Oct29

Wednesday, October 28, 2020 10:29 PM

Defn A sample space is a (finite) set of outcomes Ω ← nonempty

A probability fn is a function

$$Pr : \Omega \longrightarrow \mathbb{R}$$

① $0 \le Pr(\omega) \le 1 \quad \forall \; \omega \in \Omega$

② $\sum_{\omega \in \Omega} Pr(\omega) = 1$ ←

- An event is a subset $E \subseteq \Omega$.
- The probability of an event is

$$Pr(E) = \sum_{\omega \in E} Pr(\omega)$$

Ex $E \subseteq \Omega$ ← roll 2 dice

↑ roll at least one 6

$$Pr(E) = \sum_{\substack{\omega \text{ w/} \\ \text{a } 6}} 1/36$$

Remark $\emptyset \subseteq \Omega \rightsquigarrow Pr(\emptyset) = 0$

$\Omega \subseteq \Omega \rightsquigarrow Pr(\Omega) = 1$ ←

Defn $E, F \subseteq \Omega$. Then E & F are disjoint if $E \cap F = \emptyset$

Lemma

* If E & F are disjoint events

Then $Pr(E \cup F) = Pr(E) + Pr(F)$

Proof

$$Pr(E \cup F) = \sum_{\omega \in E \cup F} Pr(\omega) \boxed{=} \sum_{\omega \in E} Pr(\omega) + \sum_{\omega \in F} Pr(\omega)$$

ω in E or F not both

$\omega \in$ both E & F I counted it twice

Lemma $E, F \subseteq \Omega$ 2 events (inclusion/exclusion)

$$Pr(E \cup F) = Pr(E) + Pr(F) - Pr(E \cap F)$$

Example Ω = roll 2 dice $= \{(m,n) \mid m,n \in \{1,2,\dots,6\}\}$

Remark $E \cup F$ = E or F

Pr(roll a 6)

$E = \{$roll ≥ 1 6$\}$

$E_1 = \{$first die is a 6$\}$

$E_2 = \{$second die a 6$\}$

$E = E_1 \cup E_2$

$Pr(E_1) = 1/6 = Pr(E_2)$

$Pr(E_1 \cap E_2) = Pr$(both are 6)

$= Pr((6,6)) = 1/36$

Lemma $\Rightarrow$ $Pr(E) = Pr(E_1) + Pr(E_2) - Pr(E_1 \cap E_2)$

$$= \frac{1}{6} + \frac{1}{6} - \frac{1}{36} = 11/36.$$

Defⁿ Let E be an event $E \subseteq \Omega$

The complement of E is

$$E^c = \{\omega \in \Omega \mid \omega \notin E\}$$

Lemma $Pr(E^c) = 1 - Pr(E)$.

Pf/ $Pr(E) + Pr(E^c) \underset{\substack{\uparrow \\ \text{disjoint}}}{=} Pr(E \cup E^c) = Pr(\Omega) = 1$ $\emptyset$

Rmk

Sometimes easier to find $Pr(E^c)$ directly.

Then use Lemma.

Example $\Omega = 2$ dice.

$H = (\text{sum of dice} \geq 4) \subseteq \Omega$.

$Pr(H) = ?$

well $H^c = (\text{sum} < 4)$

$= \{(1,1), (1,2), (2,1)\}$

$Pr(H^c) = \frac{3}{36} = \frac{1}{12}$

$\Longrightarrow Pr(H) = \frac{11}{12}$

Rmk E, F 2 events $E \cap F = E$ and F

$Pr(E \cap F) = Pr(E \text{ and } F)$

Example E first die ≥ 2

F second die ≤ 5

$$Pr(E \cap F) = \underset{\uparrow}{Pr\,E} \cdot \underset{\uparrow}{Pr(F)}$$

By counting principle

First die roll doesn't affect second

Independence of rolls allowed this computation.

In general: $Pr(E \cap F) \neq Pr(E) \cdot Pr(F)$.

Example: Drawing cards from a deck.

E = (First card is a King)

F = (Second card is a King).

