle colonne non evidenzia la natura C1P della matrice, e in ogni riga gli 1 e gli 0 si possono alternare in modo casuale. Obiettivo dell'esperimento è la costruzione di una *mappa fisica*, ossia la determinazione dell'ordine corretto dei marcatori. La correttezza dell'ordine è data dal fatto che, permutando le colonne in maniera corrispondente, si evidenziano i blocchi di 1 in ogni riga. Si consideri ora la seguente distanza (*distanza di Hamming*) definita fra coppie di colonne di A :

$$d_H(r, s) = |\{i : a_{ir} \neq a_{is}\}|.$$

(si noti che la distanza di Hamming fra due vettori binari può essere interpretata come il numero di bit che devo cambiare nel primo per ottenere il secondo). Si definisca ora un grafo pesato completo $G = (V, E, c)$ in cui i nodi V corrispondono ai marcatori e il costo del lato tra due nodi è uguale alla loro distanza di Hamming. Ogni circuito hamiltoniano in G avrà costo almeno $2m$. Infatti (assumendo che eventuali righe fatte di soli 0 o di soli 1 siano state rimosse, in quanto comunque non servirebbero in alcun modo a distinguere i marcatori fra loro), in ogni riga ci sarà sempre almeno una transizione da uno 0 ad un 1 e viceversa, e quindi la riga contribuirà almeno con 2 unità al costo complessivo. Si noti inoltre che, se la matrice è C1P, la soluzione ottima del TSP ha valore esattamente $2m$. Per cui, si può usare il TSP per trovare l'ordine dei marcatori che rende la matrice C1P (in realtà esiste un metodo più efficiente del TSP –ma molto complicato– per decidere se una matrice è C1P. Tuttavia, in presenza di errori come *falsi positivi* (1 che dovrebbero essere 0) e *falsi negativi* (0 che dovrebbero essere 1), la matrice può risultare non C1P anche se sappiamo che dovrebbe invece essere C1P. In questi casi, la soluzione del TSP cerca di minimizzare il numero di volte che un blocco di 1 contiene degli 0 al suo interno.). \diamond

ESERCIZIO 8.5. Siano $G = (V, E, c)$ un grafo completo pesato con un numero pari di nodi, H un minimo circuito hamiltoniano in G e $c(H)$ il suo costo. Detto M un matching perfetto in G di costo minimo, dimostrare che $c(M) \leq c(H)/2$. \diamond

Chapter 9

Tracce di soluzioni


9.1 Capitolo 1

SOL. 3: $n! \times (m+1)!$ 


SOL. 4: $(4!)^2$ 

SOL. 5: $\frac{14!15!25}{5!} \simeq 2.4 \times 10^{22}$ 

SOL. 9: Tre sono vere, tre false e una è indecidibile in base alle premesse. 

SOL. 10: Deve essere $b \geq a+1$ oppure $b^2 - a^2 \leq 0$. Ma allora $b^2 - a^2 \geq (a+1)^2 - a^2 = 2a+1 > a$. 

SOL. 14: Sì (l'insieme vuoto) 

SOL. 15: 6^n per $n \geq 2$; $9n+1$ mai; $(3n+1)(3n+5)+3$ mai; $3m+6n$ quando m e n danno lo stesso resto nella divisione per 3; alla roulette: per ogni n (il 36). 

SOL. 16: $3 \subset 2 \subset 1 \subset 4$. 

SOL. 18:

1. $X = \{1, 6\}$
2. nessuno

3. $X = \{1\}, X = \emptyset$
4. $X \in \mathcal{P}(\{2, 4, 5, 6\})$
5. $X \in \{\{2, 4, 5, 6\}, \{1, 2, 4, 5, 6\}, \{2, 3, 4, 5, 6\}, \{1, 2, 3, 4, 5, 6\}\}$



SOL. 21:

- $14 \leq |A \cup B| = |A \cup \bar{B}| \leq 20$
- $4 \leq |A \cap B| = |A \cap \bar{B}| \leq 10$
- $10 \leq |\bar{A} \cup B| = |\bar{A} \cup \bar{B}| \leq 16$
- $0 \leq |\bar{A} \cap B| = |\bar{A} \cap \bar{B}| \leq 6.$



SOL. 22:

1. R, S, T
2. $\neg R, S, \neg T$
3. $R, S, \neg T$
4. $\neg R, \neg S, \neg T$
5. R, S, T
6. $\neg R, \neg S, T$
7. R, S, T
8. $\neg R, S, \neg T$



SOL. 28: La funzione $f(x) = \lfloor \frac{x}{2} \rfloor$ è suriettiva in quanto $y = f(2y)$ per ogni $y \in \mathbb{Z}$, ma non è iniettiva, essendo, ad esempio, $f(4) = f(5) = 2$.



