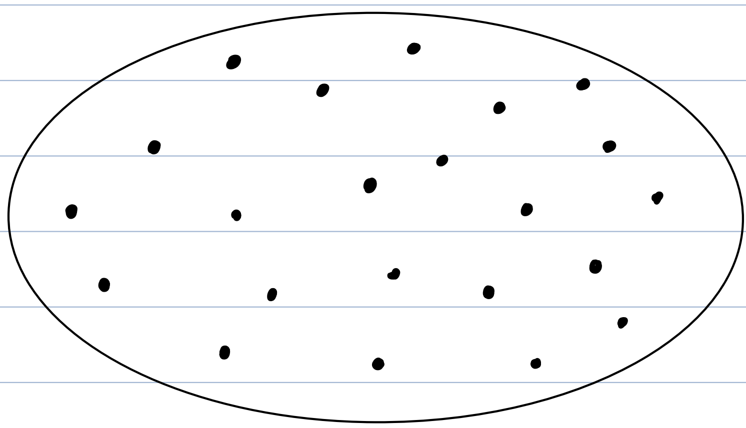
Recap :

Ω : finite / countably infinite set

$p : \Omega \longrightarrow \mathbb{R}^{\geq 0}$ s.t. $\sum_{x \in \Omega} p(x) = 1$.

Event $\mathcal{E} \subseteq \Omega$, $\Pr[\mathcal{E}] = \sum_{x \in \mathcal{E}} p(x)$.

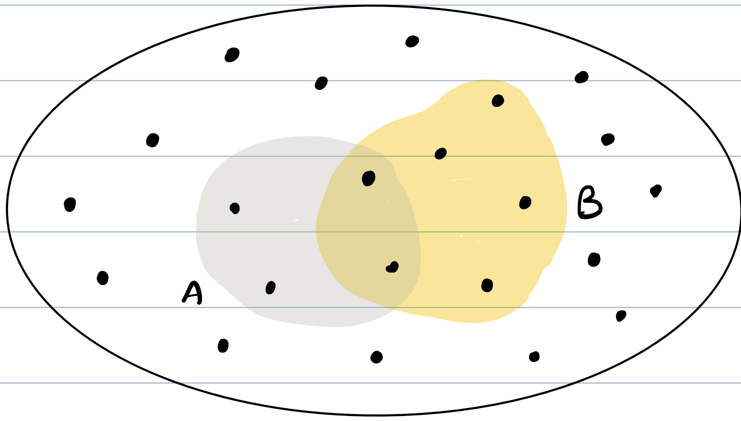


LECTURE 17

Conditional Probability :

$A \subseteq \Omega$, $B \subseteq \Omega$.

Conditional prob : what is the prob. of A, if we restrict our attention to the set B?



$$\Pr[A \mid B] = \frac{\Pr[A \cap B]}{\Pr[B]}.$$

Example 1: $n+1$ jars, numbered $0, 1, \ldots, n$. Each jar has n balls. The i^{th} jar has i blue balls, $n-i$ red balls.

We pick a uniformly random jar and sample two balls from the jar, without replacement.

p = [What is the probability that the second sampled ball is blue, given that the first sampled ball is blue?]

Using the definition of conditional probability

$$p = \frac{q}{r} \quad \text{where}$$

$$q = \Pr\left[\begin{array}{l}\text{Sample unif. rand. jar} \\ \text{Sample two balls uniformly} \\ \text{at random, without replacement} \\ \text{both balls are blue}\end{array}\right]$$

$$r = \Pr\left[\begin{array}{c}\text{Sample unif. rand. jar} \\ \text{Sample one balls uniformly at random} \\ \text{the sampled ball is blue}\end{array}\right]$$

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

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

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

$$= \frac{n(n+1)(2n-2)}{6n(n-1)(n+1)} = 1/3$$

$$\therefore \quad p = \frac{2}{3}.$$

LAW OF TOTAL PROBABILITY

Conditional probability can be useful, even when the problem statement doesn't explicitly involve conditional probility.

Let Ω be the sample space, and suppose we want to compute $\Pr[A]$ for some $A \subseteq \Omega$.

