Appunti di Lezione: Strutture Discrete

Parte III: Calcolo Combinatorio e Probabilità Discrete

V. Cutello

Contenuti

STRUTTURE DISCRETE

PARTE 3: CALCOLO COMBINATORIO e PROBABILITA' DISCRETE

1: Calcolo Combinatorio

Introduzione

- Una delle cose più importanti che un informatico (o matematico) deve imparare a fare è ... **contare** o **calcolare**.
- In particolare, vogliamo essere in grado di contare il numero di oggetti o casi che ci interessano, senza doverli esplicitare uno per uno.
- Ricordiamo che il termine "Computer" viene dal verbo inglese "Compute" che vuol dire esattamente "calcolare".
- I problemi però, a volte, sono complicati.

Domande non semplici

Per esempio, proviamo a rispondere a queste domande:

- Se sto scrivendo un programma che simula il poker, il mio programma deve fare in modo che la probabilità di un poker d'assi servito sia quella giusta. Ma qual è tale probabilità?

- Quanti sono i codici PIN di una carta bancomat a 5 cifre e quante sono le probabilità che un ladro riesca ad indovinare entro 3 tentativi?
- Quante sono le possibili password fatte di 8 simboli alfa-numerici (maiuscole e minuscole sono diverse) e quanto tempo ci mette un programma che genera 1000 passwords al secondo a trovare quella giusta?
- Se dovessi scommettere che in un'aula con 20 persone, ce ne siano almeno 2 che fanno il compleanno lo stesso giorno, scommetterei di si oppure no? E se ce ne sono $30, 40, 50$ o più di persone?
- Quante squadre di calcio diverse posso formare da un gruppo di 50 studenti?

Regola della somma

Cominciamo con la prima, e semplice, regola. Se il nostro problema è contare quanti sono gli elementi dell'unione di due insiemi disgiunti, A e B, quindi gli elementi di $A \cup B$.
Per esempio vogliamo sapere quanti sono le lettere dell'alfabeto, minuscole e maiuscole. La risposta è semplice ovvero

$$|A| + |B|$$

essendo gli insiemi disgiunti. Quindi nel caso specifico $26 + 26 = 52$.
E quanti sono allora i caratteri alfa-numerici, ovvero lettere dell'alfabeto $A \cup B$ più cifre numeriche C?

$$|(A \cup B) \cup C| = |(A \cup B)| + |C| = 52 + 10 = 62.$$

Regola del prodotto

Se il nostro problema è contare quante sono le possibili coppie di elementi, il primo scelto da un insieme A ed il secondo scelto da un insieme B, la risposta anche in questo case è molto semplice, visto che, sostanzialmente, consiste nel problema di scegliere un elemento del prodotto cartesiano $A \times B$. Ovvero $|A \times B| = |A| \cdot |B|$.
Per esempio vogliamo sapere quanti sono le possibili coppie di caratteri alfanumerici. In questo caso $A = B$ e $|A| = 62$. Quindi tutte le possibili coppie di caratteri alfanumerici sono $62 \cdot 62 = 3844$.

Regola del prodotto

Più in generale, se abbiamo da fare k operazioni di scelta, tali che

- La prima operazione si può fare in n_1 modi;
- la seconda operazione si può fare in n_2 modi, costante e indipendente dalla scelta precedente;
- $\ldots$
- la i-esima operazione si può fare in n_i modi, costante e indipendente dalle scelte precedenti;
- $\ldots$
- la k-esima operazione si può fare in n_k modi, costante e indipendente dalle scelte precedenti;

Allora, l'intera operazione, ovvero il numero di scelte totali è

$$n_1 \cdot n_2 \cdot \ldots \cdot n_k$$

Regola del prodotto: esempi

Possiamo già rispondere, quantomeno parzialmente, a 2 delle domande poste inizialmente.

- Quanti sono i codici PIN di una carta bancomat a 5 cifre? Risposta:

$$10^5 = 100000.$$

- Quante sono le password fatte di 8 simboli alfa-numerici ? Se consideriamo equivalenti lettere maiuscole e minuscole, allora la risposta è

$$36^8 = 2.821.109.907.456$$

  quindi, poco meno di tremila miliardi di passwords. E un computer che genera 1000 passwords al secondo ci metterà circa $2,8$ miliardi di secondi per provarle tutte. In un giorno ci sono 86400 secondi, quindi, serviranno circa 32 mila giorni, ovvero 88 anni.

  Un computer ben più potente che riesce a generare e controllare circa 1 miliardo di passwords al secondo, ci metterà circa tremila secondi, cioè circa un'ora.

- Se invece consideriamo come diverse lettere maiuscole e minuscole, allora la risposta è

$$62^8 = 218.340.105.584.896$$

  che è circa 77 volte il valore ottenuto considerando solo 66 caratteri alfabetici. Quindi, nel caso ottimale descritto sopra, un computer che riesce a generare e controllare circa 1 miliardo di passwords al secondo, ci metterà circa 77 ore per controllarle tutte.

Disposizioni e combinazioni

Vogliamo rispondere alle seguenti 4 domande puramente matematiche

1. Dati due insiemi A e B, con $|A| = k, |B| = n$ calcolare il numero delle applicazioni di A in B.
    - *Numero delle disposizioni con ripetizione di n elementi di classe k:* denotato con $F_{n,k}$
2. Dati due insiemi A e B, con $|A| = k, |B| = n$ calcolare il numero delle applicazioni iniettive di A in B.
    - *Numero delle disposizioni semplici di n elementi di classe k:* denotato con $D_{n,k}$

Disposizioni e combinazioni

3 Dato un insieme B, con $|B| = n$, e preso un intero $k \leq n$, trovare il numero dei sottoinsiemi di B composti di k elementi.

- *Numero delle combinazioni di n elementi di classe k:* denotato con $C_{n,k}$

4 Dato un insieme di n variabili, $\{x_1, x_2, \ldots, x_n\}$ e preso un un intero $k \leq n$, trovare il numero di monomi, con coefficiente 1, di grado k definiti sulle n variabili date. Esempio: $x_1^2 x_3 x_4^3$ monomio di grado 6, $x_2^2 x_4 x_5$ monomio di grado 4.

- *Numero delle combinazioni di n elementi di classe k con ripetizione:* denotato con $C^r_{n,k}$

Disposizioni con ripetizione

Per calcolare $F_{n,k}$ utilizziamo la regola del prodotto: per ognuno dei k elementi di A dobbiamo scegliere uno dei n elementi di B. Ogni scelta è indipendente dalle scelte fatte precedentemente. Quindi

$$F_{n,k} = n^k.$$

Esempio Funzioni booleane

Quante sono le funzioni booleane definite su un insieme di k variabili booleane? Sono tutte funzioni del tipo:

$$f : A \to \{0, 1\}$$

dove $|A| = k$. Quindi,

$$F_{2,k} = 2^k$$

Disposizioni con ripetizione

- Spesso, oltre che con il simbolo $F_{n,k}$ il numero di disposizioni con ripetizione di n elementi di classe k si indica con il simbolo $D^r_{n,k}$
- k elementi di A come coordinate di una k-upla: ogni applicazione di A in B corrisponde biunivocamente ad una k-upla x di elementi di B cioè $x \in B^k = B \times B \times \cdots \times B$.
- Quindi il numero di applicazioni da A in B corrisponde al numero di k-uple di B^k che è appunto n^k.

Esempio $B = \{a, b\}$

- le disposizioni con ripetizione di classe 1 sono: $(a), (b)$;
- classe 2: $(a, a), (a, b), (b, a), (b, b)$;
- classe 3: $(a, a, a), (a, a, b), (a, b, a), (a, b, b), (b, a, a), (b, a, b), (b, b, a), (b, b, b)$;
- etc.

Disposizioni semplici

Come prima cosa, notiamo che affinché esista un'applicazione iniettiva da A, con $|A| = k$, in B, con $|B| = n$ deve essere $n \geq k$. Per calcolare $D_{n,k}$ utilizziamo la regola del prodotto. Dobbiamo fare k operazioni di scelta, tali che

- La prima operazione si può fare in n modi;
- la seconda operazione si può fare in $n - 1$ modi, numero costante
- $\ldots$
- la k-esima operazione si può fare in $n - k + 1$ modi, numero costante

Allora, l'intera operazione, ovvero il numero di scelte totali è

$$D_{n,k} = n \cdot (n-1) \cdot \ldots \cdot (n-k+1)$$

Disposizioni semplici

Come già visto per le disposizioni con ripetizione possiamo pensare alle applicazioni iniettive da A in B come k-uple di elementi distinti di B.

Esempio $B = \{a, b, c\}$

- le disposizioni di classe 1 sono: $(a), (b), (c)$;
- classe 2: $(a, b), (a, c), (b, a), (b, c), (c, a), (c, b)$;
- classe 3: $(a, b, c), (a, c, b), (b, a, c), (b, c, a), (c, a, b), (c, b, a)$;
- etc.

Disposizioni semplici: esempi

Possiamo rispondere alla domanda:

- Quante squadre di calcio diverse posso formare da un gruppo di 50 studenti?
- Risposta:
$$D_{50,11} = 50 \cdot 49 \cdot \ldots \cdot 40 \approx 1,5 \cdot 10^{18}$$
- Stiamo ovviamente assumendo che l'ordine diverso degli studenti dia origine ad una squadra diversa.

E se invece ci chiediamo quante squadre diverse posso formare da un gruppo di 11 studenti, guardando agli insiemi di 11 studenti, e quindi ignorando l'ordine?

Permutazioni o Sostituzioni

- Il numero di permutazioni semplici o sostituzioni è il numero di disposizioni semplici di classe n cioè $D_{n,n}$.
- Dalla formula precedente segue che

$$D_{n,n} = n \cdot (n-1) \cdot \ldots \cdot (n-n+1) = n!$$

- Quindi il numero delle Permutazioni o Sostituzioni è il numero delle applicazioni iniettive di un insieme in un altro di cardinalità uguale.
- Queste applicazioni sono ovviamente anche surgettive e quindi il numero delle permutazioni o sostituzioni è il numero delle biezioni di un insieme in un altro della stessa cardinalità.

Permutazioni o Sostituzioni

- Se si prende $B = A$, spesso si indicano le Permutazioni (o Sostituzioni) di classe n con il simbolo P_n (o S_n).
- Quindi sono il numero di biezioni di un insieme in sé stesso. Possiamo vedere una permutazione come un ri-ordinamento di n elementi.