SOL. 29:

1. $gf = fg = 12x + 11$
2. $gf = fg = x$
3. $gf = 1/(x^4 + 2x^2 + 2); fg = (x^4 + 2x^2 + 2)/(x^4 + 2x^2 + 1)$
4. $gf = -3x - 1; fg = 7 - 3x$



SOL. 30: Ad esempio, siano $f : \mathbb{Z} \mapsto \mathbb{Z}$ con $f(x) = \max\{0, x\}$ e $g : \mathbb{Z} \mapsto \mathbb{Z}$ con $g(x) = \min\{0, x\}$. Allora $gf(x) = \min\{0, \max\{0, x\}\} = 0$ per ogni $x \in \mathbb{Z}$.



SOL. 31: $gf(x) = acx + bc + d$ è costante $\iff ac = 0 \iff (a = 0) \vee (c = 0) \iff (f(x) = c) \vee (g(x) = d)$ per ogni x .



SOL. 33: (i) 27; (ii) 3; (iii) e (iv) 6.



SOL. 38: Sia vero per $n-1$. Allora $(1+a)^n = (1+a)(1+a)^{n-1} \geq (1+a)(1+an-a) = 1+an+a^2(n-1) \geq 1+an$.



SOL. 39: Sia vero per $n-1$. Allora $15^n + 6 = 15(15^{n-1} + 6) - 14 \times 6$ è multiplo di 7.



SOL. 43: $\frac{n(n+1)(n+2)}{3}$



SOL. 44: Un quadrato può avere lato di lunghezza $1, 2, \dots, n$. Vediamo dove può avere il vertice alto a destra. Numeriamo, dal basso all'alto, le $n+1$ righe da 0 a n e anche le colonne. I quadrati di lato 1 hanno vertice alto a dx in tutte le righe e colonne tranne la colonna 0 e la riga 0. Perciò $n \times n$ modi. I quadrati di lato 2 hanno vertice alto a dx in tutte le righe tranne la 0 e la 1, e tutte le colonne tranne la 0 e la 1. Perciò $(n-1) \times (n-1)$ modi. Proseguendo si ha che il numero totale di quadrati è $\sum_{j=1}^n j^2$.



SOL. 48: Sia (π_1, \dots, π_{40}) la permutazione corrispondente alle carte mescolate. La carta che determina la briscola si trova in una posizione r , mentre l'ultima carta pescata è π_{40} . Perchè tale carta sia l'asso di briscola, la briscola scoperta (π_r) deve essere una carta diversa da un asso (36 possibilità). Una volta scelta questa carta, π_{40} (l'asso del seme giusto) è univocamente determinato. Infine, le altre 38 carte possono essere ordinate in uno qualsiasi dei $38!$ modi possibili. Esistono quindi $36 \times 38!$ permutazioni che danno luogo all'evento desiderato. Siccome il numero complessivo di permutazioni delle carte è $40!$, la probabilità cercata è $\frac{36 \cdot 38!}{40!} = \frac{3}{130}$.



SOL. 49: $\frac{3^3}{6^3} = \frac{1}{8}$



SOL. 51: $\Pr = 2/3$.



SOL. 52: Chiamiamo A = “ho preso la scatola mista” e B = “tutte le caramelle provate (siano esse k) erano al limone”. Ci interessa $\Pr(A|B)$. Abbiamo $\Pr(A|B) = \frac{\Pr(A \cap B)}{\Pr(B)} = \frac{\Pr(A)\Pr(B|A)}{\Pr(B)}$. Si ha $\Pr(A) = 1/2$, $\Pr(B|A) = 1/2^k$, $\Pr(B) = \frac{1}{2} \times 1 + \frac{1}{2} \times \frac{1}{2^k} = (2^k + 1)/(2^{k+1})$, da cui $\Pr(A|B) = 1/(2^k + 1)$. (i) Qui $k = 1$

quindi $\Pr(A|B) = 1/3$. (ii) Essendo $\Pr(A|B) = 1/(2^k + 1)$, la probabilità che la scatola che abbiamo scelto non sia quella mista è $(2^k)/(2^k + 1)$. Vogliamo il minimo k per cui tale valore risulta $\geq .9$. Per $k = 2$ la probabilità di successo nell'indicare l'altra come scatola mista è l'80%. Per $k = 3$ essa è circa l'88%. Per $k = 4$ è $> 90\%$. ♣

SOL. 53: In questo caso, si ha $W(2, 1, 1) = 1/2L(1, 1, 1) + 1/4(1 - W(2, 1, 1))$, da cui, $W(2, 1, 1) = 2/5L(1, 1, 1) + 1/5$. D'altro canto, $L(1, 1, 1) < 1 - 5/18 = 13/18$. Infatti, da $(1, 1, 1)$ si può vincere pescando la bianca seguita dalla rossa (prob. $1/6$) o la verde seguita dalla rossa (prob. $1/9$) e quindi in $5/18$ modi, come minimo, si vince. Sostituendo, si ha $W(2, 1, 1) < 2/5 \times 13/18 + 1/5 = 22/45 < 1/2$. ♣