$Pr(E) = \frac{1}{13}$ $\qquad Pr(F) = \frac{1}{13} = \frac{4 \text{ kings}}{52 \text{ cards}}$

But If I know card 1 is a king then changes prob card 2 is a king.

Pr(2nd a king given first was a king)

$= Pr(F \text{ given } \underline{\underline{E}})$ or $Pr(F|E)$

$= \frac{3}{51}$ (only 3 kings left).

$\left(\left[Pr(F \mid E^c) = 4/51 \right] \leftarrow \text{check} \right)$

$Pr(E \cap F) = ?$ (prob both cards kings)

$$= Pr(E) \cdot Pr(F/E)$$

$$= \frac{1}{13} \cdot \frac{3}{51} < \frac{1}{13} \cdot \frac{1}{13} = Pr(E) \cdot Pr(F).$$

$\uparrow$ First king

$G =$ (second card is an Ace).

$$Pr(G \mid E) = \frac{4}{51} \qquad \left(Pr\, G = \frac{1}{13} \right)$$

$$Pr(E \cap G) = \frac{1}{13} \cdot \frac{4}{51} > \frac{1}{13} \cdot \frac{1}{13} = Pr(E) \cdot Pr(G).$$

$\|$

$Pr(E) \cdot \underline{Pr(G/E)}$

__3rd Case__ Replace a card & shuffle after drawing. ← Adding independence

$$Pr(E \cap F) = Pr(E) \cdot Pr(F) = \frac{1}{13} \cdot \frac{1}{13}$$

Defn Let E & F be two events.

We say E & F are independent if

$$Pr(E \cap F) = Pr(E) \cdot Pr(F)$$

Bayes' Formula

E, F are 2 events

Pr(F given that E occured)

$= Pr(F/E)$

Notice

$$\rightarrow Pr(E \cap F) = Pr(E) \cdot Pr(F|E)$$

solve & get

$$\underbrace{Pr(F|E) = \frac{Pr(E \cap F)}{Pr(E)}}$$

Definition of conditional probability.

Prob F occures assuming E does $= \dfrac{\text{Prob } E \text{ and } F}{\text{Prob } E}$

Symmetric

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

$$= Pr(F) \cdot Pr(E|F).$$

Solve for Prob(E|F)

Formula Bayes' Formula

$$Pr(E|F) = \frac{Pr(E) \cdot Pr(F|E)}{Pr(F)}$$

Tip Use this formula to subdivide probability computations into knowable bits.

Prop E and F are events.

$$\underline{Pr(E)} = \underline{Pr(E|F)\cdot Pr F} + Pr(E|F^c)\cdot Pr(F^c)$$

Proof

$$E = (E\cap F)\cup(E\cap F^c) \quad \text{(disjoint union)}$$

$$Pr(E) = Pr(E\cap F) + Pr(E\cap F^c)$$

$$= Pr(E|F)\cdot Pr(F) + Pr(E|F^c)\cdot Pr(F^c) \quad \emptyset$$

Example

2 urns $\quad A = \{10 \text{ gold coins } \& \text{ } 5 \text{ silver}\}$

$B = \{\underline{2 \text{ gold}} \text{ } \& \text{ } 8 \text{ silver}\}$.

I pick an urn at random.

I pick a coin out of that urn.

Question Probability that I (picked a gold coin)

"E

$F = (\text{pick urn } A) \qquad Pr(F) = \frac{1}{2}$

$F^c = (\text{pick urn } B) \qquad Pr(F^c) = \frac{1}{2}$

$Pr(E|F) = \frac{10}{15} = \frac{2}{3}$

$Pr(E|F^c) = \frac{2}{10} = \frac{1}{5}$

$$Pr E = Pr(E|F)\cdot Pr F + Pr(E|F^c)\cdot Pr(F^c)$$

$$= \frac{2}{3}\cdot\frac{1}{2} + \frac{1}{5}\cdot\frac{1}{2} = \frac{1}{3} + \frac{1}{10} = \frac{13}{30}.$$

Corollary (Bayes' Formula)

$$Pr(E|F) = \frac{Pr(F|E)\cdot Pr E}{Pr(F|E)\cdot Pr E + Pr(F|E^c)\cdot Pr(E^c)}$$

Pf/sub prop in Bayes'

Monte-Carlo Algorithms

Example Understand correctness of probablyPrime

Test millerRabin(a, m) stuff

- True if a is a witness for compositness of m.
- False otherwise.

