

Appunti di Probabilità e Statistica

Riccardo Agatea

20 marzo 2019

Indice

1	Introduzione	1
2	Concetti di Base	1
2.1	Definizioni	1
2.2	Operazioni sugli Insiemi	3
2.3	σ -algebra \mathcal{F}	5
2.4	Misura di probabilità	7
2.4.1	Misura Empirica	9
2.4.2	Ω discreto	9
2.4.3	Probabilità Uniforme	10
3	Approfondimenti sulla Probabilità	10
3.1	Principio Fondamentale del Conteggio	10
3.2	Probabilità Condizionata	12
3.3	Indipendenza	16
3.3.1	Schema di Bernoulli	18
4	Variabili Aleatorie	20

1 Introduzione

La probabilità si prefigge di studiare eventi casuali in modo matematico. Per evento casuale non si intende solo un evento prettamente aleatorio, come il lancio di un dado, ma anche un evento essenzialmente deterministico che richiederebbe, per essere previsto, lo studio di un sistema complesso, influenzato da un numero così alto di variabili, che risulta più semplice ed efficiente studiarlo come se fosse casuale. Inoltre, in alcune situazioni la probabilità può intervenire nonostante il caso sia completamente assente: uno degli esempi più importanti è l'integrazione con il metodo Monte Carlo. Considerato un integrale

$$I = \int_0^1 f(x)dx$$

difficilmente risolvibile individuando un'antiderivata di $f(x)$, dal teorema della media integrale è noto che

$$\exists \xi \in [0, 1]: \int_0^1 f(x)dx = f(\xi).$$

Per ricavare una stima di I è possibile considerare un insieme $X = \{x_1, x_2, \dots, x_n\}$ di valori casuali tale che $X \subseteq [0, 1]$. La media dei valori assunti dalla funzione in questi punti, per le leggi dei grandi numeri, tende a I per $n \rightarrow +\infty$:

$$\frac{1}{n} * \sum_{i=1}^n f(x_i) \xrightarrow{n \rightarrow +\infty} I.$$

2 Concetti di Base

2.1 Definizioni

Definizione 2.1. Sia Ω un insieme non vuoto, sia \mathcal{F} una famiglia di sottoinsiemi di Ω (cioè un insieme di sottoinsiemi di Ω), e sia

$$P : \mathcal{F} \rightarrow [0, 1]$$

una funzione tale che $P(\Omega) = 1$. Si chiama spazio di probabilità la terna ordinata

$$(\Omega, \mathcal{F}, P).$$

- Ω si chiama spazio degli eventi elementari, contiene tutti i risultati possibili di un dato esperimento. I suoi elementi si dicono eventi elementari o esiti specifici.
- \mathcal{F} ha la struttura di una σ -algebra (concetto che verrà studiato più avanti); intuitivamente contiene tutti gli eventi che si vogliono studiare in senso probabilistico.

- P si dice misura di probabilità. Se $E \in \mathcal{F}$, e quindi E è un evento, $P(E)$ è la probabilità che E si realizzi. Si intende che se $P(E) = 0$ allora E non si verifica mai, se $P(E) = 1$ allora E si verifica sempre.

NB. Per uno stesso esperimento Ω , \mathcal{F} e P non sono necessariamente unici. Generalmente si cerca di scegliere Ω in modo che sia il più ridotto possibile, per cercare di minimizzare la complessità degli eventi da studiare.

Sono dati alcuni esempi di esperimenti, e dei relativi spazi degli eventi elementari.

Esempio 2.1. Esperimento: lancio di una moneta.

$$\Omega = \{T, C\}$$

Esempio 2.2. Esperimento: 3 lanci consecutivi di una moneta.

$$\Omega = \{TTT, TTC, TCT, TCC, CTT, CTC, CCT, CCC\}$$

Esempio 2.3. Esperimento: conteggio del numero di volte in cui esce testa su 3 lanci di una moneta.

$$\Omega = \{0, 1, 2, 3\}$$

Esempio 2.4. Esperimento: conteggio del numero di lanci necessari affinché esca testa la prima volta.

$$\Omega = \{1, 2, 3, \dots\} = \mathbb{N}$$

Esempio 2.5. Esperimento: misura della durata di vita di una lampadina (supponendo che la sensibilità del sistema di misura sia essenzialmente nulla, cioè che le misure siano corrette fino all'infinitesima cifra significativa).

$$\Omega = \mathbb{R}_+ \quad \text{oppure} \quad \Omega = [0, a] \subsetneq \mathbb{R}_+$$

Nota. Introduciamo due concetti:

Definizione 2.2. Uno spazio di probabilità (Ω, \mathcal{F}, P) si dice discreto se Ω è finito o numerabile:

$$|\Omega| \leq |\mathbb{N}|$$

Definizione 2.3. Uno spazio di probabilità (Ω, \mathcal{F}, P) si dice continuo se Ω è non numerabile:

$$|\Omega| = |\mathbb{R}|$$

Definizione 2.4. Sia $\omega \in \Omega$ il risultato osservato dall'esecuzione di un dato esperimento, e sia $E \in \mathcal{F}$ un evento. Si dice che E si è verificato se e solo se

$$\omega \in E.$$

Esempio 2.6. Esperimento: 3 lanci consecutivi di una moneta. Consideriamo:

$$\begin{aligned}\Omega &= \{TTT, TTC, TCT, TCC, CTT, CTC, CCT, CCC\} \\ E &= \{\omega \in \Omega \mid \text{testa e croce si alternano}\}\end{aligned}$$

Dall'esecuzione dell'esperimento, si osserva $\omega = TTC$.

$$\omega \notin E \Rightarrow E \text{ non si è verificato}$$

Ripetendo l'esperimento si osserva $\omega = TCT$.

$$\omega \in E \Rightarrow E \text{ si è verificato}$$

Due particolari eventi sempre presenti in \mathcal{F} sono:

- \emptyset rappresenta il non presentarsi di alcuno degli eventi elementari in Ω . Chiaramente almeno uno degli eventi elementari si deve presentare, quindi \emptyset non si verifica mai.
- Ω rappresenta il presentarsi di uno degli eventi elementari, senza limitazioni, e quindi si verifica sempre.