SOL. 54: Si ha $W(1, 1, 1) = 1/3L(0, 2, 1) + 1/3(1 - W(1, 1, 1))$, da cui, $W(1, 1, 1) = 1/4L(0, 2, 1) + 1/4$. Inoltre, $L(0, 2, 1) = 2/3 + 1/3(1 - L(0, 2, 1))$, da cui $L(0, 2, 1) = 3/4$. Sostituendo, si ha $W(1, 1, 1) = 7/16$. ♣

9.2 Capitolo 2

SOL. 1: Sia $b = pa$ e $c = ma$. Allora $b + c = (p + m)a$ e $b - c = (p - m)a$. ♣

SOL. 2: Sia $a = xc$ e $b = yc$ e sia $b = qa + r$. $r = b - qa = (y - qx)c$. ♣

SOL. 3: (i) $a^2 - 1 = (a + 1)(a - 1)$; $a^n - 1 = (\sum_{i=0}^{n-1} a^i)(a - 1)$. ♣

SOL. 4: Sia $a = qn + r$, i.e., $r = a - qn$.

(\Rightarrow) Siccome $n | ab$, esiste t con $ab = tn$. Quindi $(qn + r)b = tn$, da cui $rb = (t - qb)n$ e quindi $n | rb$.

(\Leftarrow) Sia $n | rb$, i.e., $n | (a - qn)b$. Sicuramente $n | qnb$ e quindi $n | ab - qnb + qnb$, i.e., $n | ab$. ♣

SOL. 5: Sia x il numero di caramelle che ciascun bambino riceve, sicchè $(n + 11)x = n^2 + 9n - 2 = (n + 11)(n - 2) + 20$. Otteniamo $(n + 11)(x + 2 - n) = 20$ e dovendo essere i divisori di 20 interi, si ha $n + 11 = 20$ e $x + 2 - n = 1$. Quindi $n = 9$ e $x = 8$. ♣

SOL. 6: Si usi la formula per MCD e mcm tramite fattorizzazione in primi. ♣

SOL. 7: Sia, per assurdo, $a > 1$ tale che di $a|(2^n - 1)$ e anche $a|(2^{n-1} + 1)$. Allora $a|(2^n - 1) - (2^{n-1} + 1) = 2(2^{n-2} - 1)$ e, siccome $a \nmid 2$, deve essere $a|(2^{n-2} - 1)$. Allora deve anche essere $a|(2^{n-1} + 1) - (2^{n-2} - 1) = 2(2^{n-3} + 1)$, da cui deduciamo che $a|(2^{n-3} + 1)$. Proseguendo in questo modo, abbiamo che $a|(2^d - 1)$ per ogni naturale dispari $d \leq n$ e anche $a|(2^p + 1)$ per ogni pari $p \leq n$. Questo porta a concludere che $a|1$ (per $d = 1$) e quindi non può essere $a > 1$. ♣

SOL. 8: Il fattore primo 5 compare $11 + 2 = 13$ volte. Il fattore 2 compare almeno 13 volte (esattamente, $28 + 14 + 7 + 3 + 1 = 53$ volte). Quindi, $56!$ termina con 13 zeri. ♣

SOL. 9: Abbiamo (modulo 4321), $2^{4320} = (2^{20})^{216} = 2894^{216} = (2894^4)^{54} = 3065^{54} = (((3065^6)^3)^3) = (3554^3)^3 = 2762^3 = 3910 \neq 1$. ♣

SOL. 10: Per ogni $n \geq 4$ pari si ha $(n-1)^{n-1} \equiv (-1)^{n-1} \equiv -1 \pmod{n}$ e quindi n non può essere di Carmichael. ♣

SOL. 11: Per $n = 416$ vince sempre B . Infatti, ad ogni turno, se A rimuove x sassolini, B ne rimuove $5 - x$. In questo modo il numero di sassolini cala sempre di 5 e dopo $415/5$ mosse rimane un sasso solo (l'invariante è: ogni volta che tocca ad A , il numero di sassi è pari a 1 modulo 5). Per $n = 1013$, A può vincere rimuovendo 2 sassi alla prima mossa. Infatti, in questo modo costringe B a dover muovere su un mucchio di 1011 sassi (equivalente a 1 modulo 5), e quindi B perde perchè A può ora seguire la strategia esposta nel caso precedente. ♣