Esempio $A = \{1, 2, 3\}$

$$P_3 = \{(1, 2, 3), (1, 3, 2), (2, 1, 3), (2, 3, 1), (3, 1, 2), (3, 2, 1)\};$$

e

$$|P_3| = 3! = 3 \cdot 2 \cdot 1 = 6$$

Combinazioni

- Consideriamo l'insieme di tutte le $D_{n,k}$ applicazioni iniettive di un insieme A di $k > 0$ elementi in un insieme B di n elementi ($k \leq n$).
- Data una qualunque applicazione iniettiva f, la sua immagine $f(A)$ è, come sappiamo, un sottoinsieme di B che contiene k elementi.
- Introduciamo la seguente relazione di equivalenza tra le applicazioni iniettive da A a B
$$f \approx g \Leftrightarrow f(A) = g(A)$$
- Quindi due applicazioni sono equivalenti se hanno la stessa immagine.
- Le possibili classi di equivalenza sono tante quanti i sottoinsiemi di B costituiti da k elementi, che denoteremo con $C_{n,k}$.
- In ogni classe di equivalenza ci sono tanti elementi quante sono le applicazioni biiettive di un insieme di k elementi in un insieme di k elementi, ovvero $k!$.
- Quindi
$$D_{n,k} = C_{n,k} \cdot k!$$
da cui ricaviamo che
$$C_{n,k} = \frac{n \cdot (n-1) \cdot \ldots \cdot (n-k+1)}{k!}$$

Combinazioni

- Chiariamo che $C_{n,0} = 1$ dal momento che esiste un solo insieme vuoto;
- I valori $C_{n,k}$ sono anche detti coefficienti binomiali ed indicati con il simbolo:

$$\binom{n}{k}$$

- Dato che

$$\begin{aligned}\binom{n}{k} &= \frac{n \cdot (n-1) \cdot \ldots \cdot (n-k+1)}{k!} = \\ &= \frac{n \cdot (n-1) \cdot \ldots \cdot (n-k+1)}{k!} \frac{(n-k)!}{(n-k)!} = \frac{n!}{k!(n-k)!}\end{aligned}$$

- ricaviamo l'uguaglianza

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

- Poiché è $0! = 1$ la relazione vale anche per $k = 0$ e $k = n$

Combinazioni: Esempi

Dato un insieme A con 6 elementi, i suoi sottoinsiemi di cardinalità ...

- 0 sono: $\binom{6}{0} = \frac{6!}{0!6!} = 1$ (solo l'insieme vuoto ovviamente)
- 1 sono: $\binom{6}{1} = \frac{6!}{1!5!} = 6$ (tutti e 6 gli insiemi contenenti un solo elemento)
- 2 sono: $\binom{6}{2} = \frac{6!}{2!4!} = 15$
- 3 sono: $\binom{6}{3} = \frac{6!}{3!3!} = 20$
- 4 sono: $\binom{6}{4} = \frac{6!}{4!2!} = 15$
- 5 sono: $\binom{6}{5} = \frac{6!}{5!1!} = 6$
- 6 sono: $\binom{6}{6} = \frac{6!}{6!0!} = 1$

Notiamo che

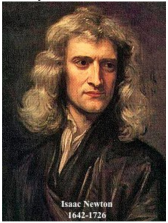
- $\binom{n}{k} = \binom{n}{n-k}$ visto che $\frac{n!}{k!(n-k)!} = \frac{n!}{(n-k)!k!}$
- La somma di tutte le quantità di insiemi è $1 + 6 + 15 + 20 + 15 + 6 + 1 = 64$ che è quanto già sapevamo dal momento che dato un insieme finito A $|pow(A)| = 2^{|A|}$, nel nostro caso $2^6 = 64$.

Combinazioni

- Dato un insieme A con n elementi, fissiamo adesso un elemento $x \in A$.
- I sottoinsiemi di k elementi, che sono $\binom{n}{k}$ si possono ripartire tra
  - i sottoinsiemi che contengono x che sono tanti quanti sono i sottoinsiemi di $k-1$ elementi di $A \setminus \{x\}$, ovvero $\binom{n-1}{k-1}$;
  - i sottoinsiemi che non contengono x che sono tanti quanti sono i sottoinsiemi di k elementi di $A \setminus \{x\}$ ovvero $\binom{n-1}{k}$;
- Quindi
$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

Teorema binomiale (formula di Newton)

Una delle scoperte più importanti di Newton, pubblicata alla fine del 1600, fu il teorema binomiale: una formula che consente di elevare a una qualsiasi potenza un binomio.
La dimostrazione è semplice ed è una conseguenza quasi immediata della definizione dei coefficienti binomiali e di semplici considerazioni algebriche.



Teorema

Siano a e b numeri reali. Allora vale l'uguaglianza:

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

Teorema binomiale (formula di Newton)

Dimostriamo il teorema di Newton

Dimostrazione

La potenza $(a+b)^n$ è il prodotto di n fattori tutti uguali a $(a+b)$.
Se sviluppiamo il prodotto

$$(a+b)\cdot(a+b)\cdot\ldots\cdot(a+b)$$

Otteniamo una somma di monomi tutti di grado n in a e b del tipo $a^{n-k}b^k$ con $0 \leq k \leq n$.
In particolare, i monomi $a^n b^0 = a^n$ e $a^0 b^n = b^n$ compariranno nella somma una sola volta, esattamente quando da ogni fattore prendiamo rispettivamente a o b.
Quante volte compare nella somma il monomio $a^{n-1}b$? Tante volte quanti sono i modi di scegliere $n-1$ degli n fattori, da cui scegliere a per sviluppare il prodotto. Ovvero $\binom{n}{n-1} = n-1$.
In generale, il monomio $a^{n-k}b^k$ compare tante volte quanti sono i modi di scegliere $n-k$ degli n fattori da cui scegliere a per sviluppare il prodotto. Ovvero $\binom{n}{k}$.
$\triangle$

Teorema binomiale

Esplicitiamo due particolari conseguenze del Teorema binomiale.

- La prima l'abbiamo già vista nell'esempio di tutti i sottoinsiemi di un insieme di cardinalità 6, ovvero, in generale

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

  Utilizzando il teorema binomiale abbiamo infatti per $a = b = 1$

$$2^n = (1+1)^n = \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} \cdot 1^k = \sum_{k=0}^{n} \binom{n}{k}$$

- Se poniamo $a = 1$ e $b = 10$ abbiamo invece

$$\sum_{k=0}^{n} \binom{n}{k} 1^{n-k} \cdot 10^k = \sum_{k=0}^{n} \binom{n}{k} 10^k = 11^n$$

Triangolo di Tartaglia o Pascal

- L'equazione $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$ permette di costruire una tabella (che si può mettere a forma di triangolo) dove ogni coefficiente binomiale è la somma dei due numeri immediatamente sopra.
- Tale tabella è universalmente conosciuta con con il nome di triangolo di Pascal o di Tartaglia, anche se precede storicamente i due matematici.

Nicolò Fontana detto Tartaglia
(1499-1557)

```
                                                        1       n=0
                                                    1       1       n=1
                                                1       2       1       n=2
                                            1       3       3       1       n=3
                                        1       4       6       4       1       n=4
                                    1       5       10      10      5       1       n=5
                                1       6       15      20      15      6       1       n=6
                            1       7       21      35      35      21      7       1       n=7
                        1       8       28      56      70      56      28      8       1       n=8
                    1       9       36      84      126     126     84      36      9       1       n=9
                1       10      45      120     210     252     210     120     45      10      1       n=10
            1       11      55      165     330     462     462     330     165     55      11      1       n=11
        1       12      66      220     495     792     924     792     495     220     66      12      1       n=12
    1       13      78      286     715     1287    1716    1716    1287    715     286     78      13      1       n=13
1       14      91      364     1001    2002    3003    3432    3003    2002    1001    364     91      14      1       n=14
k=0     k=1     k=2     k=3     k=4     k=5     k=6     k=7     k=8     k=9     k=10    k=11    k=12    k=13    k=14
```

Blaise Pascal
(1623-1662)

Triangolo di Tartaglia o Pascal

Da quanto abbiamo già visto possiamo già notare come il triangolo di Pascal abbia notevoli e sorprendenti proprietà

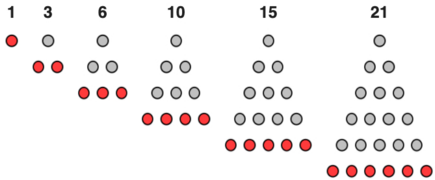
- Il triangolo è ovviamente simmetrico in quanto $\binom{n}{k} = \binom{n}{n-k}$
- La somma dei numeri in ogni riga, ossia per ogni $n \geq 0$, è uguale a 2^n.
- Se per ogni n e per ogni k consideriamo gli elementi della riga n come coefficienti della potenza k di 10 otteniamo per ogni n la potenza 11^n.
- Per esempio consideriamo le righe da $n = 0$ a $n = 5$.
  - $n = 0 : 1 = 2^0; 1 \cdot 10^0 = 1;$
  - $n = 1 : 1 + 1 = 2 = 2^1; 10^1 + \cdot 10^0 = 11 = 11^1;$
  - $n = 2 : 1 + 2 + 1 = 4 = 2^2; 10^2 + 2 \cdot 10^1 + 10^0 = 121 = 11^2;$
  - $n = 3 : 1 + 3 + 3 + 1 = 8 = 2^3; 10^3 + 3 \cdot 10^2 + 3 \cdot 10^1 + 10^0 = 1331 = 11^3;$
  - $n = 4 : 1 + 4 + 6 + 4 + 1 = 16 = 2^4;$
    $10^4 + 4 \cdot 10^3 + 6 \cdot 10^2 + 4 \cdot 10^1 + 10^0 = 14641 = 11^4;$
  - $n = 5 : 1 + 5 + 10 + 10 + 5 + 1 = 32 = 2^5;$
    $10^5 + 5 \cdot 10^4 + 10 \cdot 10^3 + 10 \cdot 10^2 + 5 \cdot 10 + 10^0 =$
    $100000 + 50000 + 10000 + 1000 + 50 + 1 = 161051 = 11^5.$

Triangolo di Tartaglia o Pascal

- Guardando alla colonna $k = 2$ troviamo i numeri triangolari, ovvero i numeri interi $t_1, t_2, t_3, \ldots$ che sono, per ogni i, la somma dei primi i numeri interi
- Quindi, i numeri $1, 3, 6, 10, 15, \ldots\ldots$ che verificano

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

- Tali numeri sono chiamati triangolari perché come si vede nella figura sotto, rappresentano quantità di "punti" che possono essere usate per formare triangoli:



Triangolo di Tartaglia o Pascal

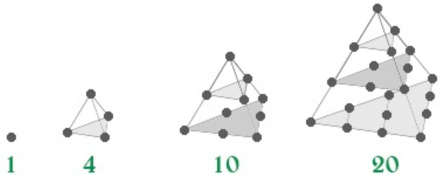
- Guardando alla colonna $k = 3$ troviamo i numeri tetraedrici, ovvero i numeri interi $t_1, t_2, t_3, \ldots$ che sono, per ogni i, la somma dei primi i numeri triangolari
- Quindi, i numeri $1, 3, 6, 10, 15, \ldots$... che verificano

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

- Si può facilmente dimostrare per induzione (esercizio) che vale

$$t_n = \frac{(n+2)(n+1)n}{6} = \binom{n+2}{3}$$

- Un numero tetraedrico, o numero piramidale triangolare, ha questo nome perché rappresenta una piramide con una base triangolare (un tetraedro)



Esercizio

- Dimostriamo per induzione che

$$t_n = \sum_{i=1}^{n} \frac{i(i+1)}{2} = \frac{(n+2)(n+1)n}{6} = \binom{n+2}{3}$$

- Per $n = 1$ abbiamo $t_1 = \frac{1(1+1)}{2} = 1$ ed inoltre $\frac{(1+2)(1+1)1}{6} = \frac{6}{6} = \binom{1+2}{3} = 1$
- Supponiamo allora che

$$t_{n-1} = \sum_{i=1}^{n-1} \frac{i(i+1)}{2} = \frac{(n+1)(n)(n-1)}{6}$$

Allora

$$\begin{aligned} t_n &= t_{n-1} + \frac{n(n+1)}{2} = \frac{(n+1)(n)(n-1)}{6} + \frac{n(n+1)}{2} = \\ &= \frac{(n+1)(n)(n-1) + 3n(n+1)}{6} = \frac{(n+1)(n)(3+n-1)}{6} = \\ &= \frac{(n+2)(n+1)n}{6} \end{aligned}$$

Combinazioni con ripetizione

- Dato un insieme di n variabili, $\{x_1, x_2, \ldots, x_n\}$ e preso un un intero $k \leq n$, il numero di monomi, con coefficiente 1, di grado k include sicuramente tutti i monomi composti da k variabili diverse, che ovviamente sono $\binom{n}{k}$.
- Vogliamo dimostrare che

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

Esempio variabili $\{x, y, z\}$ e monomi di grado 2.