2.2 Operazioni sugli Insiemi

Consideriamo uno spazio di probabilità (Ω, \mathcal{F}, P) , e due eventi $E, F \in \mathcal{F}$. Essendo \mathcal{F} una famiglia di sottoinsiemi di Ω , E e F sono insiemi, e quindi si possono applicare ad essi le comuni operazioni sugli insiemi. Quelli che si ottengono sono ancora eventi di \mathcal{F} , di cui si può studiare il verificarsi in funzione del verificarsi di E e F .

- $E \cap F$ si verifica \Leftrightarrow sia E che F si verificano
- $E \cup F$ si verifica \Leftrightarrow almeno uno fra E e F si verifica
- E^C si verifica $\Leftrightarrow E$ non si verifica
- $E \setminus F$ si verifica $\Leftrightarrow E$ si verifica e F non si verifica
- $E \Delta F$ si verifica \Leftrightarrow solo uno fra E ed F si verifica

Definizione 2.5. E ed F si dicono incompatibili se sono disgiunti:

$$E \cap F = \emptyset$$

Chiaramente, per gli elementi di \mathcal{F} continuano a valere la proprietà distributiva dell'intersezione sull'unione e dell'unione sull'intersezione, e le due leggi di De Morgan. Usando le leggi di De Morgan, è sempre possibile esprimere un'espressione in funzione del complemento e di una fra unione e intersezione.

Partizioni Ricordiamo la definizione di partizione di un insieme:

Definizione 2.6. Sia A un insieme, sia $(A_i)_i$ una famiglia di suoi sottoinsiemi. $(A_i)_i$ si dice partizione di A se e solo se

$$\bigcup_i A_i = A$$

$$A_i \cap A_j = \emptyset \quad \forall i \neq j.$$

Se l'insieme considerato è uno spazio degli eventi Ω , allora una sua partizione rappresenta una famiglia di eventi incompatibili, ma per i quali c'è la garanzia che uno e uno solo di essi si verifichi. Dato un evento $F \subseteq \Omega$ e una partizione $(E_i)_i$ di Ω , è sempre possibile *scomporre* F rispetto $(E_i)_i$, cioè si può sempre rappresentare F come l'unione delle intersezioni di F con gli insiemi di $(E_i)_i$:

$$F = \bigcup_i (F \cap E_i).$$

Chiaramente, siccome $(E_i)_i$ è una partizione di Ω , $(F \cap E_i)_i$ è una partizione di F . In modo simile, è sempre possibile scomporre l'unione di due eventi in una sua partizione: se $E, F \subseteq \Omega$ allora

$$E \cup F = (E \cap F^C) \cup (E^C \cap F) \cup (E \cap F).$$

Concettualmente, significa che "o si verifica solo E , o si verifica solo F , oppure si verificano entrambi". Un'altra scomposizione, più generalizzabile è:

$$E \cup F = E \cup (F \setminus E).$$

In questo caso, il significato è "o si verifica E , e non ci interessiamo di F , oppure se E non si verifica, allora si verifica F ". Questa scomposizione si può generalizzare alla generica famiglia di eventi $\{E_n\}_n$:

$$\bigcup_n E_n = E_1 \cup \left(\bigcup_{k \neq 1} E_k \setminus \left(\bigcup_{i=1}^{k-1} E_i \right) \right)$$

Esercizio 2.1. Dati tre eventi E, F, G , trovare l'evento corrispondente a

- si verifica solo E
- si verificano E e F , ma non G
- si verifica esattamente uno degli eventi E, F , o G
- si verifica almeno uno dei tre
- si verificano esattamente due degli eventi

2.3 σ -algebra \mathcal{F}

Abbiamo detto che \mathcal{F} è una famiglia di sottoinsiemi di Ω che contiene tutti gli eventi che ci interessa analizzare. Diamo una definizione formale di evento:

Definizione 2.7. Un sottoinsieme E di Ω si dice evento se e solo se $E \in \mathcal{F}$.

Il fatto che \mathcal{F} contenga gli eventi che ci interessano ha delle conseguenze, nello specifico significa che se un evento è presente devono essere presenti anche tutti gli eventi "equivalenti". Ad esempio, se l'evento "è uscita sempre testa" è presente, anche "non è uscita mai croce" deve essere presente, perchè danno la stessa informazione. Per questo \mathcal{F} è una σ -algebra:

Definizione 2.8. Dato un insieme A e una famiglia di suoi sottoinsiemi \mathcal{A} , \mathcal{A} è una σ -algebra se e solo se:

1. $\mathcal{A} \neq \emptyset$
2. $\forall B \subseteq \Omega \quad B \in \mathcal{A} \Rightarrow B^C \in \mathcal{A}$
3. Presa comunque una famiglia numerabile $(B_n)_n$ di sottoinsiemi di A , vale

$$\forall n \quad B_n \in \mathcal{A} \Rightarrow \bigcup_i B_i \in \mathcal{A}$$

Bastano queste condizioni perchè, come abbiamo detto, tutte le operazioni fra insiemi possono essere ridotte a combinazioni di complemento e unione. Due esempi particolarmente importanti di σ -algebra su un dato spazio degli eventi elementari Ω sono:

Esempio 2.7.

$$\mathcal{F} = \{\emptyset, \Omega\}$$

Questa è una σ -algebra perchè:

1. Chiaramente non è vuota
2. $\emptyset^C = \Omega \in \mathcal{F}$ e $\Omega^C = \emptyset \in \mathcal{F}$
3. $\emptyset \cup \Omega = \Omega \in \mathcal{F}$

Esempio 2.8.

$$\mathcal{F} = \mathbb{P}(\Omega)$$

Con $\mathbb{P}(\Omega)$ indichiamo l'insieme delle parti di Ω . La dimostrazione è triviale.