9.3 Capitolo 3

SOL. 2: Ogni numero si può fattorizzare come $2^k \times d$, con d dispari, $d \in \{1, 3, \dots, 197, 199\}$. Siano p_1, \dots, p_{100} i numeri scelti, e siano k_1, \dots, k_{100} e d_1, \dots, d_{100} tali che $p_i = 2^{k_i} d_i$ per ogni i . Se $d_i = d_j$ per qualche $i \neq j$ il risultato segue. Si supponga allora $d_i \neq d_j$ per ogni $i \neq j$. Allora d_1, \dots, d_{100} sono proprio i 100 dispari $1, 3, \dots, 199$. In particolare siccome almeno un numero tra 1 e 15 è stato scelto, avremo che:

1. o $2^{k_1} \times 1$ è stato scelto (per $k_1 \leq 3$. Copre i casi 1, 2, 4, 8)
2. o $2^{k_2} \times 3$ è stato scelto (per $k_2 \leq 2$. Copre i casi 3, 6, 12)
3. o $2^{k_3} \times 5$ è stato scelto (per $k_3 \leq 1$. Copre i casi 5, 10)
4. o $2^{k_4} \times 7$ è stato scelto (per $k_4 \leq 1$. Copre i casi 7, 14)
5. o è stato scelto uno tra $2^0 \times 9$, $2^0 \times 11$, $2^0 \times 13$, $2^0 \times 15$

Usiamo ora un ragionamento generale. Se si è scelto un numero di tipo $a = 2^p \times d$ e un altro di tipo $b = 2^q \times D$, con d che divide D , ma a non divide b , allora $p > q$.

Usiamo quest'idea per i casi di cui sopra. Avendo scelto $a = 2^p \times d$, consideriamo $p+1$ numeri dispari D_1, \dots, D_{p+1} tali che d divide D_1 , D_1 divide D_2 , D_2 divide D_3 , e così via. In particolare, siccome per ogni possibile dispari D si è scelto un numero della forma $2^h D$, sono stati scelti dei numeri del tipo $2^{k_1} D_1$, $2^{k_2} D_2$, ..., $2^{k_{p+1}} D_{p+1}$. Supponiamo che uno qualsiasi degli esponenti k_1, \dots, k_{p+1} , diciamo k_r , sia $\geq p$. Allora a divide il numero $2^{k_r} D_r$. In caso contrario, ognuno dei $p+1$ esponenti è compreso tra 0 e p . Per cui ci sono almeno due esponenti uguali (diciamo k_i e k_j , con $i < j$). Sia h tale che $h = k_i = k_j$. Ma allora $2^h D_i$ divide $2^h D_j$.

Quindi, per dimostrare il risultato, ci basta trovare almeno quattro dispari multipli di 1 (sottointeso, qui e dopo, < 200), almeno tre dispari multipli di 3, almeno due dispari multipli di 5 e due multipli di 7, almeno

un dispari multiplo di 9, uno di 11, uno di 13 e uno di 15. Ad esempio basta prendere:

- 3, 15, 45, 135 come multipli di 1
- 9, 27, 51 come multipli di 3
- 15, 45 come multipli di 5
- 21, 63 come multipli di 7
- $3x$ come multiplo di x con $x = 9, 11, 13, 15$



SOL. 5: Minimo 2, massimo 6.



SOL. 6: Si considerano i numeri modulo 10. In ogni resto posso avere al più un numero. In particolare al più uno vale 0 e al più uno vale 5. Inoltre, per ogni $i = 1, \dots, 4$, al più uno può essere i o $10 - i$. Quindi al più 6 numeri si possono avere, ma il settimo implica la concusione.



SOL. 7: La somma su tutte le triple è $3 \times \sum_{i=1}^{10} i = 165$, da cui, la media è 16.5. Quindi almeno una tripla vale ≥ 16.5 , e quindi ≥ 17 .



SOL. 8: Ognuno può avere un numero di amici nell'insieme $\{0, 2, \dots, 98\}$ (non è possibile 100 perchè sono 100 in tutto, per cui ≤ 99). Ora, o 3 persone hanno 0 amici, per cui la soluz segue. Oppure, restano almeno 98 numeri compresi tra $\{2, \dots, 98\}$, ossia in 48 slots. La media è $98/48 = 2.04\dots$ per slot, quindi in almeno uno slot vanno 3 valori, ossia 3 persone hanno lo stesso numero di amici.



SOL. 10: Una soluzione di valore 2^{n-1} si ottiene considerando i sottoinsiemi di $\{1, 2, \dots, n-1\}$ e aggiungendo a ciascuno l'elemento n . Di più non è possibile, perchè, per ogni insieme preso, il suo complementare non può essere preso.



9.4 Capitolo 4

SOL. 4: Per induzione. I casi $n = 2$ e 3 valgono. Sia ora $n > 2$ pari (similmente se dispari). Si ha $F_{n-1}F_{n+1} = F_{n-1}^2 + F_{n-1}F_n = F_{n-2}F_n + 1 + F_{n-1}F_n = F_n^2 + 1$.



