Introduzione agli Algoritmi Randomizzati

In Informatica il caso non è *fortuna o sfortuna,* ma è *potere computazionale!*

In molti contesti dà:

- **Algoritmi più semplici e più veloci** con *garanzie probabilistiche* forti.
- **Soluzioni** laddove il determinismo **fallisce**.

Obiettivi del corso

- Modellare **problemi** con strumenti di **probabilità discreta** e **variabili aleatorie**.
- Usare **disuguaglianze di coda** (Markov, Chebyshev, Chernoff) per ottenere garanzie esplicite.
- Progettare algoritmi **Las Vegas** (*sempre corretto*, costo/tempo random.) e **Monte Carlo** (*tempo fissato/limitato*, errore controllato) calibrando *tempo* e *probabilità di errore*.
- Analizzare **complessità attesa**, amplificare l'*accuratezza della soluzione*.

Gli algoritmi randomizzati sono ovunque

- **Load balancing e sharding** (balls & bins, power-of-two choices).
- **Sistemi distribuiti**: rottura della simmetria, elezione di leader, protocolli resilienti.
- **Crittografia moderna e sicurezza**: casualità come componente essenziale.
- **Ricerca vettoriale**: approssimazioni rapide per dati ad alta dimensione.
- **Intelligenza artificiale.**

La teoria come vantaggio competitivo

- **Progettare con parametri**: accuratezza ε, affidabilità δ, memoria M, latenza/tempo T → "manopole'' dell'algoritmo (numero di ripetizioni/iterazioni, ampiezza del campione, …).

- **Sapere quando e quale strumento usare**: Markov, Chebyshev, Chernoff.

- **Valutare le prestazioni:** cosa possiamo ottenere prima ancora di scrivere il codice.

- **Capire i limiti** (*impossibilità/lower bound*) per evitare soluzioni irrealistiche.

Randomizzazione in AI

- **Motore (allenamento off-line):** campionamento casuale dei dati e aggiornamenti stocastici rendono l'addestramento possibile su scala. Si impara in fretta su dataset enormi (non serve leggere "tutto" a ogni passo).

- **Scudo (richiesta/risposta online):** un pizzico di casualità nelle strategie evita che sistemi interattivi siano *prevedibili e sfruttabili*, cioè **aggirabili** da utenti malintenzionati/spam che "giocano" contro *regole fisse*.

- **Collante (scalabilità):** mescolare i dati, inizializzazioni casuali ⇒ stabilità quando modelli e dataset crescono.

Randomizzazione in AI

- L'**AI** recente **funziona sorprendentemente bene**, ma non tutto è spiegato/chiaro fino in fondo.
- Capire perché certi modelli funzionano e come ottimizzarli richiede **solide basi teoriche**.
- La **randomizzazione** e la **probabilità discreta** sono elementi chiave per fare luce su questi fenomeni.
- **Obiettivo del corso**: fornire strumenti per *progettare*, *analizzare* e *capire* — **oggi e domani.**

Contenuti del corso

- **Parte I — Fondamenti di probabilità**: richiami, probabilità su eventi, variabili aleatorie discrete.
- **Parte II — Limiti di coda e applicazioni**: Markov–Chebyshev–Chernoff; balls & bins, hashing.
- **Parte III — Algoritmi randomizzati**: Las Vegas, Monte Carlo, complessità attesa e con alta probabilità.

Modalità d’esame - Panoramica

- **Esame scritto.**
- **Orale facoltativo** (su richiesta del docente per chiarimenti o su richiesta dello studente).
- **Due tipologie di domande**: (1) teoria; (2) analisi/progettazione di algoritmi.
- **Dettagli pratici** (date, durata, materiali consentiti) saranno comunicati sul canale del corso.

Domande di tipo 1 - Teoria

- Riguardano **qualsiasi argomento trattato a lezione**.

- **Esempi**: indipendenza di eventi; Legge della probabilità totale; Teorema di Bayes; enunciare il Chernoff bound.

- **Criterio di valutazione**: correttezza, chiarezza, notazione.