Definizione 2.9. Sia $E \subseteq \Omega$, la σ -algebra generata da E è

$$\mathcal{F} = \{\emptyset, \Omega, E, E^C\}$$

Si dimostra che è una σ -algebra:

Dimostrazione. 1. Trivialmente, $\mathcal{F} \neq \emptyset$

2.

$$\begin{aligned}\emptyset^C &= \Omega \in \mathcal{F} \\ \Omega^C &= \emptyset \in \mathcal{F} \\ E^C &\in \mathcal{F} \\ (E^C)^C &= E \in \mathcal{F}\end{aligned}$$

3. Per dimostrare che \mathcal{F} è chiusa rispetto l'unione non è necessario considerare le unioni con Ω , perchè $\Omega \cup x = \Omega \ \forall x$. Non è necessario considerare neanche \emptyset , perchè esso è l'elemento neutro dell'unione, e quindi $\emptyset \cup x \in \mathcal{F} \Leftrightarrow x \in \mathcal{F} \ \forall x$. Resta da dimostrare che $E \cup E^C \in \mathcal{F}$, che è triviale in quanto $E \cup E^C = \Omega$.

CVD

Le proprietà di una σ -algebra sono:

- $\emptyset, \Omega \in \mathcal{F} \quad \forall \mathcal{F}$

Dimostrazione.

$$\begin{aligned}\mathcal{F} &\neq \emptyset \\ \Rightarrow \exists G \in \mathcal{F} \\ \Rightarrow G^C &\in \mathcal{F} \\ \Rightarrow G \cup G^C &\in \mathcal{F} \\ \Rightarrow \Omega &\in \mathcal{F} \\ \Rightarrow \Omega^C &= \emptyset \in \mathcal{F}\end{aligned}$$

CVD

- \mathcal{F} è chiusa rispetto le unioni finite

Dimostrazione. Sia $\{E_1, \dots, E_n\} \subseteq \mathcal{F}$ una famiglia finita di sottoinsiemi di Ω . Questa può essere estesa definendo $E_i = \emptyset \ \forall i > n$; segue:

$$\bigcup_{i=1}^n B_i \in \mathcal{F} = \bigcup_{i \in \mathbb{N}} B_i \in \mathcal{F} \quad \text{CVD}$$

- \mathcal{F} è chiusa rispetto le intersezioni

Dimostrazione. Sia $(E_n)_n \subseteq \mathcal{F}$ una famiglia numerabile di sottoinsiemi di Ω .

$$\begin{aligned}
& \forall i \ E_i \in \mathcal{F} \\
& \Rightarrow \forall i \ E_i^C \in \mathcal{F} \\
& \Rightarrow \bigcup_i E_i^C \in \mathcal{F} \\
& \Rightarrow \left(\bigcup_i E_i^C\right)^C \in \mathcal{F} \\
& \Rightarrow \bigcap_i E_i \in \mathcal{F} \qquad \text{CVD}
\end{aligned}$$

Proposizione 2.1. Se Ω è discreto, allora si può sempre prendere $\mathcal{F} = \mathbb{P}(\Omega)$, ed è quello che si fa di solito.

2.4 Misura di probabilità

Diamo una definizione di misura di probabilità:

Definizione 2.10. Una funzione

$$P: \mathcal{F} \rightarrow [0, 1]$$

si dice misura di probabilità se

1. $P(\Omega) = 1$
2. P è σ -additiva, cioè: sia $(E_i)_i \subseteq \mathcal{F}$ una famiglia numerabile di eventi mutualmente incompatibili, allora

$$P\left(\bigcup_i E_i\right) = \sum_i P(E_i)$$

Le proprietà di P sono:

- $\forall E \in \mathcal{F} \quad P(E^C) = 1 - P(E)$

Dimostrazione.

$$\begin{aligned}
& E \cup E^C = \Omega \\
& \Rightarrow P(E \cup E^C) = P(\Omega) \\
& \Rightarrow P(E) + P(E^C) = 1 \\
& \Rightarrow P(E^C) = 1 - P(E) \qquad \text{CVD}
\end{aligned}$$

- $\forall E, F \in \mathcal{F} \quad E \subseteq F \Rightarrow P(E) \leq P(F)$

Dimostrazione.

$$\begin{aligned} F &= (F \cap E) \cup (F \cap E^C) \\ &= E \cup (F \cap E^C) \\ \Rightarrow P(F) &= P(E) + P(F \cap E^C) \end{aligned}$$

Essendo $P(F \cap E^C) \geq 0$, segue la tesi.