SOL. 6: Per ogni caramella si tratta di decidere a chi va data. Ci sono 12 possibilità. Per cui, il totale è 12^{20} .



SOL. 7: Ogni bambino può ricevere un insieme T di tipi di caramelle, dove T è un sottoinsieme di tutti i tipi possibili. T può essere preso in 2^{20} modi. Per ciascun bambino ci sono 2^{20} possibilità per un totale di $2^{20} \times \dots \times 2^{20} = (2^{20})^{12}$.



SOL. 8: Numeriamo le cinque maglie rosse e quelle bianche, e aggiungiamo una maglia verde per il portiere. Assegnando le 11 maglie ai bambini in tutti i modi possibili, si hanno tutti i possibili modi di formare le squadre. In conclusione, ci sono $11!$ possibilità. Se, d'altro canto, volessimo considerare come identiche due soluzioni in cui le squadre sono composte dagli stessi giocatori, nei medesimi ruoli, ma cambia solo il colore della maglietta (ossia, immaginiamo che i cinque giocatori con maglietta rossa si scambino le maglie, ruolo per ruolo con quelli dalla maglietta bianca), allora il numero di soluzioni diventa $11!/2$. ♣

SOL. 11: 4^{23} . ♣

SOL. 14: (i) $2 \times \binom{6}{4} \times \binom{5}{4} \times \binom{5}{2} = 1500$.

(ii) $\binom{40}{3} \times \binom{120}{7} \times \binom{100}{6}^2 = 835,168,024,527,161,631,428,618,496,000,000$. ♣

SOL. 15: Numeriamo i colori da 1 a 5, per cui il tentativo era $(1, 2, 3, 4, 5)$. I colori giusti al posto giusto possono essere presi in $\binom{5}{2}$ modi. Supponiamo siano i primi due, per cui la soluzione è $(1, 2, x, y, z)$. Il colore giusto ma al posto sbagliato può essere preso in tre modi, e al suo posto ci dovrebbe essere un colore tra due possibili (ossia diverso da lui e dagli altri due sbagliati). Supponiamo sia il 3, per cui la soluzione è $(1, 2, x, y, z)$ con $x \in \{1, 2\}$ e $(y = 3) \vee (z = 3)$ (in quanto tale colore dovrebbe apparire al posto di uno degli sbagliati (due scelte)). Supponiamo $y = 3$. Infine l'ultimo posto del colore sbagliato andrebbe cambiato con un colore diverso da lui e dall'altro sbagliato. Nel nostro caso la soluzione sarebbe $(1, 2, x, 3, z)$ con $z \neq 4, 5$. In questo modo però si conta due volte la soluzione $(1, 2, x, 3, 3)$ per cui il numero totale di soluzioni compatibili è

$$\binom{5}{2} \times 3 \times 2 \times (2 \times 3 - 1) = 300$$

♣

SOL. 17: $\binom{8}{5} \times 5! \times \binom{8}{4} \times 4! \times \binom{7}{5} \times 5! = 28,449,792,000$. ♣

SOL. 23: $\binom{17}{9} = 24310$. ♣

SOL. 24: Ci sono $\binom{20+10-1}{9}$ mazzi possibili. ♣

SOL. 25: Introduciamo variabili non-negative $y_1 = x_1 - 2$, $y_3 = x_3 + 5$, $y_4 = x_4 - 8$. Si ottiene $2 + y_1 + x_2 - 5 + y_3 + 8 + y_4 = 30$, ossia $y_1 + x_2 + y_3 + y_4 = 25$ che si risolve al solito modo. ♣

SOL. 27:

1. $\binom{20}{6}$

2. Detta x_i la distanza fra il bastoncino $i - 1$ e l' i -mo preso (per $i = 1, \dots, 7$), si ha $x_1 + x_2 + \dots + x_7 = 14$ e $x_2, x_3, \dots, x_6 \geq 1$. Allo stesso modo dell'esercizio 25, si prova che i modi sono $\binom{15}{6}$.

3. Con la medesima notazione di sopra, si ha $x_2, \dots, x_6 \geq 2$. Le soluzioni sono $\binom{10}{6}$.



9.5 Capitolo 5

SOL. 1: Sia S l'insieme di tutte le permutazioni. Siccome si tratta di permutazioni del multi-insieme $\{3 \cdot V, 2 \cdot I, 3 \cdot A, 1 \cdot L, 1 \cdot T\}$ si ha $|S| = \frac{10!}{3!2!3!} = 50400$. Consideriamo A_1 come l'insieme di permutazioni in cui si legge “VIVA”. Questo corrisponde alle permutazioni del multi-insieme $\{1 \cdot VIVA, 1 \cdot V, 1 \cdot I, 2 \cdot A, 1 \cdot L, 1 \cdot T\}$ e quindi