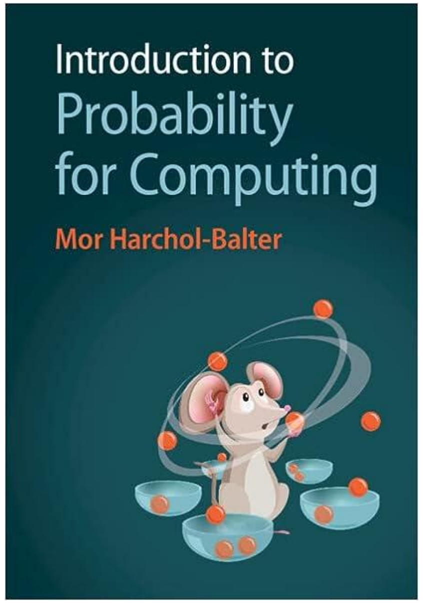
Domande di tipo 2 – Analisi e progettazione

- **Analisi**: probabilità di terminazione/errore o tempo atteso (es. entro *x* iterazioni).
- **Progettazione**: scelta randomizzata o schema per ottenere prestazioni target (ε, δ, memoria, tempo).
- **Valutazione**: idea, impostazione, calcolo e conclusione.

Come prepararsi

- **Niente domande trabocchetto**: gli esercizi d'esame riflettono quelli svolti a lezione.
- Per ogni **tipologia potenzialmente assegnabile** ci saranno esercizi svolti durante il corso.
- **Suggerimenti**:
  - Studiare passo passo.
  - Non limitarsi alla lettura delle diapositive ma approfondire gli argomenti sul libro.
  - Svolgere tutti gli esercizi assegnati durante il corso.

Libro di testo



Author: **Mor Harchol-Balter**

Published: 2024
Publisher: Cambridge University Press (CUP)
ISBN: 978-1-009-30907-3

https://www.cs.cmu.edu/~harchol/Probability/book.html

Si parte!

Probabilità su Eventi

Spazio Campionario e Eventi

Parleremo di **Probabilità** solo in relazione ad un **esperimento** e al suo corrispondente **spazio campionario** (*sample space*), indicato con Ω che è l'insieme di tutti i possibili risultati dell'esperimento.

Ω = Spazio campionario dell'esperimento = Insieme di tutti i possibili risultati.

Lanciamo un dado. 

Esperimento: lancio di un dado.

Spazio campionario: $\Omega = \{1, 2, 3, 4, 5, 6\}$.

Spazio Campionario e Eventi

Def: Un **evento**, E, è un qualsiasi sottoinsieme dello spazio campionario, Ω.

Esempio: Lancio di un dado.

Alcuni possibili eventi:

- $E = \{3\}$ definisce l'evento «è uscito il numero 3».
- $E' = \{2, 4, 6\}$ definisce l'evento «è uscito un numero pari».
- $E'' = \{1, 3, 5\}$ definisce l'evento «è uscito un numero dispari».

Un elemento di Ω è talvolta chiamato *evento semplice* o anche *evento elementare (sample point)*.
Un sottoinsieme $E \subseteq \Omega$ viene anche detto *evento composto*.

Spazio Campionario e Eventi

Def: Un **evento**, E, è un qualsiasi sottoinsieme dello spazio campionario, Ω.

Esperimento: Lancio di *due* dadi.

Spazio campionario: $\Omega = \{(x, y) | \; x, y \in \{1, 2, 3, 4, 5, 6\}\}$

Alcuni possibili eventi:

- $E_1 = \{(1,2), (2,2), (3,2), (4,2), (5,2), (6,2)\}$ definisce l'evento «è uscito il numero 2 sul secondo dado».
- $E_2 = \{(1,4), (1,5), (1,6)\}$ definisce l'evento «è uscito il numero 1 sul primo dado e un numero maggiore di 3 sul secondo».

Spazio Campionario e Eventi

<u>Def</u>: Un **evento**, E, è un qualsiasi sottoinsieme dello spazio campionario, Ω.

Usiamo la notazione insiemistica.

$E_1 \cup E_2$: "o E_1 o E_2(o entrambi) occorrono".

$E_1 \cap E_2$: "sia E_1 sia E_2 occorrono simultaneamente".

$E_1 \setminus E_2$: "occorre E_1 ma non E_2". Cioè occorre un evento (elementare) che è in E_1 ma non in E_2".

$\overline{E} = \Omega \setminus E$: "$E$ non occorre" (complemento di E).

Spazio Campionario e Eventi

Def: Un **evento**, E, è un qualsiasi sottoinsieme dello spazio campionario, Ω.