TRUE $\xRightarrow{100\%}$ m composite

TRUE $\xleftarrow{\geq 75\%}$ m composite

↑ 75% choices of a.

$$Pr(\text{m composite} \mid \text{millerRabin returns TRUE}) = 1$$

$$Pr(\text{mR TRUE} \mid \text{m composite}) \geq .75$$

Want to know

If millerRabin returns FALSE ~~20~~ N times
what is probability that m is prime
(not composite).

Q: $\Pr(m \text{ not comp} \mid mR \text{ returns FALSE } N \text{ times}) = ?$

Setup a general framework

- Large set of integers S ← int
- Interesting property $\mathcal{A}$ ← composite
- Know approx what proportion of S satisfy $\mathcal{A}$. ↙ prime number thm
- Difficult to determine if a particular $m \in S$ is or isn't $\mathcal{A}$.

A Monte-Carlo algorithm is:

Input	Output
an $m \in S$ to be tested	YES or No
potential witness ↓ r random #	

Satisfying:

① If the algorithm returns YES then m is $\mathcal{A}$.

② If m is $\mathcal{A}$ the alg returns YES $\geq \frac{1}{2}$ the time.

① $\Pr(m \text{ is } \mathcal{A} \mid \text{returns YES}) = 1$

② $\Pr(\text{returns YES} \mid m \text{ is } \mathcal{A}) \geq \frac{1}{2}$. ← 1

(rmk perfect alg returns YES $\Longleftrightarrow$ m is $\mathcal{A}$)

Suppose MC alg returns No N times

How confident are we that m is not $\mathcal{A}$?

Compute $\Pr(m \text{ not } \mathcal{A} \mid \text{return No } N \text{ times})$

Claim As $N >> 0$ prob is close to 1

Proof For simplicity assume 99% of S is $\mathcal{A}$.

① Define two events

→ $E = (\overset{\text{an}}{m \in S} \text{ is not } \mathcal{A})$.

$F = (\text{Algorithm returns No } N\text{-times})$.

Goal $\Pr(E/F)$

Bayes'

$$\underline{\Pr(E/F)} = \frac{\Pr(F|E)\cdot\Pr(E)}{\underline{\Pr(F|E)\cdot\Pr(E)} + \underline{\boxed{\Pr(F|E^c)}\,\Pr(E^c)}}$$

$\Pr(E) = .01$

$\Pr(E^c) = .99$

$\Pr(F|E) = \Pr(\text{return No } N \text{ times} \mid m \text{ is not } \mathcal{A}) = 1$

If return YES $\Longrightarrow$ m is $\mathcal{A}$.

returns No $\Longleftarrow$ m not $\mathcal{A}$

$\Swarrow$

return No N-times

Left w/ $Pr(F|E^c)$

$= Pr(\text{return No n-times} \mid m \text{ is } \mathcal{A}) \le \left(\frac{1}{2}\right)^N$

m is $\mathcal{A}$ $\nearrow \ge \frac{1}{2}$ yes

$\searrow \le \frac{1}{2}$ no.

$= Pr(\text{return No} \mid m \text{ is } \mathcal{A})^N$

$= (1 - Pr(\text{return YES} \mid m \text{ is } \mathcal{A}))^N$

$\le \left(\frac{1}{2}\right)^N.$

$$Pr(E|F) = \frac{1 \cdot .01}{1 \cdot .01 + .99 \cdot \left(\frac{1}{2}\right)^N} = \frac{.01}{.01 + 2^{-N}(.99)}$$

$$= \frac{1}{1 + 2^{-N}(99)}$$

$$= \frac{2^N + 99 - 99}{2^N + 99}$$

$$= 1 - \frac{99}{2^N + 99}.$$

As $N >> 0$ approaches 1

e.g. $N = 100$ get $1 - 10^{-321}$