Dato un insieme di 3 variabili, i monomi di grado 2 sono i seguenti $6 = \binom{3+2-1}{2} = \binom{4}{2}$

$$xy \; xz \; yz$$
$$x^2 \; y^2 \; z^2$$

Combinazioni con ripetizione

- Vediamo un altro esempio. Supponiamo di avere 5 variabili, $\{a, b, c, d, e\}$,
- i monomi di grado 3 sono i seguenti $C^r_{5,3} = \binom{5+3-1}{3} = \binom{7}{3} = 35$

$$
\begin{array}{r}
abc\ abd\ abe\ acd\ ace \\
ade\ bcd\ bce\ bde\ cde \\
a^2b\ a^2c\ a^2d\ a^2e \\
ab^2\ b^2c\ b^2d\ b^2e \\
ac^2\ bc^2\ dc^2\ ec^2 \\
ad^2\ bd^2\ cd^2\ ed^2 \\
ae^2\ be^2\ ce^2\ de^2 \\
a^3\ b^3\ c^3\ d^3\ e^3
\end{array}
$$

Combinazioni con ripetizione

- Dato un insieme di n variabili, $\{x_0, x_2, \ldots, x_{n-1}\}$ e preso un un intero $k \leq n$, dimostriamo che i monomi di grado k sono

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

- Assumiamo che il monomio sia rappresentato da un'array di interi M di lunghezza n dove $M[i]$ è il grado della variabile x_i nel monomio. Ovviamente se $M[i] = 0$ la variabile non appare nel monomio. Inoltre, dal momento che il monomio è di grado k abbiamo che

$$\sum_{i=0}^{n-1} M[i] = k.$$

Combinazioni con ripetizione

- Sia M un'array di lunghezza n rappresentante un monomio di grado k in n variabili, dove per ogni $0 \leq i \leq n-1$ $M[i]$ è il grado della variabli x_i.
- Associeremo ad M, in maniera univoca, un'array (lista) binaria L di $n+k-1$ tale che $n-1$ dei suoi elementi avranno valore 0 ed i rimanenti k avranno valore 1.
- Per decidere dove mettere i valori 0 in L, costruiamo come prima cosa un'array di indici I di lunghezza $n-1$, i cui elementi ci diranno dove mettere i valori 0, in questo modo
  - Fissiamo $I[0] = M[0]$ e
  - per ogni $0 < j \leq n-2$ poniamo $I[j] = I[j-1] + M[j] + 1$
- Data l'array di indici I, costruiamo L come segue
  - Per ogni $0 \leq j \leq n-2$ poniamo $L[I[j]] = 0$
  - Poniamo uguale ad 1 le rimanenti k posizioni di L.
- Intuitivamente, allora, gli 1 prima del primo zero, ci danno la potenza della prima variabile, quelli dopo l'ultimo zero la potenza dell'ultima variabile, e quelli tra lo i-esimo zero e lo $(i+1)$-esimo, ci danno la potenza della i-esima variabile.

Combinazioni con ripetizione

- Utilizzando l'esempio di prima, 5 variabili, $\{a, b, c, d, e\}$, e monomi di grado 3 vediamo in alcuni casi la costruzione delle rispettive array L

$$
\begin{array}{rcl}
abc & \rightarrow & M = [1,1,1,0,0], I = [1,3,5,6], L = [1,0,1,0,1,0,0] \\
bde & \rightarrow & M = [0,1,0,1,1], I = [0,2,3,5], L = [0,1,0,0,1,0,1] \\
a^2c & \rightarrow & M = [2,0,1,0,0], I = [2,3,5,6], L = [1,1,0,0,1,0,0] \\
bc^2 & \rightarrow & M = [0,1,2,0,0], I = [0,2,5,6], L = [0,1,0,1,1,0,0] \\
de^2 & \rightarrow & M = [0,0,0,1,2], I = [0,1,2,4], L = [0,0,0,1,0,1,1] \\
a^3 & \rightarrow & M = [3,0,0,0,0], I = [3,4,5,6], L = [1,1,1,0,0,0,0] \\
b^3 & \rightarrow & M = [0,3,0,0,0], I = [0,4,5,6], L = [0,1,1,1,0,0,0] \\
c^3 & \rightarrow & M = [0,0,3,0,0], I = [0,0,5,6], L = [0,0,1,1,1,0,0] \\
d^3 & \rightarrow & M = [0,0,0,3,0], I = [0,0,0,6], L = [0,0,0,1,1,1,0] \\
e^3 & \rightarrow & M = [0,0,0,0,3], I = [0,1,2,3], L = [0,0,0,0,1,1,1]
\end{array}
$$

Combinazioni con ripetizione

- Con la formalizzazione appena definita, possiamo dire che ogni monomio di n variabili di grado k corrisponde alla scelta di k posizioni da un insieme di $n+k-1$ posizioni.
- Quindi
$$C^r_{n,k} = \binom{n+k-1}{k}$$

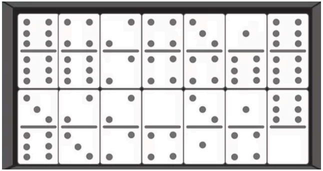
Esempio insieme di 7 variabili

I monomi di grado 3 sono

$$C^r_{7,3} = \binom{7+3-1}{3} = \binom{9}{3} = \frac{9!}{3!6!} =$$

Esercizio 1: il Domino

Nel gioco del domino si usano delle tavoletta divise in due parti uguali, ciascuna contenente un numero da 0 a 6. I numeri sulle due parti di una stessa tavoletta possono essere uguali. Una tavoletta può quindi essere rappresentata dal simbolo $[x, y]$ con $x, y \in \{0, 1, 2, 3, 4, 5, 6\}$. Quante tavolette ci sono?



Risposta: Il numero di tavolette con numeri diversi è ovviamente $\binom{7}{2} = 21$ ovvero tutti i modi possibili di scegliere 2 elementi da un insieme di 7. Se aggiungiamo le 7 tavolette dove i due numeri coincidono, otteniamo il totale: 28.

Esercizio 2: Gruppi di persone

Il capo del personale di una azienda deve assumere 4 persone. Al colloquio si presentano 8 candidati di cui 5 uomini e 3 donne.

(1) Quanti sono i possibili gruppi di 4 persone scelte ?

(2) I possibili gruppi formati solo da candidati maschi sono di più di quelli in cui ci sono tutte e tre le donne?

Risposta:

(1) Quanti sono i possibili gruppi di 4 persone scelte ? $\binom{8}{4} = (8 \cdot 7 \cdot 6 \cdot 5)/(4!) = 70$.

(2) I possibili gruppi formati solo da candidati maschi sono di più di quelli in cui ci sono tutte e tre le donne? Nel primo caso, i gruppi sono $\binom{5}{4} = 5$ e nel secondo caseo $\binom{5}{1} = 5$ quindi lo stesso numero.

Esercizio 3: Parole di 4 lettere

Quante sono le parole (non necessariamente di senso compiuto) formate da quattro lettere distinte che si possono ottenere utilizzando il vocabolo "CATANIA" ?

Risposta: Le lettere del vocabolo CATANIA sono $\{C, A, T, N, I\}$.
I gruppi di 4 lettere sono allora $\binom{5}{4} = 5$.
Ognuno di questi 5 gruppi consente di creare $4! = 24$ parole.
Quindi, in totale, $24 \cdot 5 = 120$.

Esercizio 4: Gelato per tutti

20 studenti vanno da un gelataio per comprare un cono gelato. Ci sono 8 gusti di gelato diversi ed ognuno può scegliere 3 porzioni di gelato (anche uguali) per formare il suo cono gelato. E' possibile per gli studenti avere tutti un gelato diverso? Ovvero, quanti diversi tipi di cono gelato si possono formare ?

Risposta: Il numero di coni possibili è il numero di combinazioni con ripetizione di classe 3 di 8 elementi. Ovvero

$$C^r_{8,3} = \frac{10!}{3!7!} = \frac{10 \cdot 9 \cdot 8}{6} = 120$$

Quindi, la risposta è positiva.

Introduzione

Il *Principio dei cassetti*, detto anche
principio del *buco della piccionaia* (in inglese *Pigeonhole principle*)
è un esempio di argomento in calcolo combinatorio applicabile
a molti problemi. Fu introdotto dal matematico tedesco Dirichlet

Nella sua forma più semplice, il Principio afferma che
se dobbiamo fare entrare $n+1$ piccioni
in una piccionaia che contiene n cassette,
allora almeno una cassetta dovrà contenere più di un piccione.
Più in generale, se abbiamo $n = km + 1$ oggetti da sistemare in
m contenitori, allora almeno un contenitore dovrà contenere
$k+1$ oggetti.

Esempio: la coppia di calzini

- Immaginiamo di avere il cassetto di un comodino pieno di calzini, neri e blue.
- Vogliamo, prendere al buio il numero minimo di calzini sufficiente ad avere una coppia completa.
- Immaginiamo che ogni colore sia "un cassetto". Se prendiamo 3 calzini, almeno 2 calzini saranno dello stesso colore.
- Infatti, in questo caso, possiamo avere o 3 calzini dello stesso colore, oppure 2 di un colore ed il terzo dell’altro colore.

Esempio: Numero di capelli

- Un essere umano ha, in media, circa 110000 capelli sulla testa. Qualcuno, arriva sino a 150000 mila. Se vogliamo esagerare, possiamo pensare che ci siano persone che abbiano sino a 200000 capelli in testa.
- Domanda: esistono due persone con lo stesso numero di capelli in testa?
- Risposta: si. Ed ecco la prova:
  - Catania città ha più di 300000 abitanti.
  - Dal momento che il numero di abitanti è superiore al numero massimo di capelli possibile, esisteranno sicuramente almeno 2 abitanti di Catania che hanno lo stesso numero di capelli in testa.