Esperimento: Lancio di due dadi.

$$
\begin{array}{cccccccc}
 & & E_1 & & & E_2 & \\
\Omega = & \left\{ \begin{array}{c} \\ \\ \\ \\ \\ \\ \end{array} \right. \hspace{-2em} &
\end{array}
\begin{array}{cccccc}
(1,1) & (1,2) & (1,3) & (1,4) & (1,5) & (1,6) \\
(2,1) & (2,2) & (2,3) & (2,4) & (2,5) & (2,6) \\
(3,1) & (3,2) & (3,3) & (3,4) & (3,5) & (3,6) \\
(4,1) & (4,2) & (4,3) & (4,4) & (4,5) & (4,6) \\
(5,1) & (5,2) & (5,3) & (5,4) & (5,5) & (5,6) \\
(6,1) & (6,2) & (6,3) & (6,4) & (6,5) & (6,6)
\end{array}
$$

- Cosa è $E_1 \cup E_2$?
- Cosa è $\overline{E_1}$?
- Sono E_1 e E_2 indipendenti? Vedremo…

Spazio Campionario e Eventi

<u>Def</u>: Se $E_1 \cap E_2 = \emptyset$, allora E_1 e E_2 sono **mutuamente esclusivi (disgiunti)**.

<u>Def</u>: Se $E_1, E_2, \ldots, E_n$ sono eventi tali che $E_i \cap E_j = \emptyset, \ \forall i \neq j,$
e tali che $\bigcup_{i=1}^{n} E_i = F$ allora diciamo che gli eventi $E_1, E_2, \ldots, E_n$ formano una **partizione** di F.

Qual è un esempio di eventi che partizionano Ω per il lancio di due dadi?

$$E_k = \{(x, y) \mid x = k\}, \qquad k = 1, 2, 3, 4, 5, 6.$$

Infatti $\quad \bigcup_{k=1}^{6} E_k = \Omega, \qquad E_i \cap E_j = \emptyset, \ \forall\, i \neq j$

Spazio Campionario e Eventi

<u>Def</u>: Uno spazio campionario è **discreto** se il numero dei risultati è ***numerabile***.
Uno spazio campionario è **continuo** se il numero dei risultati è ***non numerabile***.

Quali di questi esperimenti ha uno spazio campionario discreto/continuo?

- ❑ Lancia una moneta 2 volte. Discreto.
- ❑ Lancia una freccetta sull’intervallo [0,1] . Continuo.
- ❑ Lancia una moneta fino ad ottenere testa la prima volta. Discreto.
- ❑ Segna il momento in cui arriva la centesima email. Continuo.

Probabilità Definita su Eventi

$\boldsymbol{P}\{E\}$ $=$ probabilità dell'evento E
$=$ probabilità che il risultato dell'esperimento sia nell'insieme E.

<u>I tre Assiomi di Probabilità</u>:

Non-negatività: $\boldsymbol{P}\{E\} \geq 0$ per qualsiasi evento E.

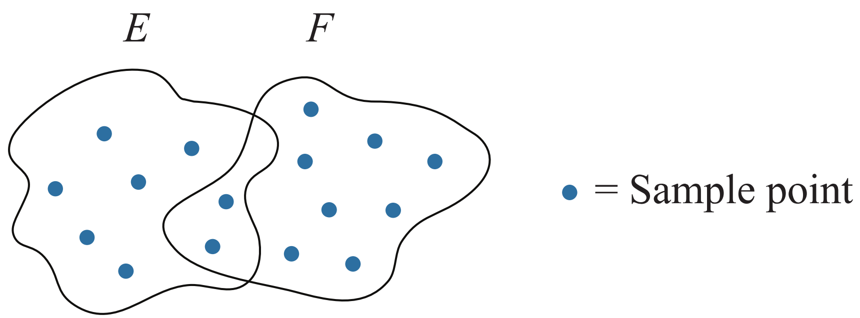
Additività: Se $E_1, E_2, E_3, \ldots$ è una sequenza numerabile di eventi disgiunti, allora

$$\boldsymbol{P}\{E_1 \cup E_2 \cup E_3 \cup \cdots\} = \boldsymbol{P}\{E_1\} + \boldsymbol{P}\{E_2\} + \boldsymbol{P}\{E_3\} + \cdots$$

Normalizzazione: $\boldsymbol{P}\{\Omega\} = 1$.

Conseguenze dei 3 Assiomi di Probabilità

$P\{\bar{E}\} = 1 - P\{E\}$



Come lo dimostriamo?   Usiamo la *normalizzazione* e l'*additività*.

E e $\bar{E}$ sono ovviamente disgiunti: $E \cap \bar{E} = \emptyset$.