Let $\Omega_1 \cdots \Omega_n$ be a partition of Ω
(i.e. $\bigcup_{i=1}^{n} \Omega_i = \Omega$, $\Omega_i \cap \Omega_j = \phi$ for $i \neq j$)

$$\Pr[A] = \sum_{i=1}^{n} \Pr[A \cap \Omega_i]$$

$$= \sum_{i=1}^{n} \Pr[A \mid \Omega_i] \cdot \Pr[\Omega_i].$$

There can be several ways to partition Ω, and depending on the problem, one partitioning might be better than another.

Example : σ is a uniformly random permutation from $\{1, 2, \ldots, n\}$ to $\{1, 2, \ldots, n\}$.

$$\mathcal{E}_i = \text{for all } j < i, \ \sigma(j) < \sigma(i).$$

$$\Pr[\mathcal{E}_i] = ?$$

Approach 1 : Ω = set of all permutations from $\{1, 2, \ldots, n\}$ to $\{1, 2, \ldots, n\}$.

For $j \in \{1, 2, \ldots, n\}$, $\Omega_j = \left\{ \sigma \in \Omega \text{ s.t. } \sigma(i) = j \right\}$

$$\Pr[\mathcal{E}_i] = \sum_{j=1}^{n} \Pr[\mathcal{E}_i \cap \Omega_j]$$

Now, note that if $j < i$,

$$\mathcal{E}_i \cap \Omega_j = \phi \qquad \sigma \text{ is a permutation}$$

$$\therefore \Pr[\mathcal{E}_i] = \sum_{j=i}^{n} \Pr[\mathcal{E}_i \mid \Omega_j] \cdot \Pr[\Omega_j].$$

First, check that $\Pr[\Omega_j] = 1/n$ for all j.

$$\Pr[\mathcal{E}_i \mid \Omega_j] = \binom{j-1}{i-1} \Big/ \binom{n-1}{i-1}$$

Hence, $\Pr[\mathcal{E}_i] = \frac{1}{n} \sum_{j=i}^{n} \binom{j-1}{i-1} \Big/ \binom{n-1}{i-1}$.

$\blacksquare$

Approach 2: Take any set $S \subseteq \{1, 2, \ldots, n\}$, $|S| = i$.

$$\Omega_S = \left\{ \begin{array}{ll} \sigma \in S & \text{s.t.} \\ \sigma(j) \in S & \text{for all } j \leq i \end{array} \right\}$$

$$\Pr[\mathcal{E}_i] = \sum_{\substack{S \subseteq \{1, \ldots, n\} \\ |S| = i}} \Pr[\mathcal{E}_i \cap \Omega_S]$$

$$= \sum_{\substack{S \subseteq \{1 \ldots n\} \\ |S| = i}} \underbrace{\Pr[\mathcal{E}_i \mid \Omega_S]}_{1/i} \Pr[\Omega_S]$$

$$= \frac{1}{i} \sum_{\substack{S \subseteq \{1 \ldots n\} \\ |S| = i}} \Pr[\Omega_S]$$

Since $\bigcup_{\substack{S \subseteq \{1 \ldots n\} \\ |S| = i}} \Omega_S = \Omega$ and $\Omega_S \cap \Omega_{S'} = \phi$ for all $S \neq S'$

$$\sum_{\substack{S \subseteq \{1,\dots,n\} \\ |S| = i}} \Pr[\Omega_S] = 1.$$

Hence $\Pr[\mathcal{E}_i] = 1/i$.

$\blacksquare$

Take-home message: Appropriately partitioning the sample space can make the probability computation significantly simpler (and cleaner).

Example: r red balls, b blue balls and a green ball in a jar.

The balls are picked one after another, uniformly at random, without replacement.

What is the probability that the green ball is picked before all the blue balls?

Intuition: If there were no red balls, then this probability is $1/b+1$. And the red balls do not affect the probability. Need to formalize this by appropriately partitioning the sample space.

Approach 1: based on the position where green ball is picked.