$$|A_1| = \frac{7!}{2!} = 2520.$$

Si noti che è importante il fatto che il multiinsieme $\{1 \cdot V, 1 \cdot I, 2 \cdot A, 1 \cdot L, 1 \cdot T\}$ non permette di comporre la parola “VIVA”, o altrimenti ci sarebbero state delle permutazioni in A_1 contate due o più volte. Sia A_2 l'insieme di permutazioni che contengono “LA”. Si tratta delle permutazioni di $\{1 \cdot LA, 3 \cdot V, 2 \cdot I, 2 \cdot A, 1 \cdot T\}$ e quindi

$$|A_2| = \frac{9!}{3!2!2!} = 15120.$$

Infine, sia A_3 l'insieme di permutazioni in cui si legge “VITA”. Questo corrisponde alle permutazioni del multi-insieme $\{1 \cdot VITA, 2 \cdot V, 1 \cdot I, 2 \cdot A, 1 \cdot L\}$ e quindi

$$|A_3| = \frac{7!}{2!2!} = 1260.$$

L'insieme $A_1 \cap A_2$ ha le permutazioni in cui si legge sia “VIVA” che “LA”. Questo insieme corrisponde alle permutazioni del multi-insieme $\{1 \cdot VIVA, 1 \cdot LA, 1 \cdot V, 1 \cdot I, 1 \cdot T, 1 \cdot A\}$ e quindi

$$|A_1 \cap A_2| = 6! = 720.$$

L'insieme $A_1 \cap A_3$ ha le permutazioni in cui si legge sia “VIVA” che “VITA”. Questo insieme corrisponde alle permutazioni del multi-insieme $\{1 \cdot VIVA, 1 \cdot VITA, 1 \cdot L, 1 \cdot A\}$ e quindi

$$|A_1 \cap A_3| = 4! = 24.$$

L'insieme $A_2 \cap A_3$ ha le permutazioni in cui si legge sia “LA” che “VITA”. Questo insieme corrisponde alle permutazioni del multi-insieme $\{1 \cdot LA, 1 \cdot VITA, 2 \cdot V, 1 \cdot I, 1 \cdot A\}$ e quindi

$$|A_2 \cap A_3| = \frac{6!}{2!} = 360.$$

Infine, in $A_1 \cap A_2 \cap A_3$ abbiamo le permutazioni che contengono sia “VIVA” che “LA” che “VITA”. Queste corrispondono alle permutazioni del multi-insieme $\{1 \cdot VIVA, 1 \cdot LA, 1 \cdot VITA\}$, per cui

$$|A_1 \cap A_2 \cap A_3| = 3! = 6.$$

Dal principio di inclusione-esclusione abbiamo

$$|\bar{A}_1 \cap \bar{A}_2 \cap \bar{A}_3| = 50400 - (2520 + 151202 + 1260) + (720 + 24 + 360) - 6$$

e quindi $|\bar{A}_1 \cap \bar{A}_2 \cap \bar{A}_3| = 32598$.



SOL. 2: 46



SOL. 3: Sono 4350.



SOL. 9: Sono 8400.



9.6 Capitolo 7

SOL. 2: In un tale grafo si avrebbe $\sum_v d(v) = 2000$ ma anche $\sum_v d(v) = 3k$ per qualche $k \in \mathbb{Z}$. Siccome 2000 non è multiplo di 3, un tale grafo è impossibile.



SOL. 3: Consideriamo il caso generale. Dati n vertici, il grafo completo ha $n(n-1)/2$ lati. Ogni altro grafo è identificato da un sottoinsieme dei lati del grafo completo. Ci sono pertanto

$$2^{n(n-1)/2}$$

grafi possibili su n nodi specificati. Nel caso di questo esercizio, la risposta è 2^{190} .



SOL. 4: Un tale grafo ha $n = 8$ nodi. Se non fosse connesso, potrebbe essere decomposto in due sottografi, senza archi da un sottografo all'altro, di n_1 e n_2 nodi. Si noti che $n_1, n_2 \geq 4$ per via dei gradi. Quindi, $n_1 = n_2 = 4$. Ma un nodo v di grado 4 avrebbe almeno un vicino nell'altro sottografo rispetto a quello in cui è v .



SOL. 7: Se un grafo non è connesso esiste una partizione dei nodi che lascia x nodi, $1 \leq x \leq n-1$ da una parte e $n-x$ dall'altra, senza lati tra i due gruppi di nodi. Il numero massimo di archi in una tale partizione è:

$$f(x) = \frac{x(x-1)}{2} + \frac{(n-x)(n-x-1)}{2}$$

cioè $f(x) = x^2 - nx + n(n-1)$. Il massimo di questa funzione nell'intervallo $[1, \dots, n-1]$ è ottenuto per $x = 1$ e per $x = n-1$, e vale $(n-1)(n-2)/2$. Non appena si aggiunge un ulteriore lato, il grafo non può più essere non connesso.