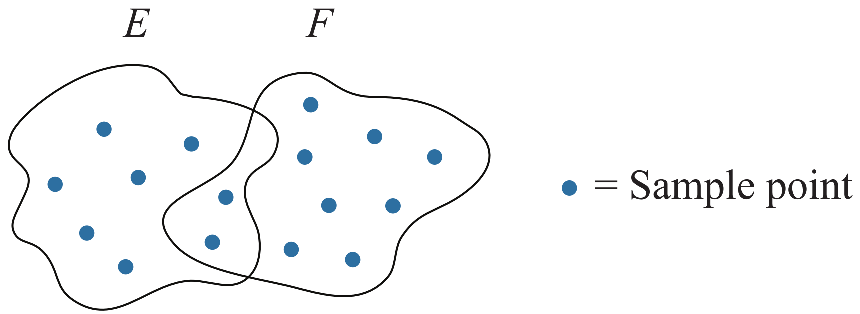
Inoltre formano una partizione dello spazio campionario: $E \cup \bar{E} = \Omega$.

Normalizzazione: $\boldsymbol{P}\{E \cup \bar{E}\} = \boldsymbol{P}\{\Omega\} = 1.$

Additività: $\boldsymbol{P}\{E \cup \bar{E}\} = \boldsymbol{P}\{E\} + \boldsymbol{P}\{\bar{E}\}.$

Quindi $\boldsymbol{P}\{\bar{E}\} = 1 - \boldsymbol{P}\{E\}.$

Conseguenze dei 3 Assiomi di Probabilità



<u>Lemma 2.5</u>: $\boldsymbol{P}\{E \cup F\} = \boldsymbol{P}\{E\} + \boldsymbol{P}\{F\} - \boldsymbol{P}\{E \cap F\}$.

Come lo dimostriamo? Usiamo l'*additività*.

E e F non sono disgiunti, **ma $\boldsymbol{E}$ e $\boldsymbol{F \setminus E}$ lo sono!**

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

L'additività ci dice: $\boldsymbol{P}\{E \cup F\} = \boldsymbol{P}\{E \cup (F \setminus E)\} = \boldsymbol{P}\{E\} + \boldsymbol{P}\{F \setminus E\}$.

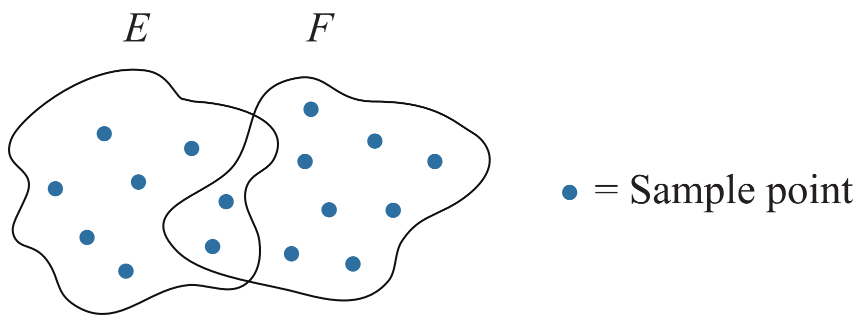
Anche $F \setminus E$ e $E \cap F$ sono disgiunti e formano una partizione di F. Cioè: $F = (F \setminus E) \cup (E \cap F)$.

L'additività ci dice: $\boldsymbol{P}\{F\} = \boldsymbol{P}\{(F \setminus E) \cup (E \cap F)\} = \boldsymbol{P}\{F \setminus E\} + \boldsymbol{P}\{E \cap F\}$

Quindi: $\boldsymbol{P}\{E \cup F\} = \boldsymbol{P}\{E\} + \boldsymbol{P}\{F\} - \boldsymbol{P}\{E \cap F\}$

Conseguenze dei 3 Assiomi di Probabilità

Lemma 2.6 (union bound): $\boldsymbol{P}\{E \cup F\} \leq \boldsymbol{P}\{E\} + \boldsymbol{P}\{F\}$.



$$\boldsymbol{P}\{E \cup F\} = \boldsymbol{P}\{E\} + \boldsymbol{P}\{F\} - \boldsymbol{P}\{E \cap F\} \leq \boldsymbol{P}\{E\} + \boldsymbol{P}\{F\}.$$

Perché $\boldsymbol{P}\{E \cap \mathrm{F}\} \geq 0.$

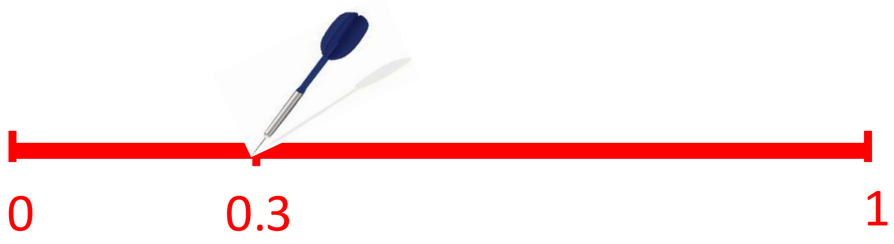
Quando si ha $\boldsymbol{P}\{E \cup F\} = \boldsymbol{P}\{E\} + \boldsymbol{P}\{F\}$?