CVD

- $\forall E, F \in \mathcal{F} \quad P(E \cup F) = P(E) + P(F) - P(E \cap F)$

Dimostrazione. Per definizione di misura di probabilità, P è additiva su unioni disgiunte, quindi:

$$\begin{aligned} E \cup F &= E \cup (F \setminus E) \\ \Rightarrow P(E \cup F) &= P(E) + P(F \setminus E) \end{aligned}$$

Ricordiamo che, per definizione:

$$F \setminus E = F \cap E^C$$

Inoltre:

$$F = (F \cap E) \cup (F \cap E^C)$$

Sostituendo:

$$F \setminus E = F \cap E^C$$

(ecc)

CVD

- La precedente si può generalizzare a una famiglia $\{E_n\}_n$ di eventi non necessariamente disgiunti:

$$P\left(\bigcup_n E_n\right) \leq \sum_n P(E_n)$$

Dimostrazione. (ecc)

CVD

- $P(E \cup F \cup G) = P(E) + P(F) + P(G) - P(E \cap F) - P(E \cap G) - P(F \cap G) + P(E \cap F \cap G)$

Dimostrazione. (per casa)

CVD

- $P(E \Delta F) = P(E) + P(F) - 2P(E \cap F)$

Chiaramente, P non è determinata univocamente da Ω e \mathcal{F} , però ci sono dei metodi "standard" per costruirla, soprattutto nelle applicazioni pratiche.

2.4.1 Misura Empirica

Consideriamo una coppia (Ω, \mathcal{F}) fissata in modo da rappresentare un esperimento ripetibile. Eseguendo l'esperimento n volte si otterrà una sequenza di n risultati

$$(\omega_1, \dots, \omega_n) \quad \omega_i \in \Omega \quad \forall i \in \{1, \dots, n\}$$

Sia $E \in \mathcal{F}$, definiamo una quantità n_E che rappresenti il numero di volte in cui E si è verificato

$$n_E := |\{i \in \{1, \dots, n\} : \omega_i \in E\}|$$

Definizione 2.11. Si dice misura di probabilità empirica la funzione

$$\begin{aligned} \hat{P}_n : \mathcal{F} &\rightarrow [0, 1] \\ E &\mapsto \frac{n_E}{n} \end{aligned}$$

Questa misura in modo empirico il numero di volte in cui un dato evento si è verificato. Il limite più importante è che l'esperimento deve essere ripetibile.

2.4.2 Ω discreto

Nel caso in cui Ω sia discreto e $\mathcal{F} = \mathbb{P}(\Omega)$, si può dimostrare che per identificare univocamente P è sufficiente identificare i valori p_ω tali che

$$p_\omega = P(\{\omega\}) \quad \text{con} \quad \sum_{\omega \in \Omega} p_\omega = 1$$

Segue dalla σ -additività di P che:

$$P(E) = \sum_{\omega \in E} p_\omega \quad \forall E \in \mathcal{F}$$

Si ricava che se Ω è finito

$$\Omega = \{\omega_1, \dots, \omega_n\}$$

identificare P equivale ad identificare una famiglia

$$\{p_1, \dots, p_n\}$$

tale che

$$\sum_{i=1}^n p_i = 1$$

Osservazione 2.1. In realtà sono sufficienti $n - 1$ valori p_i , perchè vale necessariamente:

$$p_n = 1 - \sum_{i=1}^{n-1} p_i$$

Se invece Ω è numerabile, identificare P equivale ad identificare una successione $(p_n)_n$ tale che

$$\sum_{i=1}^{+\infty} p_i = 1$$

2.4.3 Probabilità Uniforme

Un caso particolare del punto precedente si ha se Ω è finito e tutti gli eventi elementari hanno la stessa probabilità:

Definizione 2.12. Sia Ω spazio di probabilità finito, la funzione di probabilità uniforme è la misura di probabilità identificata dalla famiglia di valori p_i tali che:

$$p_i = \frac{1}{n} \quad \forall i \in \{1, \dots, n\}$$

In questo caso, vale che dato un evento $E \in \mathcal{F}$:

$$\begin{aligned} P(E) &= \sum_{\omega \in E} P(\{\omega\}) \\ &= \sum_{\omega \in E} p_\omega \\ &= \sum_{\omega \in E} \frac{1}{n} \\ &= \frac{1}{n} * \sum_{\omega \in E} 1 \\ &= \frac{1}{n} * |E| \\ &= \frac{|E|}{|\Omega|} \end{aligned}$$

In altre parole, la probabilità di un evento E è pari al numero di risultati favorevoli ad E diviso per il numero totale di risultati.

3 Approfondimenti sulla Probabilità

3.1 Principio Fondamentale del Conteggio

Principio (Fondamentale del Conteggio). *Dovendo eseguire R scelte consecutive tali che*

1. $\forall r \in \{1, \dots, R\}$ la scelta va eseguita fra n_r elementi
2. $\forall r \in \{1, \dots, R\}$ la scelta non dipende dalle precedenti
3. da due successioni distinte di R scelte si giunge a risultati diversi

Il numero totale di risultati possibili è

$$\prod_{i=1}^R n_i$$

In generale, i problemi in cui interviene il principio fondamentale del conteggio riguardano il campionamento, secondo uno schema riconducibile all'estrazione di k palline da un'urna che ne contiene n . Ci sono due possibilità riguardo le palline, ed altrettante riguardo l'estrazione:

- Per quanto riguarda le palline, possono essere:
 - tutte diverse (e quindi, virtualmente numerabili da 1 a n)
 - diverse a gruppi (con $m < n$ gruppi)
- Per quanto riguarda l'estrazione, può essere:
 - con reinserimento (con la possibilità di estrarre $k \in \mathbb{N}$ palline)
 - senza reinserimento (limitando il numero di estrazioni a $k \leq n$)

Inoltre è possibile distinguere fra due possibilità sugli aspetti interessanti delle palline estratte:

- ci interessa la disposizione delle palline estratte (cioè ci interessa quali palline sono estratte e in quale ordine)
- ci interessa la combinazione delle palline estratte (cioè ci interessa solo quali palline sono estratte, ma non in quale ordine, e quindi ci interessa quante palline di ciascun tipo sono state estratte)

I problemi si possono quindi analizzare in base alle loro caratteristiche attraverso il calcolo combinatorio.