SOL. 10: In entrambi i casi è impossibile. Si tratta di un circuito hamiltoniano su un grafo bipartito. Nel primo caso non esiste perchè il grafo ha un numero dispari di nodi. Nel secondo caso, si disegni il grafo, e

si osservi che le caselle d'angolo hanno grado 2, e quindi c'è un solo modo di visitarle. Ma gli archi forzati inducono dei sottocicli. ♣

SOL. 11: 7 volte. ♣

SOL. 12: (\Rightarrow) Sia G connesso. Presi x e y in G' , se $x, y \in V$ allora erano già collegati in G . Altrimenti, senza perdita di generalità, sia $x = c$. Allora esiste un cammino a, \dots, y e quindi il cammino x, a, \dots, y collega x a y in G' .

(\Leftarrow) Sia G' connesso e siano x, y in G . Siccome G' è euleriano, esiste un circuito x, \dots, y, \dots, x . Questo circuito va da x a y e poi da y a x . Siccome c può essere solo nel tratto “di andata” o solo in quello “di ritorno”, uno dei due tratti è completamente incluso in G , che quindi è connesso. ♣

SOL. 13: Siano $D = \{1, 3, 5, \dots, 19\}$ e $P = \{2, 4, 6, \dots, 20\}$ rispettivamente i numeri dispari e pari in V .

1. Risulta $ab \in E$ se $a \in D, b \in D$ o $a \in P, b \in P$. Quindi D e P inducono due clique, disgiunte, di 10 nodi ciascuna. Quindi G non è connesso, non è bipartito, le sue componenti non sono euleriane (ogni nodo ha grado 9) ma sono hamiltoniane.
2. Risulta $ab \in E$ se $a \in D, b \in P$. Quindi G è bipartito completo, con bipartizione data da D e P . G è connesso, ed euleriano (ogni nodo ha grado 10). Infine G è hamiltoniano. Ad esempio, il ciclo $2, 1, 4, 3, 6, 5, \dots, 20, 19, 2$ è un circuito hamiltoniano.
3. Risulta $ab \in E$ se almeno uno fra a e b è in P . G risulta uguale al grafo in 2. più una clique sui nodi in P . Come prima, G è connesso e hamiltoniano. G però non è più bipartito, nè ha componenti tutte euleriane (ogni nodo in P ha grado 19).
4. Risulta $ab \in E$ se $a, b \in D$. Ogni nodo in P è isolato e quindi G non è connesso. D è una clique di 10 nodi e quindi G non è bipartito. Inoltre G ha componenti non euleriane (ogni nodo in D ha grado 9). Le componenti di G sono hamiltoniane.
5. In G esistono nodi isolati. Ad esempio, tutti i nodi primi ≥ 7 . Infatti se p è un numero primo e $pq = r = x^2$, nella decomposizione di r in primi deve comparire il fattore p^2 . In particolare, p deve dividere x . Inoltre la divisione di r per p^2 deve essere a sua volta un quadrato, > 1 . Ora, il più piccolo quadrato è 4, e $4 \times 7 = 28 \notin V$.

Quindi, siccome ci sono nodi isolati, G non è nè connesso. G non è bipartito. Infatti, per ogni coppia di numeri x, y tali che sia x che y sono dei quadrati, esiste il lato xy . Questo implica che i nodi 1, 4, 9, 16 inducono una clique, e quindi G non è bipartito. In G esistono nodi di grado 1, per cui G ha componenti non euleriane. Ad esempio, il nodo 5, per il ragionamento di cui sopra, può avere un lato solo verso un nodo che sia multiplo di 5 e di 4, e in G c'è un solo tale nodo, il nodo 20. Infine, tutte le componenti connesse di G con almeno 3 nodi sono hamiltoniane, in quanto ciascuna di esse è una clique. Infatti, siano x, y, z tre nodi tali che $xy, xz \in E$. Consideriamo la fattorizzazione di x, y e z sugli stessi fattori primi, i.e., sull'unione dei loro fattori (si noti che alcuni esponenti possono essere zero). Detto p un tale fattore primo, e detti a, b, c gli esponenti di p nelle fattorizzazioni di x, y e z si vede che a, b, c hanno la stessa parità, dovendo essere $a + b$ pari e $a + c$ pari. Ne segue che $b + c$, i.e., l'esponente di p nella fattorizzazione di $y \times z$, è sempre pari. Questo vale per tutti i fattori di $y \times z$ e quindi $y \times z$ è un quadrato, ossia $yz \in E$. Questo fatto implica che ogni componente connessa è una clique perchè non possono esserci cammini di lunghezza maggiore di 1.

