Foundations of Privacy — Fall 2022
Homework 0: Due Sunday, September 10th, 2023, 11:59 PM

Overview

This homework is ungraded. Rather, it is designed to give you a sense of how comfortable you are with various aspects of probability theory. Probability theory can be a tricky subject, but it is ultimately at the heart of understanding theoretical aspects of privacy. You are not expected to know how to solve all of the following problems, but you should know how to solve at least a few. You should submit at least 5 of the problems on Canvas so that the course staff can get a sense of your familiarity with probability. (For example, problem 1 (a) counts as one problem.) Questions marked with * are trickier, but provide extra insight into the topics being covered.

Submission instruction. You are required to type up the homework in LaTeX and submit the pdf on Canvas.

1. **Expectation and Variance**

   The notions of *expected value* and *variance* are central in the study of probability. Expected value, roughly, gives a sense of the "center" of a probability distribution. For a discrete random variable X (that is, a random variable which takes on at most countably many values), expected value is defined as $\mathbb{E}[X] = \sum_{x \in \Omega} x \mathbb{P}(X = x)$, where $\Omega \subset \mathbb{R}$ is some at most countable set. For a continuous random variable Y with density $f(x)$, the expectation is given by $\mathbb{E}[Y] = \int_{\mathbb{R}} x f(x) dx$.

   The variance of a random variable X (either continuous or discrete) is given by $Var[X] = \mathbb{E}(X - \mathbb{E}[X])^2$. Roughly, the variance tells us how spread out a distribution is with respect to its center. Please try to answer the following questions about expected value and variance.

   (a) Let X be a random variable. Show that the variance of X can be expressed as $Var[X] = \mathbb{E}[X^2] - \mathbb{E}[X]^2$.

   (b) Suppose X and Y are *independent random variables*, i.e., for any events $A, B \subset \mathbb{R}$, we have

   $$\mathbb{P}(X \in A, Y \in B) = \mathbb{P}(X \in A)\mathbb{P}(Y \in B)$$

   (In terms of densities, if $f(x, y)$ is the joint density of X and Y, independence implies $f(x, y) = f_X(x)f_Y(y)$, where f_X and f_Y are the marginal densities of X and Y). Show that $\mathbb{E}[XY] = \mathbb{E}[X]\mathbb{E}[Y]$.

   (c) Suppose X, Y are independent random variables. Show that $Var[aX + bY] = a^2 Var[X] + b^2 Var[Y]$. (The previous part should be useful).

   (d) Let X be a random variable. Which constant $B \in \mathbb{R}$ minimizes $\mathbb{E}\left[(X - B)^2\right]$? What does this say about $\mathbb{E}[X]$ as a measure of the center of the distribution of X?

   (e) Lastly, suppose $X_1, \ldots, X_n$ are independent random variables with mean μ and variance σ^2. Define the *sample average* to be $\overline{X} = \frac{1}{n}(X_1 + \cdots + X_n)$. What is $\mathbb{E}[\overline{X}]$? What about $Var[\overline{X}]$?

   (f) * Suppose X is a non-negative random variable. Show we have the equivalence $\mathbb{E}[X] = \int_0^\infty \mathbb{P}(X > t)dt$.

   (g) * Now, which constant $B \in \mathbb{R}$ minimizes $\mathbb{E}\left[|X - B|\right]$?

2. **Key Distributions**

   There are many important distributions which play a central role in fields such as differential privacy, statistics, and machine learning. While you may have heard of the following distributions, it is always good to brush up on key properties.

(a) Suppose we toss one biased coin with probability of heads $p \in (0, 1)$. Let $X = 1$ if the coin turns up heads, $X = 0$ if the coin lands tails. What is $\mathbb{E}[X]$? What about $Var[X]$? X is said to be a Bernoulli random variable with probability of success p. We write $X \sim Ber(p)$.

(b) Now, suppose we toss n independent coins, each of which has probability p of turning up heads. Let N denote the number of heads out of the n tosses. What is $\mathbb{P}(N = k)$, for $k = 0, 1, \ldots, n$? What is $\mathbb{E}[N]$? What about $Var[N]$? (Hint: these last two points can be solved easily with the previous question). Such a random variable is said to be Binomially distributed with n trials and probability of success p. We write $X \sim Bin(n, p)$ correspondingly.

(c) Instead of tossing a fixed number of coins, you now toss independent coins until you see the first heads, where p is still the probability that any given coin lands heads up. Let N represent this number of tosses. What is $\mathbb{P}(N = n)$ for $n \in \mathbb{N}$? Likewise, what is $\mathbb{E}[N]$? $Var[N]$? The random variable with said distribution is said to be *Geometrically distributed with parameter p*. We write this as $N \sim Geo(p)$.

(d) * Now, we talk about some continuous distributions. X is said to be *exponentially distributed with parameter λ* if X has density $f(x) = \lambda e^{-\lambda x}$ for all non-negative x. What is $\mathbb{E}[X]$? What about $Var[X]$? Show, using *Bayes rule*, that $\mathbb{P}(X > t + s | X > s) = \mathbb{P}(X > t)$, for any $s, t \geq 0$. In words, what does this equality say?

(e) * We say X is *normally distributed with mean μ and variance σ^2*, denoted $X \sim N(\mu, \sigma^2)$, if X has density $f(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{\frac{-(x-\mu)^2}{2\sigma^2}}$. Show that if X and Y are independent random variables with $X \sim N(\mu_1, \sigma_1^2)$ and $Y \sim N(\mu_2, \sigma_2^2)$, then $X + Y \sim N(\mu_1 + \mu_2, \sigma_1^2 + \sigma_2^2)$ (Hint: you may need to look up something called *convolution*).

3. **Basic Probability Computations**

The first three sections asked about theoretical aspects of probability theory, but probability is also useful for doing computations! Try your hand at a few of the following problems!

(a) Suppose you roll 3 dice consecutively. What is the probability that the values shown by the dice are in *strictly* increasing order?

(b) Suppose there is a 50 percent chance that it rains on any given day. Moreover, assume that whether or not it rains on any given day is independent of whether or not it will rain on any other given day. What is the probability that it rains at least once in a 7 day week.

(c) Suppose there are 25 people in a room, and each person has their birthday drawn uniformly at random from the 365 days of a year (sorry leap years!). What is the expected number of people that share a birthday with at least one other person?