Disposizione con reinserimento In questo caso, assumendo che le palline siano tutte diverse, ad ogni estrazione ci sono n possibilità diverse di estrarre la pallina, e quindi le possibili disposizioni sono:

$$\underbrace{n \cdot n \cdot \dots \cdot n}_{k \text{ volte}} = n^k$$

Disposizione senza reinserimento Problema molto simile al precedente, con la differenza che le palline non vengono reinserite nell'urna. Ad ogni estrazione il numero di palline che è possibile estrarre diminuisce di 1. Le possibili disposizioni sono:

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

Un caso particolare si ha quando $k = n$, cioè se vengono estratte tutte le palline dall'urna. In questo caso, le disposizioni sono:

$$\frac{n!}{(n-k)!} = \frac{n!}{(n-n)!} = \frac{n!}{0!} = n!$$

Queste si dicono permutazioni, in quanto sono modi diversi di disporre gli stessi elementi.

Combinazioni senza reinserimento Anche in questo caso ad ogni estrazione il numero di palline che è possibile estrarre diminuisce di 1; inoltre, data una sequenza di palline estratte, questa è equivalente a tutte le sue permutazioni. Il numero di combinazioni si può quindi ottenere dividendo il numero di disposizioni ottenibili in questa situazione per il numero di permutazioni possibili della sequenza estratta:

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

Per convenzione si pone:

$$\binom{0}{0} = \binom{n}{0} = \binom{n}{n} = 1$$

Un'applicazione importante del coefficiente binomiale è la formula del binomio di Newton:

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

Alcune proprietà sono:

$$\begin{aligned} 2^n &= \sum_{k=0}^n \binom{n}{k} \\ \binom{n}{k} &= \binom{n}{n-k} \\ \binom{n}{k} &= \binom{n-1}{k} + \binom{n-1}{k-1} \end{aligned}$$

Permutazioni con palline uguali Nel caso i colori siano $m < n$, e ci siano n_i palline dell' i -esimo colore, il numero di modi di estrarle tutte si può ottenere dividendo il numero di modi di estrarre tutte le palline se fossero tutte diverse per il numero di modi di scambiare fra di loro le palline uguali:

$$\frac{n!}{n_1! \cdot n_2! \cdot \dots \cdot n_m!}$$

Questo caso corrisponde al trovare il numero di anagrammi di una parola con lettere ripetute.

3.2 Probabilità Condizionata

Finora abbiamo visto situazioni in cui la probabilità di un dato evento E dipende esclusivamente da E , cioè in cui la misura di quanto verosimile sia E è basata solo sulle caratteristiche "di partenza" dello spazio di probabilità. In alcuni casi, è utile valutare come varia la probabilità di E se sono fornite informazioni aggiuntive; l'obiettivo è formalizzare il concetto molto intuitivo che, ad esempio,

la probabilità che piova quando è sereno è diversa dalla probabilità che piova quando è nuvoloso. In particolare, l'informazione relativa al clima deve avere un effetto sulla probabilità che piova. Questo viene formalizzato introducendo la misura di probabilità condizionata:

Definizione 3.1. Sia (Ω, \mathcal{F}, P) uno spazio di probabilità, sia $F \in \mathcal{F}$ tale che $P(F) > 0$; si definisce misura di probabilità condizionata a F la funzione

$$\begin{aligned} P(\cdot|F) : \mathcal{F} &\rightarrow [0, 1] \\ E &\mapsto P(E|F) \end{aligned}$$

dove:

$$P(E|F) = \frac{P(E \cap F)}{P(F)} \quad \forall E \in \mathcal{F}$$

La probabilità $P(E|F)$ misura la probabilità che se si verifica F , si verifichi anche E . Si dimostra che la misura di probabilità condizionata $P(\cdot|F)$ è effettivamente una misura di probabilità:

Dimostrazione. 1.

$$\begin{aligned} P(\Omega|F) &= \frac{P(\Omega \cap F)}{P(F)} \\ &= \frac{P(F)}{P(F)} = 1 \end{aligned}$$

2. Considerando una famiglia $\{E_n\}_n$ di sottoinsiemi di Ω :

$$\begin{aligned} P\left(\bigcup_n E_n \middle| F\right) &= \frac{P((\bigcup_n E_n) \cap F)}{P(F)} \\ &= \frac{P(\bigcup_n (E_n \cap F))}{P(F)} \\ &= \sum_n \frac{P(E_n \cap F)}{P(F)} \end{aligned}$$

CVD

Nota. Chiaramente, ha senso considerare la probabilità di E condizionata a F solo se $P(F) > 0$.

Alcune proprietà:

- $P(E^C|F) = 1 - P(E|F) \quad \forall E \in \mathcal{F}$
- $E \cap F = \emptyset \Rightarrow P(E|F) = 0$

- $F \subseteq E \Rightarrow P(E|F) = 1$
- $P(E) = 0 \Rightarrow P(E|F) = 0$
- $P(E) = 1 \Rightarrow P(E|F) = 1$
- *Formula di moltiplicazione:* sia $\{E_n\}_n$ una famiglia di eventi non necessariamente disgiunti, allora vale

$$\begin{aligned} P\left(\bigcap_{i=1}^n E_i\right) &= P\left(E_n \mid \bigcap_{i=1}^{n-1} E_i\right) \cdot \dots \cdot P(E_1) \\ &= \prod_{k=2}^n P\left(E_k \mid \bigcap_{i=1}^{k-1} E_i\right) \cdot P(E_1) \end{aligned}$$

- Dalla precedente, per $n = 2$, si ricava

$$P(E \cap F) = P(E|F) \cdot P(F)$$

Nota. Nel contesto della probabilità condizionata, $P(E)$ si dice anche probabilità a priori di E , mentre $P(E|F)$ è detta, per contrasto, probabilità a posteriori.