Esercizio: insieme di interi

- Sia S un insieme di $n+1$ interi diversi. Vogliamo dimostrare che esistono 2 interi $a, b \in S$ tali che $a-b$ è un multiplo di n.
- Come fare?
- Consideriamo l'insieme di interi $M = \{a \bmod n : a \in S\}$. Dal momento che i resti modulo n sono esattamente n di sicuro $|M| \leq n$
- Ma gli interi in S sono $n+1$, quindi esistono due interi tali $a, b \in S$ tali che $a \bmod n = b \bmod n$ e quindi $a - b \equiv 0 \mod n$.

Esercizio: Numero di amici

- Supponiamo di avere n persone in una stanza (tutte rigorosamente con la mascherina ed a distanza di almeno 1 metro l'una dall'altra!).
- Dimostriamo che almeno 2 di queste persone hanno lo stesso numero di amici tra le persone nella stanza.
- Procediamo per casi
  - Caso 1: esiste una persona x che non ha amici. Allora le altre $n-1$ persone possono avere ciascuno al massimo $n-2$ amici. Se esiste y che non ha amici, allora x e y hanno lo stesso numero di amici, ossia 0. Se invece ognuna delle $n-1$ persone ha almeno 1 amico, il numero di amici per ognuno di loro è compreso tra 1 e $n-2$. Ossia, $n-2$ valori totali per un numero di $n-1$ persone. Quindi, per il Pigeonhole principle almeno 2 di essi hanno lo stesso numero di amici.
  - Caso 2: tutte le n persone hanno almeno un amico. Ognuno di loro ha quindi un numero di amici che varia da 1 a $n-1$ e come prima, allora, ce ne saranno almeno 2 per cui tale valore coincide.

Esercizio: Classi modulo n

- Supponiamo di avere un insieme S di m interi positivi, e sia $0 < n < m$.
- Dividiamo m per n ed otteniamo quoziente q e resto r.
- Allora, se $r = 0$ esistono almeno q interi in S tutti congrui modulo n, ovvero che hanno lo stesso resto della divisione per n.
- Se invece $r \neq 0$, esistono almeno $q + 1$ interi in S tutti congrui modulo n.
- Vediamo degli esempi
  - Per $m = 100$ e $n = 7$ esistono almeno 15 interi in S che divisi per 7 hanno lo stesso resto
  - Per $m = 100$ e $n = 5$ ne esistono 20 di interi tra loro congrui modulo 5
  - Per $m = 100$ e $n = 11$ esistono 10 interi tra loro congrui modulo 11.

Esercizio: Classi modulo n

- Dimostriamo la proprietà. Supponiamo, quindi, di avere un insieme S di m interi positivi, e sia $0 < n < m$.
- Dividiamo m per n e siano q il quoziente e r il resto.
  - Caso 1: supponiamo $r = 0$. Quindi $m = q \cdot n$. Distribuiamo gli m numeri in S in n cassetti numerati da 0 a $n - 1$, ovvero i resti della divisione per n. Quando abbiamo distribuito $m - n$ numeri, e non abbiamo ancora un cassetto con q numeri, vuol dire che ci sono $q - 1$ numeri in ognuno dei n cassetti. La distribuzione dei rimanenti n ci garantisce che almeno uno di tali cassetti alla fine ne conterrà almeno q.
  - Caso 2: supponiamo $r \neq 0$. Come nel caso precedente, distribuiamo i m numeri in S in n cassetti numerati da 0 a $n - 1$. Quando ne avremo distribuiti $m - r$ ed ancora non ne abbiamo $q + 1$ nello stesso cassetto, vuol dire che ognuno dei $n - 1$ cassetti ne contiene esattamente q. I rimanenti r ci garantiscono che almeno uno di tali cassetti alla fine ne conterrà almeno $q + 1$.

STRUTTURE DISCRETE

PARTE 3: CALCOLO COMBINATORIO e PROBABILITA' DISCRETE

2: Probabilità Discrete

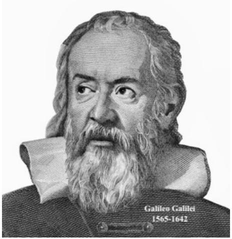
Introduzione

Lo studio sistematico della Teoria delle Probabilità nasce, tra la fine del XVI e gli inizi del XVII secolo, da problemi legati al gioco d'azzardo, tra cui il gioco dei dadi.

Uno dei padri fondatori è di sicuro il medico, matematico e filosofo italiano, Gerolamo Cardano. La sua vita è degna di un film drammatico e d'avventura. Ma limitiamoci a dire che, tra le altre cose, aveva il "vizio" del gioco ed in particolare dei dadi. Scrisse un libro il "De Ludo Aleae" dove introdusse i concetti fondamentali della teoria della probabilità e dove, tra le altre cose, chiariva alcuni aspetti su come fare a barare.

Introduzione

Su richiesta del Granduca di Toscana, Galileo scrive un libro, "Sulla scoperta dei dadi", in cui dimostra che lanciando 3 dadi, la probabilità di ottenere la somma 10 oppure 11 è più alta della probabilità di ottenere 9 o 12.



Introduzione

Successivamente, un nobile accanito giocatore francese, pone a Pascal il seguente problema: è più probabile che esca un 6 lanciando 4 volte un dado o avere almeno una volta il doppio 6 lanciando 24 volte 2 dadi?

Pascal ne scrive a Fermat.
Dalla loro collaborazione epistolare nascono le prime leggi della probabilità e si approfondisce il calcolo combinatorio e l'utilizzo dei coefficienti binomiali.

Eventi e spazio dei Campionii

- Le probabilità sono definite su uno spazio di campioni S, i cui elementi sono detti eventi elementari.
- Ogni evento elementare è l?esito di un esperimento ed è un sottoinsieme dello spazio dei campioni.
- S stesso è l'evento certo, mentre $\emptyset$ è l'evento nullo
- Due eventi E_1 e E_2 sono mutuamente esclusivi se $E_1 \cap E_2 = \emptyset$.

Esempio

Per l'esperimento del lancio di 2 monete, lo spazio dei campioni è costituito da tutte le possibili coppie $S = \{TT, TC, CT, CC\}$.
L'evento "si ottiene una testa ed una croce" è $E = \{TC, CT\}$

Intuizione

- La definizione classica ed intuitiva della probabilità del verificarsi di un evento A è il rapporto tra il numero di casi favorevoli, f_A ed il numero di casi totali n quindi

$$P(A) = \frac{f_a}{n}$$

- Notiamo che questa definizione assume implicitamente che tutti gli eventi possono accadere con la stessa "probabilità." Quindi, è una definizione "circolare".

Esempio

Per l'esperimento del lancio di un dado, e l'evento "Esce un numero inferiore a 3 lo spazio dei campioni è costituito da tutte i possibili esiti del lancio, ovvero $S = \{1, 2, 3, 4, 5, 6\}$ e gli esiti favorevoli sono solo 2 ovvero $\{1, 2\}$.
Quindi la probabilità di tale evento è $\frac{2}{6} = \frac{1}{3}$.

Definizione frequentista

- La definizione classica non considerava la possibilità di eventi non equiprobabili.
- Per superare tali problemi un matematico austriaco-americano, Richard von Mises, propose la definizione frequentista (e peraltro è anche famoso per avere definito e proposto il paradosso del compleanno).

Semplificando il discorso, assumiamo di ripetere un esperimento n volte e verifichiamo quante volte si è verificato l'esito studiato. Per esempio, lanciamo il dado 10 volte e vediamo quante volte è uscito un numero inferiore a 3. Definiamo la probabilità dell'evento come il limite del rapporto tra il numero di volte in cui si è verificato l'esito f_A ed il numero degli esperimenti n

$$P(A) = \lim_{n \to \infty} \frac{f_A}{n}$$

Definizioni assiomatiche

- La definizione frequentista ha un problema di fondo insuperabile: non tutti gli esperimenti sono ripetibili e quindi alcune probabilità non sarebbero calcolabili.
- Per esempio, qual'è la probabilità che entro i prossimi 100 anni un meteoroide colpisca la terra generando la quasi estinzione della vita come accadde ai tempi dei dinosauri?

Probabilità soggettive

Per superare questi problemi, il matematico italiano Bruno De Finetti propose una una definizione di probabilità soggettiva per poter anche definire valori di probabilità di eventi elementari non tutti equiprobabili o ottenuti da esperimenti non ripetibili.

Utilizzabili nel campo dei giochi, tali assiomi devono soddisfare un criterio di coerenza, ovvero le probabilità degli eventi devono essere attribuite in modo tale che non sia possibile ottenere una vincita o una perdita certa.

Inoltre, un qualunque giocatore che gioca non tenendo conto di tali assiomi è destinato a perdere.

Definizione assiomatica

L'impostazione assiomatica della probabilità venne proposta dal matematico russo Andrej Kolmogorov nel 1933, all'interno della teoria matematica della misura.

La definizione assiomatica
non è una definizione operativa e quindi non ci fornisce metodologie di calcolo dei valori di probabilità.

È quindi una definizione assiomatica che si può utilizzare sia nell'ambito di un approccio oggettivista che nell'ambito di un approccio soggettivista.

Teoria della Probabilità

Dagli studi di De Finetti e Kolmogorov, otteniamo gli assiomi della Teoria della Probabilità.

- Una distribuzione di probabilità **P** in uno spazio di campioni S associa agli eventi numeri reali, soddisfacendo i seguenti assiomi:
- Siano A e B due eventi qualsiasi (sottoinsiemi di S)

A1 $0 \leq P(A) \leq 1$
A2 $P(S) = 1$ e $P(\emptyset) = 0$
A3 $P(A \cup B) = P(A) + P(B) - P(A \cap B)$

Teoria della Probabilità

- L'assioma (A3) può essere riscritto utilizzando il formalismo logico, in questo modo:

$$P(A \vee B) = P(A) + P(B) - P(A \wedge B)$$

- ossia: "*La probabilità che si verifichi A oppure B è la probabilità che si verifichi A più la probabilità che si verifichi B meno la probabilità che si verifichino entrambi.*
- Se due eventi A e B sono mutuamente esclusivi ovvero se $A \cap B = \emptyset$, si ha allora

$$P(A \vee B) = P(A) + P(B)$$

- In particolare, quindi, abbiamo

$$P(A \vee \neg A) = P(S) = 1$$

  e quindi

$$P(\neg A) = 1 - P(A)$$

  ovvero, la probabilità che un evento non si verifichi è uguale a 1 meno la probabilità che l'evento si verifichi.
- La distribuzione di probabilità è detta uniforme se tutti gli eventi sono equiprobabili.