Esistono però in G componenti connesse di un unico arco, che quindi non sono hamiltoniane. In particolare, l'arco $5, 20$ è una tale componente connessa.

6. Risulta $ab \in E$ se il resto di a e b per 3 è lo stesso (ossia se $a = b \pmod{3}$). V si divide nelle seguenti classi (la classe C_i dà resto i nella divisione per 3): $C_0 = \{3, 6, 9, 12, 15, 18\}$, $C_1 = \{1, 4, 10, 13, 16, 19\}$, $C_2 = \{2, 5, 8, 11, 14, 17, 20\}$. Ogni C_i induce una clique e quindi G non è bipartito. Non si hanno archi tra C_i e C_j , con $i \neq j$, e quindi G non è connesso. Siccome i nodi in C_0 e C_1 hanno grado dispari (5), G ha componenti non euleriane. Infine, ogni componente di G è hamiltoniana.

♣

SOL. 14: Detto x il numero di archi si ha $2x/(x+1) = 1.99$.

♣

SOL. 15: Detto x il numero di nodi di grado 1, si ha $(3 \times 10 + x)/2 = 10 + x - 1$.

♣

SOL. 17: Un tale albero ha esattamente 2 nodi interni. Detti a, b, c, d i nodi di un cammino massimo, a e d sono foglie, e tutti i rimanenti 100 archi sono incidenti in b o c . In b possono essere incidenti $0, 1, \dots, 50$ archi, per cui ci sono 51 tali alberi.

♣

SOL. 21: Usiamo l'induzione su n . Supponiamo vero il risultato per grafi di $1, 2, \dots, n-1$ nodi. Preso D_n , consideriamo D_{n-1} , ottenuto escludendo da D_n il nodo n e gli archi ad esso incidenti. Per induzione, esiste un cammino hamiltoniano in D_{n-1} , sia esso $(v_1, v_2, \dots, v_{n-1})$. Se per ogni $i = 1, \dots, n-1$ si ha $(v_i, n) \in D_n$, allora (v_1, \dots, v_{n-1}, n) è un cammino hamiltoniano in D_n . Altrimenti, sia $1 \leq j \leq n-1$ il minimo indice tale che $(v_i, n) \in D_n$ per $i = 1, \dots, j-1$, e $(n, v_j) \in D_n$. Allora $(v_1, \dots, v_{j-1}, n, v_j, v_{j+1}, \dots, v_{n-1})$ è un cammino hamiltoniano in D_n .

♣

9.7 Capitolo 8

SOL. 3: (i) Falso. (ii) Falso.

♣

SOL. 4: Diamo due soluzioni alternative, una ricorsiva (1) e l'altra diretta (2).

(1) Chiamiamo $S(n)$ il numero di matching perfetti nel grafo K_{2n} . Il caso base è $S(1) = 1$. In generale, dati $2n$ vertici, il vertice 1 può essere accoppiato a uno qualsiasi fra $2n-1$ vertici. Restano $2(n-1)$ vertici, che ammettono $S(n-1)$ possibili accoppiamenti perfetti. Quindi

$$S(n) = (2n-1)S(n-1) \quad (9.1)$$

Usando la formula (9.1), sostituendo $n-1$ al posto di n , si ricava $S(n-1) = (2(n-1)-1)S(n-2) = (2n-3)S(n-2)$. Allo stesso modo, $S(n-2) = (2n-5)S(n-3)$, e così via. Sostituendo i vari valori di $S(\cdot)$ nella formula (9.1), si ottiene:

$$S(n) = (2n-1) \times (2n-3) \times (2n-5) \times \dots \times 3 \times 1$$

Quindi, $S(n)$ è il prodotto di tutti i numeri dispari compresi tra 1 e $2n$.

(2) Supponiamo di disporre tutti i vertici in una permutazione (il che può essere fatto in $(2n)!$ modi), e di considerare come lati del matching le coppie di vertici, a due a due, incontrate nella permutazione. In questo modo, però più permutazioni possono dare luogo allo stesso matching, per cui bisogna evitare di ricontare matching identici. Ad esempio, le n coppie di elementi adiacenti in una permutazione possono essere permutate fra loro e darebbero luogo allo stesso matching. Questo può essere fatto in $n!$ modi. Inoltre, per ogni permutazione, i due elementi adiacenti all'interno di una qualsiasi coppia potrebbero essere scambiati fra loro, e la permutazione individuerrebbe ancora lo stesso matching. Questo scambio si può effettuare in 2^n modi. Si ottiene che il numero di matching perfetti è:

$$\frac{(2n)!}{2^n n!}$$

Si noti che questa formula chiusa, apparentemente più complessa da comprendere, in effetti restituisce il prodotto $S(n)$ degli n numeri dispari compresi tra 1 e $2n$. 