Vediamo adesso alcune formule legate alla probabilità condizionata.

Formula di Probabilità Totale Partendo dalla formula di moltiplicazione:

$$\begin{aligned} P(E \cap F) &= P(E|F) \cdot P(F) \\ P(E \cap F^C) &= P(E|F^C) \cdot P(F^C) \end{aligned}$$

$E \cap F$ e $E \cap F^C$ sono eventi disgiunti, e vale $(E \cap F) \cup (E \cap F^C) = E$. Segue:

$$\begin{aligned} P(E) &= P(E \cap F) + P(E \cap F^C) \\ &= P(E|F)P(F) + P(E|F^C)P(F^C) \end{aligned}$$

Questa formula si può generalizzare: consideriamo una partizione $\{F_n\}_n$ di Ω , cioè una famiglia di sottoinsiemi di Ω tale che

$$\begin{aligned} \bigcup_i F_i &= \Omega \\ F_i \cap F_j &= \emptyset \quad \forall i \neq j \end{aligned}$$

Inoltre, imponiamo che

$$P(F_i) > 0 \quad \forall i$$

Allora, dato un evento $E \in \mathcal{F}$ si può scrivere:

$$P(E) = \sum_{i=1}^n P(E|F_i) \cdot P(F_i)$$

Dimostrazione. Essendo $\{F_n\}_n$ una partizione di Ω , vale:

$$\begin{aligned} E &= \bigcup_{i=1}^n (E \cap F_i) \\ \Rightarrow P(E) &= P\left(\bigcup_{i=1}^n (E \cap F_i)\right) \\ &= \sum_{i=1}^n P(E \cap F_i) \\ &= \sum_{i=1}^n \frac{P(E \cap F_i)}{P(F_i)} P(F_i) \\ &= \sum_{i=1}^n P(E|F_i) P(F_i) \end{aligned} \quad \text{CVD}$$

Formula di Bayes La formula di Bayes segue da un'interpretazione della formula di probabilità totale: ciascuno degli eventi F_i si può interpretare come una possibile causa di E . Ciascuno degli addendi $P(E|F_i)P(F_i)$ rappresenta la probabilità che E si verifichi dopo che si è verificato F_i . Ci chiediamo ora quale sia la probabilità che, avendo osservato che E si verifica, si sia verificato F_i . Applicando le formule di moltiplicazione e di probabilità totale, considerando uno specifico evento F_k della partizione, segue:

$$\begin{aligned} P(F_k|E) &= \frac{P(F_k \cap E)}{P(E)} \\ &= \frac{P(E|F_k)P(F_k)}{\sum_{i=1}^n P(E|F_i)P(F_i)} \end{aligned}$$

Esempio 3.1. Un'applicazione della formula di Bayes si ha in molti casi in cui si cerca di studiare un dato fenomeno non direttamente osservabile, e che quindi porta alla necessità di effettuare un test indiretto per valutare il presentarsi o meno del fenomeno. In modo semplificato, possiamo considerare che per l'evento ha $\{D, d\}$ come possibili outcome, rappresentanti rispettivamente il verificarsi o meno dell'evento, e il test ha $\{T, t\}$ come possibili risultati, che rappresentano rispettivamente il rilevare il verificarsi o il non verificarsi del fenomeno. Gli outcome dell'esperimento sono quindi:

- TD se il test ha correttamente rilevato il verificarsi dell'esperimento
- td se il test ha correttamente rilevato il non verificarsi dell'esperimento

- Td se il test ha rilevato un falso positivo, detto anche errore di prima specie
- tD se il test ha rilevato un falso negativo, detto anche errore di seconda specie

Due probabilità che caratterizzano l'esperimento sono:

- $P(T|D)$, detta sensibilità
- $P(t|d)$, detta specificità

In particolare, date queste probabilità, è possibile ricavare quanto probabile sia che il fenomeno si sia verificato dopo aver ricevuto un risultato positivo al test:

$$P(D|T) = \frac{P(T|D)P(D)}{P(T|D)P(D) + P(T|d)P(d)}$$

3.3 Indipendenza

Definizione 3.2. Dati due eventi $E, F \in \mathcal{F}$, E e F si dicono indipendenti, e si indica

$$E \perp\!\!\!\perp F$$

se e solo se

$$P(E \cap F) = P(E)P(F)$$

Il concetto di eventi indipendenti formalizza l'idea che se due eventi sono completamente slegati, allora la probabilità che uno si verifichi non ha nessuna influenza sulla probabilità che si verifichi anche l'altro. Alcune proprietà:

- $E \perp\!\!\!\perp \emptyset$
- $E \perp\!\!\!\perp \Omega$
- $E \perp\!\!\!\perp E \Leftrightarrow E = \Omega \vee E = \emptyset$
- Se $P(E) > 0$ e $P(F) > 0$, allora vale

$$E \perp\!\!\!\perp F \Leftrightarrow P(E|F) = P(E) \Leftrightarrow P(F|E) = P(F)$$

- $E \perp\!\!\!\perp F \Leftrightarrow E^C \perp\!\!\!\perp F \Leftrightarrow E \perp\!\!\!\perp F^C \Leftrightarrow E^C \perp\!\!\!\perp F^C$

Per tre eventi, la definizione di indipendenza è lievemente più complessa:

Definizione 3.3. Dati tre eventi $E, F, G \in \mathcal{F}$, questi si dicono indipendenti se e solo se

1.

$$E \perp\!\!\!\perp F \wedge E \perp\!\!\!\perp G \wedge F \perp\!\!\!\perp G$$

2.

$$P(E \cap F \cap G) = P(E)P(F)P(G)$$

NB. Le due condizioni sono slegate: ci sono casi in cui gli eventi sono indipendenti a due a due, ma la loro intersezione non ha probabilità pari al prodotto delle singole probabilità, o viceversa la probabilità dell'intersezione coincide con il prodotto delle probabilità, ma gli eventi non sono indipendenti a due a due.