Probabilità condizionata e Indipendenza

- Il verificarsi di un evento talvolta può cambiare la probabilità che si verifichi un altro evento, e talvolta invece non ha influenza. La probabilità di un evento A, condizionata al verificarsi di un evento B (non nullo) è definita come

$$P(A|B) = \frac{P(A \wedge B)}{P(B)}$$

- Due eventi si dicono indipendenti se
  - $P(A|B) = P(A)$
  - $P(B|A) = P(B)$
- Quindi, se A e B sono indipendenti

$$P(A \wedge B) = P(A) \cdot P(B)$$

Indipendenza

- Il concetto di indipendenza è spesso *dimenticato* causando errori molto gravi.
- Per esempio, errore comune, per chi gioca al "lotto", è pensare che se un numero non esce da tante estrazioni, allora la probabilità di uscire alla prossima è più alta.
- Niente di più falso, perché la probabilità rimane la stessa, essendo le estrazioni eventi indipendenti.

Esempio semplice

Lanciamo un dado 3 volte. La probabilità della sequenza $[2, 1, 6]$ è più alta della probabilità della sequenza $[3, 3, 3]$?
Risposta: no, le due probabilità sono uguali.
La probabilità di ottenere 2 al primo lancio è $\frac{1}{6}$, così come la probabilità di ottenere 1 al secondo e 6 al terzo. Quindi $P([2, 1, 6]) = \frac{1}{216}$.
Lo stesso ragionamento ci porta a concludere che $P([3, 3, 3]) = \frac{1}{216}$.

Regola di Bayes

Dalla definizione di probabilità condizionata, si ricava agevolmente una delle regole probabilistiche con il maggior numero di applicazioni in quasi tutti i campi della scienza ed in particolare in Informatica, in generale, e Intelligenza Artificiale in particolare.

Prende il nome da Thomas Bayes, un matematico, statistico e sacerdote presbiteriano britannico che per primo la usò su problemi matematici nella prima metà del 1700.

Regola di Bayes

- Ricordiamo che la probabilità di un evento A, condizionata al verificarsi di un evento B (non nullo) è definita come

$$P(A|B) = \frac{P(A \wedge B)}{P(B)} \text{ ovvero } P(A|B) \cdot P(B) = P(A \wedge B)$$

- Parimenti, la probabilità di B condizionata la verificarsi di A è

$$P(B|A) = \frac{P(B \wedge A)}{P(A)} \text{ ovvero } P(B|A) \cdot P(A) = P(B \wedge A)$$

- Quindi, dal momento che $P(A \wedge B) = P(B \wedge A)$ abbiamo l'equazione che è conosciuta universalmente come *Regola di Bayes*

$$P(B|A) = \frac{P(A|B) \cdot P(B)}{P(A)}$$

Regola di Bayes

- La regola di Bayes ha avuto grandi applicazioni nei sistemi esperti e inferenziali con particolare riferimento ai sistemi diagnostici
- Diagnosi vuol dire: "se sappiamo che un certo evento E causa certi effetti S, se osserviamo gli effetti S possiamo risalire alla causa?"
- La regola di Bayes ci consente l'automazione del processo di diagnosi se conosciamo le probabilità a priori di causa ed effetto.
- Supponiamo, per esempio, $P(E) = \frac{1}{10}$, $P(S) = \frac{4}{10}$ e $P(S|E) = \frac{7}{10}$. Allora

$$P(E|S) = \frac{P(S|E) \cdot P(E)}{P(S)} = \frac{\frac{7}{10} \cdot \frac{1}{10}}{\frac{4}{10}} = \frac{7}{40}$$

Teorema della Probabilità Totale

- Il calcolo della probabilità condizionata risulta essere molto spesso più semplice rispetto alla probabilità "a priori" ovvero quella non condizionata al verificarsi di altri eventi.
- In alcuni altri casi, il calcolo della probabilità di un evento deve tenere conto di due o più processi casuali.
- Il seguente teorema ci aiuta.

Teorema (Probabilità Totale)

Sia A un evento e siano $B_1, B_2, \ldots, B_n$ n eventi mutuamente esclusivi, tali che $P(B_i) \neq 0$ per ogni i ed inoltre $P(B_1 \vee B_2 \vee \cdots \vee B_)) = 1$, ovvero gli eventi sono esaustivi.
Allora

$$\begin{aligned} P(A) &= P(A|B_1)P(B_1) + P(A|B_2)P(B_2) + \cdots P(A|B_n)P(B_n) = \\ &= \sum_{i=1}^{n} P(A|B_i)P(B_i) \end{aligned}$$

Teorema della Probabilità Totale

Dimostrazione

- La dimostrazione del teorema è molto semplice.
- Dal momento che gli eventi $B_1, B_2, \ldots, B_n$ sono esaustivi, almeno uno di loro si deve verificare.
- Quindi se A si verifica, ci sarà un evento B_j tale che anche B_j si verifica. Dal momento che gli eventi B_i sono mutuamente esclusivi abbiamo
$$P(A) = P(A \wedge B_1) + \cdots + P(A \wedge B_n)$$
- dalla definizione di probabilità condizionata abbiamo per ogni i
$$P(A \wedge B_i) = P(A|B_i) \cdot P(B_i)$$
- e utilizzando tale uguaglianza si completa la dimostrazione.

$\triangle$

Teorema della Probabilità Totale: Esempio

- Supponiamo di dividere un mazzo di 52 carte in due mazzi: M_1 con 30 carte e M_2 con le rimanenti 22 carte.
- Supponiamo che in M_1 ci siano 3 dei 4 assi. Mentre in M_2 c'è il quarto asso.
- Scegliamo un mazzo a caso, e da quel mazzo scegliamo una carta a caso.
- Qual è la probabilità di pescare un asso $P(A)$?
- Chiaramente se scegliamo M_1 abbiamo $P(A|M_1) = \frac{3}{30} = \frac{1}{10}$
- Se scegliamo M_2 abbiamo $P(A|M_2)) = \frac{1}{22}$
- Per il teorema della probabilità totale

$$\begin{aligned} P(A) &= P(A|M_1) \cdot P(M_1) + P(A|M_2) \cdot P(M_2) = \frac{1}{10} \cdot \frac{1}{2} + \frac{1}{22} \cdot \frac{1}{2} = \\ &= \frac{1}{20} + \frac{1}{44} = \frac{16}{220} = \frac{4}{55} \end{aligned}$$

Problemi d'urna

- Tutti gli eventi che si possono formalizzare come "Estraiamo una o più palline numerate, da una o più urna" vengono detti, in calcolo delle probabilità "Problemi d'urna."
- Esempi:
  - Il lancio di uno o più dadi;
  - Estrazione dei numeri del lotto
- L'ipotesi comune è che le estrazioni siano, ovviamente, non truccate, e
- ogni estrazione è indipendente dalla precedente.

Problemi d'urna

- Le estrazioni da un'urna si possono classificare in 4 modi, combinando i seguenti 2 criteri
  - Estrazioni ordinate oppure no. Ovvero, se l'ordine di estrazione delle palline è importante oppure no.
  - Estrazione con reinserimento oppure no. Ovvero, se ad ogni estrazione di una pallina, la pallina estratta viene reinserita nell'urna.

Problemi d'urna

- Supponiamo di estrarre k palline da un'urna contenente n palline. Nei 4 casi possibili, il numero totale è
  - $D^r_{n,k} = n^k$ ovvero numero delle disposizioni con ripetizione, se l'ordine è importante e la pallina, dopo ogni estrazione, viene reinserita nell'urna.
  - $D_{n,k} = n \cdot (n-1) \cdot \ldots \cdot (n-k+1)$ ovvero numero delle disposizioni semplici, se l'ordine è importante ma la pallina estratta non viene reinserita nell'urna.
  - $C_{n,k} = \binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}$ ovvero combinazioni semplici, se l'ordine non è importante e la pallina estratta non viene reinserita nell'urna
  - $C^r_{n,k} = \frac{(n+k-1)!}{k! \cdot (n-1)!}$ ovvero numero combinazioni con ripetizione se l'ordine non è importante e la pallina estratta viene reinserita nell'urna

Codici PIN

- Rispondiamo ad una delle domande iniziali: Quanti sono i codici PIN di una carta bancomat a 5 cifre e quante sono le probabilità che un ladro riesca ad indovinare entro 3 tentativi? Abbiamo già visto che i codici PIN sono: $10^5 = 100000$.
  - La probabilità di sbagliare il primo tentativo è $\frac{10^5-1}{10^5}$.
  - La probabilità di sbagliare il secondo tentativo è $\frac{10^5-2}{10^5-1}$.
  - La probabilità di sbagliare anche il terzo tentativo è $\frac{10^5-3}{10^5-2}$.
- Quindi, la probabilità di sbagliare tutti e 3 i tentativi è

$$\frac{10^5-1}{10^5} \cdot \frac{10^5-2}{10^5-1} \cdot \frac{10^5-3}{10^5-2} = \frac{10^5-3}{10^5}$$

- Da cui, ne deduciamo che la probabilità di indovinare entro i primi tre tentativi, ovvero di non sbagliare tutti e 3 i primi 3 tentativi, è

$$1 - \frac{10^5-3}{10^5} = \frac{3}{10^5}$$

Galileo e il Granduca

Aiutiamo Galileo a rispondere alla domanda del Granduca di Toscana e proviamo a calcolare la probabilità di ottenere la somma 10 oppure 11, oppure la somma 9 o 12 lanciando 3 dadi

- Lo spazio dei campioni S sono tutte le triple $[x, y, z]$ corrispondenti al lancio dei 3 dadi, con x risultato del lancio del dado 1, y del dado 2 e z del dado 3. Quindi, la dimensione dello spazio del campioni è $6^3 = 216$.
- Ma le somme che si possono ottenere sono tutti i valori da 3 a 18, ovvero 16. Ma 16 non è un divisore di 216 quindi, necessariamente, alcune somme si ottengono un numero di volte diverso da altre.
- Per esempio la somma 3 posso ottenerla in un solo modo: quando tutti e 3 i dadi hanno valori 1. Analogamente la somma 18 posso ottenerla in un solo modo: quando tutti e 3 i dadi hanno valori 6.
- La somma 4 posso ottenerla solo come $1 + 1 + 2$ e questa somma corrisponde a 3 triple diverse: $[1, 1, 2]$, $[1, 2, 1]$, e $[2, 1, 1]$.
- La somma 6 posso ottenerla come (ma non solo) $1 + 2 + 3$ e questa somma corrisponde a 6 triple diverse: $[1, 2, 3]$, $[1, 3, 2]$, $[2, 1, 3]$, $[2, 3, 1]$, $[3, 1, 2]$, $[3, 2, 1]$.
- Quindi, la somma di 3 numeri uguali la ottengo una sola volta; la somma di 2 numeri uguali ed il terzo diverso, la ottengo in 3 modi diversi, e la somma di 3 numeri diversi la ottengo in 6 modi diversi.