Quando $\boldsymbol{P}\{E \cap \mathrm{F}\} = 0$ cioè quando E e F sono disgiunti.

Conseguenze dei 3 Assiomi di Probabilità

Lanciamo una freccetta, con uguale probabilità di finire in qualsiasi punto dell'intervallo [0,1].

E = "freccetta finisce su 0.3". Qual è la probabilità di E ?



Dimostriamo che $\boldsymbol{P}\{E\} = 0$.

Supponiamo che $\boldsymbol{P}\{E\} = \epsilon > 0$.

Qual è la probabilità che la freccetta finisca su 0.5? Ovviamente ancora ϵ.
Qual è la probabilità che finisca su 0.45? Su 0.891? Su 0.0034? … Sempre ϵ. Tutti questi eventi sono ovviamente disgiunti e quindi le loro probabilità si sommano (additività).
Prendiamo $N = \left\lceil \frac{1}{\epsilon} \right\rceil + 1$ punti. Qual è la probabilità che la freccetta finisca su uno di essi?

$$\sum_{\{i=1\}}^{N} \epsilon = \mathrm{N}\epsilon > 1$$

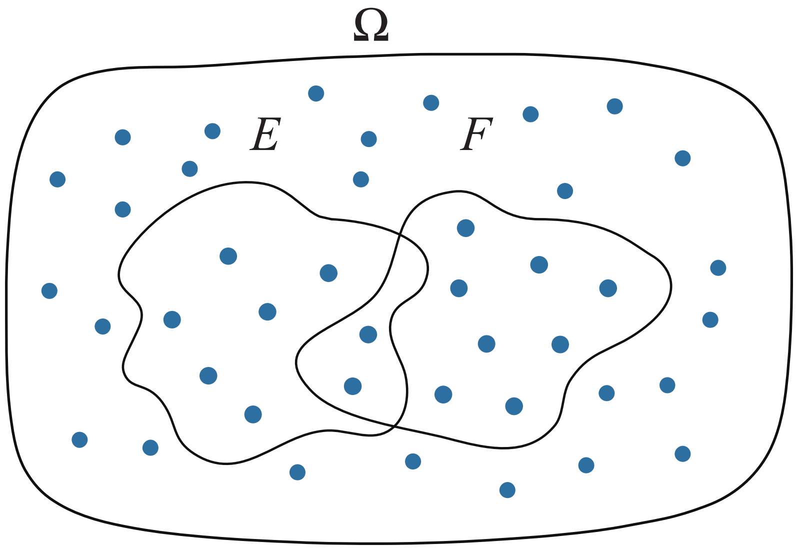
Assurdo! Quindi $\boldsymbol{P}\{E\} = 0$.

Probabilità Condizionata su Eventi

<u>Def</u>: La probabilità condizionata dell'evento E dato l'evento F è

$$\boldsymbol{P}\{E|F\} = \frac{\boldsymbol{P}\{E \cap F\}}{\boldsymbol{P}\{F\}}$$

assumendo $\boldsymbol{P}\{F\} > 0$.



<u>Due equivalenti prospettive</u>:

$$\boldsymbol{P}\{E \mid F\} = \frac{2}{10}$$

(dei 10 risultati nell'insieme F, soltanto 2 sono nell'insieme E)

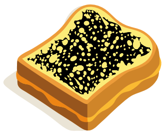
$$\boldsymbol{P}\{E \mid F\} = \frac{\boldsymbol{P}\{E \cap F\}}{\boldsymbol{P}\{F\}} = \frac{\frac{2}{42}}{\frac{10}{42}} = \frac{2}{10}$$

Probabilità Condizionata su Eventi

<u>Def</u>: La probabilità condizionata dell'evento E dato l'evento F è

$$\boldsymbol{P}\{E|F\} = \frac{\boldsymbol{P}\{E \cap F\}}{\boldsymbol{P}\{F\}}$$

assumendo $\boldsymbol{P}\{F\} > 0$.