Il concetto di indipendenza si estende a più eventi:

Definizione 3.4. Data una famiglia finita di eventi $\{E_n\}_n \subseteq \mathcal{F}$, si dice famiglia di eventi indipendenti se e solo se $\forall r \in \{2, 3, \dots, n\}$ ogni sottofamiglia di $\{E_n\}_n$ composta da r eventi è indipendente.

Le due condizioni continuano ad essere slegate. Si nota che il numero di casi da considerare aumenta quadraticamente al crescere del numero di eventi.

Definizione 3.5. Data una famiglia numerabile di eventi $\{E_n\}_n \subseteq \mathcal{F}$, si dice famiglia di eventi indipendenti se $\forall \{F_k\}_k \subseteq \{E_n\}_n$ con $\{F_k\}_k$ famiglia finita, $\{F_k\}_k$ è famiglia di eventi indipendenti.

Osservazione 3.1. Se $\{A_n\}_n$ è una famiglia di eventi indipendenti (non importa quanti), allora anche la famiglia formata sostituendo alcuni (non necessariamente tutti) eventi con i rispettivi complementari è indipendente.

Esercizio 3.1. Dimostrare che se $\{A, B\}$ sono indipendenti, anche $\{A^C, B^C\}$ sono indipendenti

Soluzione.

$$P(A^C \cap B^C) = P((A \cup B)^C)$$



Esercizio 3.2. A tre studenti viene posta la stessa domanda. Sappiamo che il primo risponde correttamente con probabilità $\frac{1}{2}$, il secondo con probabilità $\frac{2}{3}$, il terzo con probabilità $\frac{1}{3}$. Gli studenti non possono comunicare fra loro. Vogliamo calcolare la probabilità che, se un solo studente ha risposto correttamente, sia stato il secondo.

Soluzione. Consideriamo gli eventi relativi ai possibili outcome di cui ci può interessare:

S_i = "l' i -esimo studente ha risposto correttamente"

E_i = "ci sono state i risposte esatte"

Siccome è noto che solo uno studente ha risposto correttamente, la probabilità da calcolare è la probabilità di S_2 condizionato a E_1 :

$$P(S_2|E_1) = \frac{P(S_2 \cap E_1)}{P(E_1)}$$

Concettualmente, possiamo riscrivere $S_2 \cap E_1$ ed E_1 come unioni ed intersezioni di eventi più semplici:

$$P(S_2|E_1) = \frac{P(S_2 \cap E_1)}{P(E_1)} = \frac{P(S_1^C \cap S_2 \cap S_3^C)}{P((S_1 \cap S_2^C \cap S_3^C) \cup (S_1^C \cap S_2 \cap S_3^C) \cup (S_1^C \cap S_2^C \cap S_3))}$$

Siccome gli eventi parte dell'unione sono disgiunti, la probabilità si può distribuire:

$$P(S_2|E_1) = \frac{P(S_2 \cap E_1)}{P(E_1)} = \frac{P(S_1^C \cap S_2 \cap S_3^C)}{P(S_1 \cap S_2^C \cap S_3^C) + P(S_1^C \cap S_2 \cap S_3^C) + P(S_1^C \cap S_2^C \cap S_3)}$$

Siccome gli studenti non possono comunicare, la risposta di ciascuno non influenza la risposta degli altri, e quindi possiamo assumere che i tre eventi siano indipendenti:

$$\begin{aligned} & \frac{P(S_1^C \cap S_2 \cap S_3^C)}{P(S_1 \cap S_2^C \cap S_3^C) + P(S_1^C \cap S_2 \cap S_3^C) + P(S_1^C \cap S_2^C \cap S_3)} \\ &= \frac{P(S_1^C)P(S_2)P(S_3^C)}{P(S_1)P(S_2^C)P(S_3^C) + P(S_1^C)P(S_2)P(S_3^C) + P(S_1^C)P(S_2^C)P(S_3)} \\ &= \frac{P(\frac{1}{2})P(\frac{2}{3})P(\frac{2}{3})}{P(\frac{1}{2})P(\frac{1}{3})P(\frac{2}{3}) + P(\frac{1}{2})P(\frac{2}{3})P(\frac{2}{3}) + P(\frac{1}{2})P(\frac{1}{3})P(S_3)} \quad 0.57 \end{aligned}$$

3.3.1 Schema di Bernoulli

Detto anche *Modello Binomiale per Eventi*. Consideriamo un esperimento con queste caratteristiche:

- Vengano eseguite n prove identiche, effettuate in sequenza
- Ciascuna prova ha solo due possibili risultati, che generalmente si indicano con $\{0, 1\}$
- Il risultato di ciascuna prova non influenza il risultato di nessuna delle altre

L'esperimento si può descrivere con un modello di probabilità dato da $\Omega = \{0, 1\}^n$, $\mathcal{F} = \mathbb{P}(\Omega)$, e da una misura di probabilità P che rispetti le condizioni:

- Gli eventi

$$B_j = \{(b_1, \dots, b_n) | b_j = 1\}$$

sono equiprobabili, cioè

$$P(B_j) = p \quad \forall j \in \{1, \dots, n\} \text{ con } p \in [0, 1]$$

- La famiglia

$$\{B_1, \dots, B_n\}$$

è una famiglia di eventi indipendenti.