Galileo e il Granduca

- Come posso ottenere il numero 10?
  - Risposta: con 6 somme diverse: $1+3+6$, $1+4+5$, $2+2+6$, $2+3+5$, $2+4+4$, $3+3+4$.
  - Per quanto visto prima, le 3 somme con 3 addendi diversi corrispondono ad un totale di 18 triple, e le 3 somme con 2 addendi uguali corrispondono ad un totale di 9 triple.
  - Quindi, la probabilità di ottenere 10, data dal rapporto dei casi favorevoli rispetto al totale, è

$$\frac{27}{216} = \frac{1}{6}.$$

Galileo e il Granduca

- In quanti modi posso ottenere 9, e qual è la probabilità?
  - Risposta: con 6 somme diverse: $1 + 2 + 6$, $1 + 3 + 5$, $1 + 4 + 4$, $2 + 2 + 5$, $2 + 3 + 4$, $3 + 3 + 3$.
  - Le 3 somme con 3 addendi diversi corrispondono ad un totale di 18 triple, le 2 somme con 2 addendi uguali corrispondono ad un totale di 6 triple, e la somma con 3 addendi uguali corrisponde ad una sola tripla.
  - Quindi, la probabilità di ottenere 9, data dal rapporto dei casi favorevoli rispetto al totale, è

$$\frac{25}{216}$$

Il paradosso del compleanno

- Rispondiamo adesso ad una delle domande iniziali:
- *Se dovessi scommettere che in un'aula con* 20 *persone, ce ne siano almeno* 2 *che fanno il compleanno lo stesso giorno, scommetterei di si oppure no? E se ce ne sono* $30, 40, 50$ *o più di persone?*.
- Ovvero ci stiamo chiedendo se, dato un certo numero di persone in un aula, la probabilità che 2 di esse facciano il compleanno lo stesso giorno sia maggiore di $\frac{1}{2}$
- Il problema è noto come *Il paradosso del compleanno* non perché la risposta corretta genera un paradosso logico ma perché è apparentemente controintuitiva.
- Notiamo subito che in un aula con più di 366 persone, di sicuro almeno 2 fanno il compleanno lo stesso giorno, per il Pigeonhole Principle.

Il paradosso del compleanno

- Rispondiamo per prima ad una domanda più semplice:
- *Qual è il numero minimo di persone presenti in un aula tale che la probabilità che due di esse siano nate lo stesso mese è maggiore di $\frac{1}{2}$?*.
- Ovviamente, se ci sono 13 persone, per il Pigeonhole Principle, almeno 2 di esse sono nate nello stesso mese.
- Proviamo con 3, e calcoliamo qual è la probabilità che siano nate tutte in mesi diversi.

Il paradosso del compleanno

- Abbiamo allora 3 persone $p1, p2, p3$ ed ognuna di esse può essere nata in uno qualunque dei 12 mesi dell'anno.
- Il numero totale di terne "[mese di nascita di $p1$, mese di nascita di $p2$, mese di nascita di $p3$]" è ovviamente
$$12^3 = 1728$$
- il numero totale di terne dove tutti e 3 i numeri sono diversi è dato dal numero totale di modi in cui possiamo scegliere tre valori diversi dall'insieme dei mesi, però contando le 6 permutazioni totali per ognuno di essi, quindi
$$3! \cdot \binom{12}{3} = 3! \frac{12!}{3!9!} = 12 \cdot 11 \cdot 10 = 1320$$
- Quindi, il numero di terne composte da numeri diversi è maggiore della metà del numero di terne totali, e di conseguenza la probabilità che 3 persone siano nate in un mese diverso è maggiore di $\frac{1}{2}$. Nello specifico tale probabilità è $\frac{1320}{1728} \simeq 0,76$.

Il paradosso del compleanno

- Un altro modo per calcolare tale probabilità è il seguente.
- Dato il mese di nascita della prima persona, avremo 11 casi su 12 possibili per la seconda persona e $10/12$ per la terza.
- Quindi la probabilità è data da

$$\frac{11}{12} \cdot \frac{10}{12} = \frac{110}{144} \simeq 0,76.$$

Il paradosso del compleanno

- Supponiamo allora di avere $n < 366$ persone.
- Calcoliamo la probabilità che facciano tutti il compleanno in un giorno diverso. Mettiamoci nel caso "peggiore", ovvero consideriamo l'anno bisestile ed assumiamo che i giorni dell'anno siano 366.
- Esempio:
  - Se $n = 2$ abbiamo 365 su 366 giorni possibili per la seconda, se devono essere giorni diversi. Quindi, la probabilità che siano nati in giorni diversi è $\frac{365}{366} = 0,997$.
  - Se $n = 3$ abbiamo 365 su 366 giorni possibili per la seconda, e 364 su 366 per la terza, se devono essere giorni diversi. Quindi, la probabilità che siano nati in giorni diversi è $\frac{365 \cdot 364}{366^2} = 0,991$.

Il paradosso del compleanno

- In generale, se abbiamo p persone, la probabilità che siano nate tutte in giorni diversi è

$$
\begin{aligned}
P_d(p) &= \frac{p! \cdot \binom{366}{p}}{366^p} = \frac{365!}{366^{p-1} \cdot (366-p)!} = \\
&= \frac{365 \cdot 364 \ldots \cdot (366-p+1)}{366^{p-1}}
\end{aligned}
$$

- Notiamo che

$$
P_d(p+1) = \frac{365 \cdot 364 \ldots \cdot (366-(p+1)+1)}{366^p} = P_d(p)\frac{366-p}{366}
$$

e in generale

$$
\begin{aligned}
P_d(p+h) &= \frac{365 \cdot 364 \ldots \cdot (366-(p+h)+1)}{366^{p+h-1}} = \\
&= P_d(p)\frac{(366-p) \cdot (366-p-1) \ldots \cdot (366-(p+h)+1)}{366^h}
\end{aligned}
$$

Il paradosso del compleanno

- Per quanto visto, la probabilità che almeno 2 persone, da un gruppo di p, facciano il compleanno lo stesso giorno è

$$P(p) = 1 - P_d(p) = 1 - \frac{365 \cdot 364 \cdot \ldots \cdot (366 - p + 1)}{366^{p-1}}$$

- Un po' di calcoli:
  - per $p = 10$

$$P_d(p) = \frac{365 \cdot 364 \cdot \ldots \cdot 357}{366^9} \simeq 0,88$$

  - per $p = 20$

$$\begin{aligned} P_d(p)) &= \frac{365 \cdot 364 \cdot \ldots \cdot 357 \cdot 356 \cdot \ldots \cdot 347}{366^{19}} \simeq \\ &\simeq 0,88 \cdot \frac{356 \cdot \ldots \cdot 347}{366^{10}} \simeq 0,88 \cdot 0.68 \simeq 0,58 \end{aligned}$$

  - per $p = 23$

$$\begin{aligned} P_d(p) &= \frac{365 \cdot \ldots \cdot 347 \cdot 346 \cdot 345 \cdot 344}{366^{22}} \simeq \\ &\simeq 0,58 \cdot \frac{346 \cdot 345 \cdot 344}{366^3} \simeq 0,58 \cdot 0.83 \simeq 0,48 \end{aligned}$$

Il paradosso del compleanno

- Quindi, se abbiamo 23 persone, la probabilità che nessuna coppia di queste persone faccia il compleanno lo stesso giorno è circa

$$P_d(p) = 0,48$$

- Quindi la probabilità che almeno una coppia di persone faccia il compleanno lo stesso giorno è

$$P(p) = 1 - P_d(p) = 1 - 0,48 = 0,52$$

- Quindi, dovessimo scommettere, converrebbe scommettere che dato un gruppo di almeno 23 persone scelte a caso (ed assumendo che tutti i giorni dell'anno siano equiprobabili per la nascita) almeno 2 di queste fanno il compleanno lo stesso giorno.

Esercizio 1

- A lancia una moneta una volta. B lancia una moneta 2 volte. Qual è la probabilità che A ottenga più teste di B ?
- Contiamo:
  - Eventi per A: T, C
  - Eventi per B TT, TC, CT, CC
  - Globalmente
    $T-TT, T-TC, T-CT, T-CC, C-TT, C-TC, C-CT, C-CC$
- Un caso su otto va bene quindi $\frac{1}{8}$

Esercizio 2

- Da un mazzo di 10 carte numerate dall'uno al dieci ne vengono rimosse 3.
- Qual è la probabilità che le tre carte scelte siano in ordine crescente?
- Contiamo:
  - Spazio dei campioni, tutte le permutazioni delle 10 carte, ossia 10!
  - Gli eventi vincenti sono le permutazioni i cui primi 3 elementi sono in ordine crescente. L'ordine degli altri 7 elementi non è importante.
  - 6 sono le possibili permutazioni di 3 elementi, una sola delle quali è quella ordinata.
- Quindi $\frac{1}{6}$

Esercizio 3

- Avete una moneta truccata che ritorna
  - Testa (T) con probabilità p
  - Croce (C) con probabilità $1 - p$
  - e $p \neq \frac{1}{2}$
- Volete usare tale moneta (l'unica che avete in tasca) per generare T e C con probabilità $\frac{1}{2}$, ovvero volete usare una moneta "truccata" per costruirne una non truccata. Come fare?

Esercizio 3: soluzione

- Utilizziamo il seguente algoritmo

_Moneta_non_truccata_
while (1) **do**
    $x = Lancio\_moneta\_falsa$;
    $y = Lancio\_moneta\_falsa$;
    if $x \neq y$ **return** x;
end_while

- In pratica, facciamo 2 lanci della moneta truccata.
- Se otteniamo lo stesso valore, ripetiamo. Altrimenti, diamo in output il primo dei due valori.

Esercizio 3: soluzione

- Abbiamo allora:
  - $P(Moneta\_non\_truccata() = T) = P(x = T \text{ e } y = C) = p(1-p)$
  - $P(Moneta\_non\_truccata() = C) = P(x = C \text{ e } y = T) = p(1-p)$
  - Le due probabilità sono uguali, quindi, in output il programma produce i valori di testa e croce con uguale probabilità
- Domanda (a cui risponderemo tra un po'): Quanti cicli del **while**-loop ci aspettiamo siano eseguiti prima di avere una risposta?