<u>Scelte per un panino</u>: 

Lun – marmellata
Mar – formaggio
Mer – tacchino

$\Big\}$ 1ª metà della settimana

Gio – formaggio
Ven – tacchino
Sab – formaggio
Dom – niente

$\Big\}$ 2ª metà della settimana

Qual è $\boldsymbol{P}\{\text{formaggio} \mid 2^{a} \text{ metà della settimana}\}$?

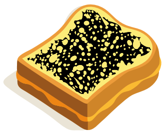
Vediamo entrambi i punti di vista.

Probabilità Condizionata su Eventi

<u>Def</u>: La probabilità condizionata dell'evento E dato l'evento F è

$$\boldsymbol{P}\{E|F\} = \frac{\boldsymbol{P}\{E \cap F\}}{\boldsymbol{P}\{F\}}$$

assumendo $\boldsymbol{P}\{F\} > 0$.

<u>Scelte per un panino</u>: 

Lun – marmellata
Mar – formaggio
Mer – tacchino

1^a metà della settimana

Gio – formaggio
Ven – tacchino
Sab – formaggio
Dom – niente

2^a metà della settimana

Qual è $\boldsymbol{P}\{\text{formaggio} \mid 2^a \text{ metà della settimana}\}$?

Dei 4 giorni della seconda metà della settimana, 2 prevedono
Il formaggio:

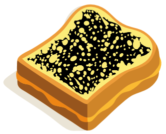
$$\boldsymbol{P}\{\text{formaggio} \mid 2^a \text{ metà}\} = \frac{2}{4} = \frac{1}{2}.$$

Probabilità Condizionata su Eventi

Def: La probabilità condizionata dell'evento E dato l'evento F è

$$\boldsymbol{P}\{E|F\} = \frac{\boldsymbol{P}\{E \cap F\}}{\boldsymbol{P}\{F\}}$$

assumendo $\boldsymbol{P}\{F\} > 0$.

Scelte per un panino: 

Lun – marmellata
Mar – formaggio
Mer – tacchino

1^a metà della settimana

Gio – formaggio
Ven – tacchino
Sab – formaggio
Dom – niente

2^a metà della settimana

Qual è $\boldsymbol{P}\{\text{formaggio} \mid 2^a \text{ metà della settimana}\}$?

$$\boldsymbol{P}\{\text{formaggio} \mid 2^a \text{ metà}\} = \frac{\boldsymbol{P}\{\text{formaggio} \cap 2^a \text{ metà}\}}{\boldsymbol{P}\{2^a \text{ metà}\}} = \frac{\frac{2}{7}}{\frac{4}{7}} = \frac{2}{4}$$

Probabilità Condizionata su Eventi

Il cucciolo di cavallo è chiamato *puledro*.
Le cavalle partoriscono un puledro alla volta.
Ogni puledro ha **uguale probabilità** di essere **maschio (colt)** o **femmina (filly).**

Ci viene detto che **una coppia di cavalli ha avuto 2 puledri**, e che **almeno uno di questi è un maschio**.

Qual è $\boldsymbol{P}\{\text{entrambi maschi} \mid \geq 1 \text{ maschio}\}$?

$$\boldsymbol{P}\{\text{entrambi maschi} \mid \geq 1 \text{ maschio}\} = \frac{\boldsymbol{P}\{\text{entrambi maschi} \cap \geq 1 \text{ maschio}\}}{\boldsymbol{P}\{\geq 1 \text{ maschio}\}}$$

$$= \frac{\boldsymbol{P}\{\text{entrambi maschi}\}}{\boldsymbol{P}\{\geq 1 \text{ maschio}\}} = \frac{\frac{1}{4}}{\frac{3}{4}} = \frac{1}{3}$$

Probabilità Condizionata su Eventi

Il cucciolo di cavallo è chiamato puledro.
Le cavalle partoriscono un puledro alla volta.
Ogni puledro ha **uguale probabilità** di essere un **maschio** o una **femmina.**

Ci viene detto che **una coppia di cavalli ha avuto 2 puledri**, e che **almeno uno di questi è un maschio**.

Qual è $\boldsymbol{P}\{\text{entrambi maschi} \mid \geq 1 \text{ maschio}\}$?

$$\boldsymbol{P}\{\text{entrambi maschi} \mid \geq 1 \text{ colt}\} = \frac{1}{3}$$

	maschio	femmina
maschio	✓	
femmina		