Esempio 3.2. Consideriamo un sistema di comunicazione formato da n componenti, ciascuno dei quali ha probabilità p di funzionare. Nella sua totalità, il sistema funziona se almeno metà delle componenti funzionano. Ci chiediamo per quali valori di p un sistema a tre componenti ha maggiore probabilità di funzionare rispetto a un sistema formato da un solo componente.

Soluzione. L'idea è di rappresentare il problema attraverso lo schema di Bernoulli. Identifichiamo:

- una prova con il test di un componente
- il numero di prove ripetute con il numero di componenti
- gli esiti $\{0, 1\}$ con $\{\text{"funziona"}, \text{"non funziona"}\}$ come

$$\begin{aligned}\text{"funziona"} &\mapsto 1 \\ \text{"non funziona"} &\mapsto 0\end{aligned}$$

- la probabilità di successo con $P(B_j) = p$

Per il sistema a 3 componenti vale:

$$\begin{aligned}P(\text{"sistema funziona"}) &= P(\text{"almeno due componenti su tre funzionano"}) \\ &= P(\{\text{"esattamente 2 componenti funzionano"}\} \cup \{\text{"esattamente 3 componenti funzionano"}\}) \\ &= P(\{\text{"2 componenti su 3 funzionano"}\}) + P(\{\text{"tutti e 3 i componenti funzionano"}\}) \\ &= P\left(\bigcup_{I \subset \{1,2,3\} \wedge |I|=2} \{(b_1, b_2, b_3) \in \{0,1\}^3 \mid b_j = 1 \Leftrightarrow j \in I\}\right) + P(\{(1, 1, 1)\})\end{aligned}$$

essendo gli eventi nell'unione disgiunti:

$$\begin{aligned}&= \sum_{I \subset \{1,2,3\} \wedge |I|=2} P(\{(b_1, b_2, b_3) \in \{0,1\}^3 \mid b_j = 1 \Leftrightarrow j \in I\}) + P(\{(1, 1, 1)\}) \\ &= \sum_{I \subset \{1,2,3\} \wedge |I|=2} \prod_{j \in I} P(B_j) \cdot \prod_{j \notin I} P(B_j^C) + P(\{(1, 1, 1)\})\end{aligned}$$

siccome $|I| = 2$:


$$\begin{aligned}&= \sum_{I \subset \{1,2,3\} \wedge |I|=2} p^2(1-p) + p^3 \\ &= \binom{3}{2} p^2(1-p) + p^3 \\ &= 3 \cdot p^2(1-p) + p^3\end{aligned}$$

Per il sistema ad una componente, chiaramente vale:

$$P(\text{"sistema funziona"}) = p$$

Quindi dobbiamo cercare p tale che:

$$\begin{aligned} 3 \cdot p^2(1-p) + p^3 &> p \\ \Leftrightarrow 3p^2 - 2p^3 &> p \\ \Leftrightarrow p &> \frac{1}{2} \end{aligned}$$

Nel complesso, si ottiene che ha senso usare più componenti solo se ciascuna ha più probabilità di funzionare di $\frac{1}{2}$. 

4 Variabili Aleatorie

Spesso, negli esperimenti concreti ha senso raccogliere i dati attraverso dei costrutti che si possano analizzare più approfonditamente degli spazi di probabilità.

Definizione 4.1. Sia $(\Omega, \mathbb{P}(\Omega), P)$ spazio di probabilità discreto. Si dice variabile aleatoria una mappa (funzione)

$$X: \Omega \rightarrow \mathbb{R}$$

Definizione 4.2. Data una variabile aleatoria X si dice alfabeto di X e si indica \mathcal{X} l'immagine di Ω rispetto X :

$$\mathcal{X} = \{x \in \mathbb{R} \mid \exists \omega \in \Omega: X(\omega) = x\}$$

Nota. Dato uno spazio di probabilità ci sono infinite variabili aleatorie associate.

Per un dato spazio di probabilità $(\Omega, \mathbb{P}(\Omega), P)$ e un evento $E \in \mathbb{P}(\Omega)$, una variabile aleatoria che si può sempre definire è detta *uno grasso*, ed è definita come:

$$\mathbf{1}_E(\omega) = \begin{cases} 1 & \text{se } \omega \in E \\ 0 & \text{se } \omega \notin E \end{cases}$$

Osservazione 4.1. Le variabili aleatorie sono funzioni a valori reali, quindi se sono definite sullo stesso Ω si possono combinare attraverso le consuete operazioni aritmetiche fra reali.

Possiamo assegnare ad un certo alfabeto \mathcal{X} una probabilità, assegnando ai singoletti di \mathcal{X} (cioè ai suoi sottoinsiemi di cardinalità 1) una probabilità P^X che sia compatibile con la misura di probabilità P dello spazio di probabilità su cui è definita X .

Definizione 4.3. Si dice misura di probabilità indotta la funzione

$$\begin{aligned} P^X &\rightarrow [0, 1] \\ x_k &\mapsto P^X(x_k) = P(X^{-1}(x_k)) \end{aligned}$$

dove P è la misura di probabilità data dallo spazio di probabilità su cui è definita X .

$X^{-1}(x_k)$ è l'insieme degli eventi elementari che X mappa in x_k , quindi $P^X(x_k)$ rappresenta la probabilità che l'esito dell'esperimento venga mappato nel numero x_k da X . In altre parole, $P^X(x_k)$ rappresenta la probabilità dell'evento "si verifica un esito che viene mappato in x_k da X ".

Lemma 4.1. *La misura di probabilità indotta è una misura di probabilità, definita sullo spazio campionario \mathcal{X} e sulla σ -algebra $\mathbb{P}(\mathcal{X})$.*