Variabile casuale e valore atteso

- Una variabile casuale è una funzione X che associa un numero reale ad un evento. Definiamo quindi un evento come il fatto che la variabile X assume un valore x ovvero $X = x$
- Possiamo allora definire il concetto di valore medio o valore atteso di una variabile casuale X come

$$E[X] = \sum_{x} x \cdot P[X = x]$$

Esempio

Se la variabile casuale X contiene il valore ottenuto dopo il lancio di un dado. Abbiamo che

$$E[X] = \sum_{x} x \cdot P[X = x] = 1 \cdot \frac{1}{6} + 2 \cdot \frac{1}{6} + 3 \cdot \frac{1}{6} + 4 \cdot \frac{1}{6} + 5 \cdot \frac{1}{6} + 6 \cdot \frac{1}{6} \cdot 6 = \frac{21}{6} = 3,5$$

Proprietà del valore atteso

- Il valore atteso ha una proprietà di linearità.
- Ovvero se abbiamo due variabili casuali X e Y e consideriamo la variabile casuale "somma" $X + Y$ allora

$$E[X + Y] = E[X] + E[Y]$$

Esempio

Se lanciamo due dadi, il valore atteso della somma Abbiamo che

$$E[X + Y] = E[X] + E[Y] = 3,5 + 3,5 = 7.$$

Esercizio

- Se lanciamo due dadi, qual è il valore atteso del massimo dei 2 valori?
- In questo caso, quindi, abbiamo una variabile casuale X il cui valore è il massimo dei due valori dati dal lancio dei 2 dadi.
- Abbiamo 36 casi possibili $\{(1,1),(1,2),\ldots,(6,5),(6,6)\}$ tutti equiprobabili, con probabilità $\frac{1}{36}$
    - Di coppie con "6" ne abbiamo 11
    - Di coppie con "5" ma senza "6" ne abbiamo 9
    - Di coppie con "4" ma senza "5" o "6" be abbiamo 7
    - Di coppie con "3" ma senza "4", "5", o "6" ne abbiamo 5
    - Di coppie con "2" ma senza "3", "4", "5" o "6" ne abbiamo 3
    - Di coppie con solo "1" ne abbiamo solo 1.
- Quindi

$$E[X] = [6 \cdot 11 + 5 \cdot 9 + 4 \cdot 7 + 3 \cdot 5 + 2 \cdot 3 + 1]/36 = \frac{161}{36} \simeq 4.47$$

Domanda

Conviene scommettere che, lanciando due dadi, il massimo dei 2 valori ottenuti sia maggiore di 4 ? Risposta: **SI**

Prova di Bernoulli

Una delle figure più importanti nello studio della probabilità fu il matematico svizzero Jacob Bernoulli (membro di una famiglia di Bernoulli molto prolifica).

Tra le sue scoperte più conosciute la costante e base dei logaritmi naturali e, nel calcolo delle probabilità formalizzò la *Legge dei Grandi Numeri* , di cui parleremo tra un po'.

Una prova di Bernoulli (o prova binomiale) è un esperimento probabilistico che ha esattamente due risultati: successo o fallimento.

Prova di Bernoulli

- Abbiamo quindi un esperimento con 2 uscite:
  - Successo con probabilità p
  - Insuccesso con probabilità $q = 1 - p$.
- Tutti i tentativi sono indipendenti l'uno dall'altro e
- la probabilità di successo rimane costante p.
- Se X è la variabile casuale che tiene conto del numero di tentativi (mdi una prova di Bernoulli per ottenere un successo, abbiamo

$$E[X] = 1 \cdot p + 2qp + 3q^2p + \ldots = \sum_{k=1}^{\infty} kq^{k-1}p = \frac{p}{q}\sum_{k=0}^{\infty} kq^k$$

- Supponiamo di essere bravi a calcolare sommatorie infinite ed otteniamo

$$\sum_{k=0}^{\infty} kq^k = \frac{q}{(1-q)^2} \text{ poiché per } q < 1 \ \sum_{k=0}^{\infty} q^k = \frac{1}{1-q}$$

Prova di Bernoulli

- Quindi, il valore atteso dei numeri di tentativi da fare per ottenere "successo" è
$$E[X] = \frac{p}{q}\frac{q}{(1-q)^2} = \frac{p}{p^2} = \frac{1}{p}$$
- Ne segue che minore è la probabilità dell'evento successo, maggiore è il numero di tentativi che bisogna fare.
- Esempi
  - Qual è il numero atteso di lanci di una moneta per ottenere testa? Risposta: $\frac{1}{1/2} = 2$
  - Qual è il numero atteso di lanci di un dado per ottenere "6" ? Risposta: $\frac{1}{1/6} = 6$
  - Pesco una carta da un mazzo siciliano: se è asso mi fermo, se non è asso la rimetto nel mazzo, mischio e riprovo. Qual è il numero atteso di carte che devo estrarre prima di pescare un asso? Risposta: $\frac{1}{1/10} = 10$

Prova di Bernoulli: Moneta truccata

- Riguardo all'esempio della moneta truccata, rispondiamo alla domanda: quanti cicli del il **while**-loop ci aspettiamo siano eseguiti prima di avere una risposta?
- Supponiamo la moneta dia testa con probabilità p (e croce con probabilità $1 - p$).
- il ciclo **while** termina l'esecuzione quando 2 lanci successivi danno un esito diverso.
- Le probabilità per 2 lanci sono:
  - $(T, T) : p^2$
  - $(C, C) : (1 - p)^2$
  - $(T, C) : p(1 - p)$
  - $(C, T) : (1 - p)p$
- Quindi, il ciclo **while** termina l'esecuzione con probabilità $2p(1 - p)$ e quindi, il numero atteso di cicli eseguiti è $\frac{1}{2p(1-p)}$
- Allora, se per esempio $p = \frac{1}{5}$ il numero atteso di cicli eseguiti è poco più di 3 mentre se $p = \frac{1}{20}$ il numero atteso di cicli eseguiti è poco più di 10.

Legge dei Grandi Numeri

- la Legge dei Grandi Numeri, detta anche teorema di Bernoulli, ci garantisce che la media dei risultati ottenuti dopo un grande numero di tentativi, si avvicina al valore medio atteso e, in effetti, lo eguaglia "al limite."
- Quindi, è un risultato che ci assicura, nel lungo termine, stabilità del valore medio di un evento casuale.
- Ciò implica che se dopo avere lanciato un dato per 100 volte, la media dei valori ottenuti differisce dal valor medio atteso $3,5$, dopo averlo lanciato 1000 volte la media dei valori ottenuti, "molto probabilmente" sarà più vicina al valore medio atteso.
- In altre parole, se lanciamo un dado un numero infinito di volte, la media ottenuta sarà esattamente $3,5$
- Ricordiamo, però, che la Legge vale solo su "grandi numeri", quindi ogni ragionamento del tipo: "*Il numero* 6 *non è uscito dopo* 100 *lanci, è più probabile che esca al lancio* 101", è un ragionamento **sbagliato**.

Tre assi

- Qual è la probabilità di estrarre 3 assi di seguito da un mazzo di carte (52) ?
- Rispondiamo al quesito in 2 modi diversi, che ovviamente ci daranno lo stesso risultato.
- Soluzione 1:
  - Quante sono i possibili insiemi di 3 carte? Ovviamente tante quante sono le combinazioni semplici ovvero $C_{52,3} = \binom{52}{3} = \frac{52!}{3! \cdot 49!} = 22100$
  - Quante sono le possibili terne di 3 assi? Ovviamente tante quante le combinazioni semplici $C_{4,3} = \binom{4}{3} = 4$
  - Allora, la probabilità di estrarre 3 assi di seguito è $\frac{4}{22100} = \frac{1}{5525}$
- Soluzione 2:
  - La probabilità di estrarre un asso come prima carta è $\frac{4}{52}$. Restano 3 assi e 51 carte.
  - La probabilità di estrarre un asso come seconda carta è allora $\frac{3}{51}$. Restano 2 assi e 50 carte.
  - La probabilità di estrarre un asso come terza carta è allora $\frac{2}{50}$.
  - La probabilità di estrarre 3 assi di seguito è allora: $\frac{4}{52} \cdot \frac{3}{51} \cdot \frac{2}{50} = \frac{24}{132600} = \frac{1}{5525}$
- Quindi, il numero atteso di tentativi per poter pescare 3 assi da un mazzo di 52 carte è 5525.

Poker servito

- Rispondiamo alla domanda iniziale: "Se sto scrivendo un programma che simula il poker, il mio programma deve fare in modo che la probabilità di un poker d'assi servito sia quella giusta. Ma qual è tale probabilità? "
- Soluzione
  - Una mano di poker è fatta da 5 carte, ossia ogni giocatore riceve, in maniera casuale, 5 delle 52 carte del mazzo.
  - Quante sono i possibili insiemi di 5 carte? Ovviamente tante quante sono le combinazioni semplici ovvero

$$C_{52,5} = \binom{52}{5} = \frac{52!}{5! \cdot 47!} = 2598960$$

  - Quante sono le combinazioni di 5 carte che contengono tutti i 4 assi? Ovviamente, tante quanti sono i modi diversi di scegliere la quinta carta. Quindi $52 - 4 = 48$.
  - Allora, la probabilità di avere un poker d'assi servito è $\frac{48}{2598960}$ ossia circa 18 su un milione.
- Ne segue che il numero atteso di mani di poker che bisogna giocare per avere un poker d'assi servito è poco più di 55 mila.

Scala reale servita

- Cerchiamo di essere più ambiziosi. Calcoliamo la probabilità di ricevere una scala reale servita.
- Soluzione
  - Cominciamo con il contare quante sono le scale reali per un particolare seme. Ricordiamo che una scala reale è una sequenza consecutiva di 5 carte dello stesso seme. Ricordiamo anche che l'asso (che scriviamo sia come 1 che come A) partecipa a due di queste scale: $1, 2, 3, 4, 5$ e $10, J, Q, K, A$.
  - Quindi, per contare le scale di uno stesso seme, contiamo il valore della carta minima, e scopriamo che sono esattamente 10.
  - Allora abbiamo 10 scale possibili per ognuno dei 4 semi, per un totale di 40 scale reali possibili.
  - Quindi, probabilità di avere servita una scala reale è

$$\frac{40}{C_{52,5}} = \frac{40}{2598960}$$

  ossia circa 15 su un milione.
- Ne segue che il numero atteso di mani di poker che bisogna giocare per avere una scala reale servita è poco più di 66 mila.

Palline in urna

- In un'urna ci sono 3 palline bianche e 2 nere.
- Calcolare la probabilità che in due estrazioni con reintroduzione della pallina estratta, escano 2 palline di diverso colore.
- Soluzione
  - Cominciamo con il contare quanti sono i casi possibili. Trattandosi di estrazioni con reintroduzione, i casi possibili sono $5^2 = 25$.
  - La probabilità che escano due palline bianche è $\frac{3}{5} \cdot \frac{3}{5} = \frac{9}{25}$, ovvero in 9 casi su 25 abbiamo 2 palline bianche.
  - La probabilità che escano due palline nere è $\frac{2}{5} \cdot \frac{2}{5} = \frac{4}{25}$, ovvero in 4 casi su 25 abbiamo 2 palline nere.
  - Rimangono 12 casi, e quindi la probabilità di avere due palline di diverso colore è $\frac{12}{25}$.
- Ne segue che il numero atteso di estrazioni per avere due palline di diverso colore è poco più di 2.

Urna del Lotto

- In un'urna 90 palline numerate da 1 a 90. Ne estraggo 5. Qual è la probabilità di estrarre la pallina con il numero 1 ?
- Soluzione
  - Cominciamo con il contare quanti sono i casi possibili. Il numero totale di diverse estrazioni di 5 numeri è $\binom{90}{5}$.
  - Quante di queste contengono il numero 1? Esattamente tante quante sono le possibili estrazioni di 4 numeri da un insieme di 89 (e poi si aggiunge il numero 1. Quindi, $\binom{89}{4}$.
  - La probabilità allora che il numero 1 sia estratto è

$$\frac{\binom{89}{4}}{\binom{90}{5}} = \frac{2441626}{43949268} \sim \frac{5,7}{100}$$

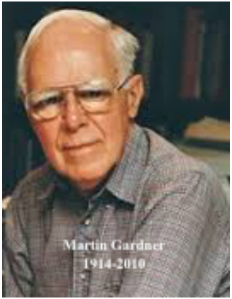
- Ne segue che il numero atteso di estrazioni per avere il numero 1 è circa 18.