Sample sp. Ω = all permutations of $G\cdot 1, R\cdot 1, \dots, R\cdot r, B\cdot 1, \dots, B\cdot b$

For each $i \in \{1, 2, \dots, r+b+1\}$, let Ω_i denote the set of all permutations where $G\cdot 1$ is at position i. Check: $\Omega = \bigcup_{i=1}^{r+b+1} \Omega_i$, $\Omega_i \cap \Omega_j = \phi$

Event $\mathcal{E}$: $G\cdot 1$ appears before $B\cdot 1, \dots, B\cdot b$.

$$\Pr[\mathcal{E}] = \sum_{i=1}^{r+b+1} \Pr[\mathcal{E} \cap \Omega_i]$$

Note that if $i > r+1$, then $\Pr[\mathcal{E} \cap \Omega_i] = 0$.

$$= \sum_{i=1}^{r+1} \Pr[\mathcal{E} \cap \Omega_i]$$

$$= \sum_{i=1}^{r+1} \underbrace{\Pr[\mathcal{E} \mid \Omega_i]}_{\text{there should be red balls in first } i-1 \text{ positions, followed by green ball, followed by any red/blue balls}} \cdot \underbrace{\Pr[\Omega_i]}_{1/r+b+1}$$

Simplify this expression?

<u>Approach 2</u>: $S \subseteq \{1, 2, \ldots, r+b+1\}$, $|S| = b+1$.

$$\Omega_S = \text{all permutations of } G\cdot 1,\ R\cdot 1, \ldots, R\cdot r,\ B\cdot 1, \ldots, B\cdot b \text{ s.t. } G\cdot 1,\ B\cdot 1, \ldots, B\cdot b \text{ are at positions in } S.$$

$$\Pr[\mathcal{E}] = \sum_{S : |S| = b+1} \Pr[\mathcal{E} \cap \Omega_S]$$

$$= \sum_{S : |S| = b+1} \underbrace{\Pr[\mathcal{E} \mid \Omega_S]}_{1/b+1} \cdot \Pr[\Omega_S]$$

$$= \frac{1}{b+1} \sum_{S : |S| = b+1} \Pr[\Omega_S] = \frac{1}{b+1}.$$

∎

RANDOM VARIABLES:

Quite often, in a randomized experiment, we are interested in some numerical output of the expt.

Examples: number of heads in n coin tosses

running time of a randomized algorithm.

For this, we define the notion of random variables.

Formally, any $X : \Omega \to \mathbb{R}$ is a random var.

Example: Toss a fair coin n times.
Let X denote the number of heads.

If $n = 3$, then $\Omega =$ HHH HHT HTH HTT THH THT TTH TTT
X: 3 2 2 1 2 1 1 0

For the same sample space, we can define multiple random variables.

Example: For $\Omega = \{HHH\ HHT\ HTH\ HTT\ THH\ THT\ TTH\ TTT\}$,

we can also define Y = first position at which H appears.

Expectation of a random variable:

We are often interested in the 'average value' of a random variable. This is defined as follows:

Let (Ω, p) be a prob. dist. and let X be a random variable.

$$E[X] = \sum_{\omega \in \Omega} X(\omega) \cdot p(\omega).$$

expectation of X

Alternately, we can also express this as follows:
Let $Z = \{ X(\omega) : \omega \in \Omega \}$ and for any $z \in Z$, let
$$X^{-1}(z) = \{ \omega : X(\omega) = z \} \subseteq \Omega .$$

$$E[X] = \sum_{z \in Z} z \cdot \Pr[\underbrace{X^{-1}(z)}]$$

Sometimes, we also write this as "$X = z$". Keep in mind that this is the subset of Ω where all elements map to z.

Example: unbiased coin is tossed n times
X : number of heads.

$$X : \Omega \to \{0, 1, \dots, n\}$$

For any $i \in \{0, 1, \dots, n\}$,

$$\Pr[X^{-1}(i)] = \binom{n}{i} 2^{-n}$$

$$\therefore E[X] = \sum_{i=0}^{n} i \cdot \binom{n}{i} 2^{-n}$$

simplify this expression?