STRUTTURE DISCRETE

PARTE 3: CALCOLO COMBINATORIO e PROBABILITA' DISCRETE

3: Caso Studio: Giochi e Paradossi probabilistici

Introduzione



Come abbiamo già visto nel caso del paradosso del compleanno, ci sono dei problemi per i quali il calcolo corretto delle probabilità genera una risposta fortemente contro-intuitiva.

Molti di questi casi, proposti come giochi, sono diventati famosi sia per alcune dispute generate che per l'abilità e "genialità" dei proponenti.

Il più famoso di tutti fu di sicuro Martin Gardner, matematico e divulgatore scientifico americano, che per anni curò la rubrica "Giochi Matematici" (Mathematical Games) sulla rivista Scientific American.

Introduzione

Qui rivediamo 4 degli esempi più famosi

- Il paradosso dei 2 bambini (proposto da M. Gardner nel 1959)
- Il paradosso delle 3 carte o delle 3 scatole
- Il paradosso dei 3 prigionieri (proposto da M. Gardner nel 1959)
- Il paradosso **Monty Hall** (1975, 1990).

Paradosso dei 2 bambini

- "*Un giovane professore di Probabilità passeggia con il figlio. Quando l'ho incontrate vi dice che di figli ne ha* 2 *e poi vi chiede: qual è la probabilità che anche l'altro mio figlio sia un maschietto?*"
- Attenzione! Prima di rispondere riflettete sul fatto che il quesito appena posto è equivalente a questo
  - "*Il professore di Probabilità ha due bambini. Non sono due femmine. Qual è la probabilità che entrambi i bambini siano maschi?*"

Paradosso dei 2 bambini: Risposta

- Analizziamo i possibili scenari:

Tabella: 4 possibilità

Figlio 1	Figlio 2
F	F
F	M
M	F
M	M

- La prima possibilità è esclusa, perché uno dei due figli è maschio.
- Rimangono quindi 3 possibilità e una sola di queste è quella in cui entrambi i figli sono maschi.
- Allora la risposta è:

La probabilità che anche l'altro sia maschio è $\frac{1}{3}$

Paradosso delle 3 carte (scatole)

- Il paradosso delle 3 carte, nella versione equivalente delle 3 scatole, era già conosciuto alla fine del '800. Ecco le due versioni:
  - "*Ci sono* 3 *carte, una "R" che è rossa su entrambi i lati, un'altra "B" che è bianca su entrambi i lati, e la terza "M" che è rossa da un lato e bianca dall'altro lato. Prendiamo una delle tre carte a caso e la poniamo sul tavolo su uno dei due lati, anche questo scelto a caso. Se vediamo che il lato visibile è rosso, qual è la probabilità che anche il lato non visibile sia rosso?*"
  - "*Ci sono* 3 *scatole, una scatola "G2" contiene* 2 *monete d'oro. Un'altra scatola "A2" contiene* 2 *monete d'argento. La terza scatola "AG" contiene una moneta d'oro e una d'argento. Prendiamo una delle tre scatole a caso, la apriamo e prendiamo una delle* 2 *monete a caso. Se la moneta presa a caso è una moneta d'oro, qual è la probabilità che anche l'altra moneta dentro la scatola sia una moneta d'oro ?*"

Paradosso delle 3 carte (scatole): Risposta

- Rispondiamo al quesito nella versione delle 3 carte. La risposta al quesito delle 3 scatole sarà la stessa.
- Ogni carta ha due lati, che indichiamo con le lettere "a" e "b". Per la carta "M" assumiamo che il lato "Ma" sia rosso mentre il lato "Mb" bianco.

Tabella: 6 possibilità

Lato visibile	Lato nascosto
Ra	Rb
Rb	Ra
Ma	Mb
Mb	Ma
Ba	Bb
Bb	Ba

- Due di questi 3 casi ci dicono che il lato non visibile è pure rosso. Allora la risposta è:

La probabilità che anche il lato non visibile sia rosso è $\frac{2}{3}$

Paradosso dei 3 prigionieri

- Il paradosso dei 3 prigionieri, come proposto da Martin Gardner, è il seguente:
  - "*Ci sono* 3 *condannati a morte A, B, C, chiusi in* 3 *celle separate. Il re ha deciso di graziarne uno, che ha scelto a caso. Il carceriere sa chi dei* 3 *sarà graziato ma non può rivelarne il nome. A parla con il carceriere e lo implora di dirgli chi, tra B o C, sarà giustiziato. Gli dice: "Se B sarà graziato allora dammi il nome di C, se invece sarà C ad essere graziato dammi il nome di B. Se invece dovessi essere io ad essere graziato, allora scegline uno a caso tra B e C.*"
  - "*Il carceriere dice ad A che B sarà giustiziato. A è contento perché ritiene che a questo punto la probabilità di essere graziato sia cambiata da* $1/3$ *a* $1/2$ *perché adesso è tra lui e C. Durante l'ora d'aria dei prigionieri, dà la notizia in segreto a C. C è molto contento perché pensa che la probabilità di A di essere graziato sia rimasta* $1/3$ *mentre la sua probabilità di essere graziato sia adesso* $2/.3$. "
- Quale dei due prigionieri ha ragione? O hanno torto entrambi?

Paradosso dei 3 prigionieri: Soluzione

- Prima della risposta del carceriere, A sa che la sua probabilità di essere graziato è semplicemente $P(A) = \frac{1}{3}$ che è la stessa probabilità che hanno gli altri 2 prigionieri.
- Quali sono gli scenari che portano il carceriere a dire che B sarà giustiziato?
  - Scenario 1: sicuramente se C è graziato (la qual cosa sappiamo ha probabilità $\frac{1}{3}$). Quindi scenario 1 ha probabilità globale $\frac{1}{3}$
  - Scenario 2: con probabilità $\frac{1}{2}$ se è A ad essere graziato (la cui probabilità $\frac{1}{3}$). Quindi scenario 2 ha probabilità globale $\frac{1}{6}$
  - E notiamo che la probabilità che il carceriere dica ad A che B sarà giustiziato è la somma delle 2 probabilità sopra, quindi $\frac{1}{2}$
- Ne concludiamo che una volta accertato che B sarà giustiziato, la probabilità che C sia graziato è il doppio della probabilità che A sia graziato.
- Quindi, $P(A) = \frac{1}{3}$ e $P(C) = \frac{2}{3}$.

Paradosso dei 3 prigionieri: Soluzione

- Possiamo anche dimostrare quanto detto utilizzando la regola di Bayes. Se indichiamo con b, c rispettivamente gli eventi "carceriere dice ad A che B/C sarà giustiziato", calcoliamo $P(A|b)$.
- La regola di Bayes ci dice che

$$P(A|b) = \frac{P(b|A) \cdot P(A)}{P(b)} = \frac{\frac{1}{2} \cdot \frac{1}{3}}{\frac{1}{2}} = \frac{1}{3}$$

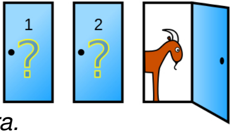
- quindi la probabilità che A sia graziato non è cambiata, e quindi, dal momento che B sarà giustiziato, la probabilità che C sia graziato è diventata $\frac{2}{3}$.

Paradosso Monty Hall

- Il paradosso Monty Hall è matematicamente equivalente al paradosso dei 3 prigionieri. E' diventato universalmente famoso per un gioco a premi televisivo americano e prende il nome dal suo conduttore.
- Il momento di maggiore notorietà, e dibattito, si ha comunque all'inizio degli anni '90 quanto viene posta una domanda, che riflette quanto chiesto nel gioco a premi, a Marilyn Vos Savant, una scrittrice e commentatrice che teneva una sua rubrica su una rivista americana.
- La Vos Savant era diventata famosa perché secondo il Guinness dei record mondiali, era la persona con il quoziente d'intelligenza più alto mai registrato.

Alla Vos Savant fu chiesto:
"Se in un gioco televisivo ti danno la scelta tra 3 porte.
Dietro una c'è un'automobile e dietro le altre 2 c'è una capra.
Supponi di scegliere la porta 1 e il presentatore,
che sa cosa c'è dietro le altre 2 porte, ne apre una,
per esempio la 3 che ha una capra.
Il presentatore ti chiede: "vuoi scambiare la tua porta con la 2?". Ti conviene farlo?"

Paradosso Monty Hall



La risposta della Vos Savant fu ovviamente: *Si ti conviene farlo perché la probabilità che l'automobile si trovi dietro la porta* 2 *è* $\frac{2}{3}$*, se assumiamo che il presentatore non apre una porta a caso, ma apre una porta che di sicuro contiene una capra.*

- Si generò una serie di vivaci polemiche e persino luminari di matematica furono in disaccordo.
- Ci vollero continui chiarimenti per poter accettare la risposta.
- Ma anche sfide di natura frequentista, del tipo: "Genera "300" casi in maniera casuale, ossia tali che in circa 100 casi l'automobile si trova dietro la porta 1, 100 casi dietro la porta 2 e 100 casi dietro la porta 3. Per ognuno di questi casi, tra la porta 2 e la 3 apri quella che contiene la capra. In quanti di questi 300 casi la capra non si trova dietro la porta 1?"
- Provate anche voi (piccolo esercizio di programmazione).

Paradosso Monty Hall

- Ovviamente, ribadiamo, il fattore chiave è che tra la 2 e la 3 si apre la porta che di sicuro non contiene l'automobile.
- Se, invece si aprisse a caso una tra le porte 2 e 3 allora il discorso cambierebbe.
- Infatti, in tale caso, con probabilità $\frac{1}{3}$ si sceglierebbe una porta che contiene l'automobile ed il gioco finirebbe.
- Invece, in caso di apertura di una porta che non contiene l'automobile, se indichiamo con $A1, A2, A3$ rispettivamente l'evento che l'automobile si trova dietro la porta 1, 2 o 3, e si apre a caso la porta $A3$ che non contiene l'automobile, si avrebbe

$$P(A1|\neg A3) = \frac{P(\neg A3|A1) \cdot P(A1)}{P(\neg A3)} = \frac{1 \cdot \frac{1}{3}}{\frac{2}{3}} = \frac{1}{2}$$

Domanda finale

- Se state partecipando ad un gioco televisivo dove ci sono 10 buste, una sola contiene un assegno di un milione di euro e le altre nove, niente.
- La busta che contiene l'assegno è scelta a caso.
- Voi avete la busta numero 1.
- Scambiereste la vostra busta con le altre 9 ?
- E se, chi sa dove si trova l'assegno, apre 8 delle altre 9 buste che di sicuro non contengono l'assegno, scambiereste la vostra busta con quella rimasta?

FINE TERZA PARTE

CALCOLO COMBINATORIO e PROBABILITA' DISCRETE