Given any k random variables $X_1, X_2, \dots, X_k$ we can define a new random variable Y that is the sum of $X_1, X_2 \dots X_k$. More formally let $Y : \Omega \to \mathbb{R}$ s.t. $\forall\, \omega \in \Omega$,

$$Y(\omega) = X_1(\omega) + X_2(\omega) + \dots + X_k(\omega).$$

$$E[Y] = \sum_{\omega \in \Omega} Y(\omega) \cdot p(\omega)$$

$$= \sum_{\omega \in \Omega} \big(X_1(\omega) + \dots + X_k(\omega)\big) \cdot p(\omega)$$

$$= \sum_{\omega \in \Omega} X_1(\omega) \cdot p(\omega) + \dots + \sum_{\omega \in \Omega} X_k(\omega) \cdot p(\omega)$$

$$= E[X_1] + \dots + E[X_k].$$

Linearity of Expectation:

$$E[X_1 + \dots + X_k] = E[X_1] + \dots + E[X_k].$$

This simple fact is very very useful. Can often simplify our calculations.

Example: unbiased coin is tossed n times

X : number of heads.

Let $X_i = \begin{cases} 1 & \text{if } i^{th} \text{ toss is H} \\ 0 & \text{otherwise.} \end{cases}$

Then $X = X_1 + X_2 + \cdots + X_n$.

For any i, $E[X_i] = 0 \cdot \Pr[X_i^{-1}(0)] + 1 \cdot \Pr[X_i^{-1}(1)]$

$\Pr[X_i^{-1}(0)] = \Pr[i^{th} \text{ coin toss is T}] = 1/2$

$\Pr[X_i^{-1}(1)] = \Pr[i^{th} \text{ coin toss is H}] = 1/2$

Therefore $E[X_i] = 1/2$.

Using lin. of expectation, $E[X] = n/2$.

$\blacksquare$

SUMMARY :

- Conditional prob. $\Pr[A \mid B] = \dfrac{\Pr[A \cap B]}{\Pr[B]}$.

- Law of total prob. : Let $\Omega_1 \cdots \Omega_t$ be partitioning of sample space.

$$\Pr[A] = \sum \Pr[A \mid \Omega_t] \cdot \Pr[\Omega_t]$$

Appropriate partitioning can make the calculations/ analysis easier.

- Random variable $X : \Omega \to \mathbb{R}$

Expectation of rand. var
$$E[X] = \sum X(\omega) \cdot p(\omega)$$
$$= \sum z \cdot \Pr[X^{-1}(z)]$$

- Linearity of expectation

$$E[X_1 + \dots + X_k] = E[X_1] + \dots + E[X_k]$$

Random variables can be decomposed as sum of simpler r.v.s in several ways. Appropriate decomposition can simplify the analysis.

PRACTICE PROBLEMS :

1. An unbiased coin is tossed n times.
   X : number of occurences of TTH.
   eg. if $n = 8$, $\omega = TTTHHTTH$ then $X(\omega) = 2$.
   Compute $E[X]$.

2\. A jar has n blue balls
n green balls
n red balls
n yellow balls.

5 balls are drawn, unif. at rand, without replacement.

$$\Pr\left[\begin{array}{c}\text{there are at most 2 distinct}\\ \text{colors in the sampled set}\end{array}\right]$$

for n > 5 : (4,2)((n,0)(n,5) + (n,1)(n,4) + .. (n,5)(n,0))/(4n,5)

3\. Problem 18.15 from [LLM18]

4\. Let $n \in \mathbb{N}$, $\ell = 4n$. Let $x_1, x_2 \in \{0,1\}^n$ be two fixed strings in $\{0,1\}^n$.
Let f be a uniformly random function $f : \{0,1\}^n \to \{0,1\}^\ell$.

One way to sample a unif. rand. fn. is as follows: for each $x \in \{0,1\}^n$, sample a unif. rand. y from $\{0,1\}^\ell$, set $f(x) = y$.

Let X be a random variable denoting the number of positions where $f(x_1) \neq f(x_2)$.

What is $E[X]$?