Section 1: Probability and Asymptotic Notation Review

CS 208 Applied Privacy for Data Science, Spring 2022

February 1, 2022

1 Agenda

- Introductions (go around and say name, year, where you are from, and why you are interested in this class)
- Section logistics (optional but encouraged, counts for participating and helps homework, we will send out poll for timings)
- Probability, bounds, asymptotic notation review
- Some exercises

2 Probability Review

Probability is the chance or likelihood that something is to happen. For example, we might look at the probability that we get 10 heads in a row when flipping a fair coin. The analysis of events governed by probability is called statistics. The elements of probability include the sample space Ω (set of all outcomes in a random experiment), events $A \subseteq \Omega$, event space $\mathcal{F}$ (set of all events, and probability measure $P : \mathcal{F} \to \mathbb{R}$. The probability measure P must follow three rules.

- $0 \leq P(A) \leq 1$, for event $A \in \mathcal{F}$
- $P(\Omega) = 1$
- For disjoint events $A_1, A_2,\;\; P(A_1 \cup A_2) = P(A_1) + P(A_2)$
- **Boole's Inequality/Union Bound**: For any n events $A_1, A_2, \ldots, A_n$,

$$\Pr\left(\bigcup_{i=1}^{n} A_i\right) \leq \sum_{i=1}^{n} \Pr\left(A_i\right).$$

Conditional probability and independence: Let B be an event with non-zero probability. The *conditional probability* of an event A given B is

$$\Pr(A|B) = \frac{\Pr(A \cap B)}{\Pr(B)}$$

A and B are *independent* if and only if $\Pr(A \cap B) = \Pr(A) \cdot \Pr(B)$. Independence is equivalent to saying that observing B does not have any effect on the probability of A.

Random variables, expectation, and variance: A *random variable* X is a function: $X : \Omega \to \mathbb{R}$. For example, $X(\omega)$ could be the number of heads which occur in a series of tosses ω. Then, the probability that 5 heads occur is

$$\Pr(X = 5) := \Pr(\omega : X(\omega) = 5)$$

X can be a discrete random variable (in the example above) or a continuous random variable. Let X be a discrete random variable with probability mass distribution $p_X(x)$. Then, the *expected value* of X is

$$E[X] = \sum_x x \cdot p_X(x)$$

Intuitively, the expectation of a random variable X is a weighted average of all its possible values x. Two properties of expectation:

- $E[X + Y] = E[X] + E[Y]$
- $E[af(X)] = aE[f(X)]$

The *variance* of a random variable X is a measure of the concentration of its distribution around its mean or expected value.

$$Var(X) = E[(X - E(X))^2]$$

Using the properties of expectation listed above, we can derive an alternate equation.

$$Var(X) = E[X^2] - E[X]^2$$

Remember that if two variables X and Y are independent, then $Var(X+Y) = Var(X)+Var(Y)$.

3 Tail Bounds

Claim 3.1 (A Chernoff-Hoeffding Bound)**.** *For $i = 1, \ldots, n$, let X_i be an independent random variable within $[a, b]$ with mean μ. Then,*

$$\Pr\left[\sum_{i=1}^{n} X_i - n\mu \geq t\right] \leq \exp\left(-\frac{2t^2}{n(b-a)^2}\right).$$

Claim 3.2 (Laplace Tail Bound)**.** *Let Z be a Laplace random variable with mean 0 and scale b (variance $2b^2$). Then for every $t > 0$,*

$$\Pr[Z > t] = \frac{1}{2}e^{-t/b}, \quad \Pr[|Z| > t] = e^{-t/b}.$$

Claim 3.3 (Gaussian Tail Bound)**.** *Let Z be a standard normal random variable with mean 0 and variance 1. Then for every $t > 0$,*

$$\Pr[Z > t] \leq \exp(-t^2/2).$$

3.1 Exercises

1. Suppose you independently flip 15 fair coins, what is the probability that you get 5 heads?

   Solution:

$$\Pr[5 \text{ heads}] = \binom{15}{5}(0.5)^5(0.5)^{10}$$

2. Let $X_1, \ldots, X_n$ be independent $\{0,1\}$-valued Bernoulli random variables where $\Pr[X_i = 1] = p$ for all $i \in [n]$ (e.g., coin tosses where the probability of heads is p). How large does n need to be to make sure that the mean of observed outcomes (i.e., $\frac{1}{n}\sum_{i=1}^{n} X_i$) is within ϵ of p with probability at least 0.9?

   Solution:

$$\Pr\left[\left|\frac{1}{n}\sum_{i=1}^{n} X_i - p\right| \geq \epsilon\right] \leq 2\exp\left(-2\epsilon^2 n\right) < 0.1$$

$$n > \ln(20)/(2\epsilon^2)$$

3. Let X be a Gaussian random variable with mean 0 and standard deviation 1. What is the probability that X is greater than 4?

   Solution:

$$\Pr\left[X > 4\right] \leq \exp\left(-16/2\right) = \frac{1}{e^8}$$

4. Let X be a Laplace random variable with mean 0 and scale of s. What is the probability that X is greater than $4\sqrt{2}s$?

   Solution:

$$\Pr\left[X > 4\sqrt{2}s\right] = \frac{1}{2}\exp\left(-4\sqrt{2}s/s\right) = \frac{1}{2e^{4\sqrt{2}}}$$

4 Asymptotic Notation Review

In asymptotic analysis, we ask: how does a function $f(n)$ behave as its input size n goes to infinity? Here are the different ways to classify the growth rate of a function.

- **Big-O (upper bound):** $f(n) = O(g(n))$ if and only if there exists constants c and N such that for all $n \geq N$,

$$0 \leq f(n) \leq c \cdot g(n).$$

- **Little-o (strict upper bound):** $f(n) = o(g(n))$ if and only if

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0.$$

- **Big-Ω (lower bound):** $f(n) = \Omega(g(n))$ if and only if there exists constants c and N such that for all $n \geq N$,
$$0 \leq c \cdot g(n) \leq f(n).$$
- **Little-ω (strict lower bound):** $f(n) = \omega(g(n))$ if and only if
$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = \infty.$$
- **Θ (tight bound):** $f(n) = \Theta(g(n))$ if and only if $f(n) = O(g(n))$ and $f(n) = \Omega(g(n))$.

4.1 Exercises

1. Let $f(n) = 3n^2 + 2n + 5$. Is $f(n) = O(n^2)$?
2. Let $f(n) = 3n^2 + 2n + 5$. Is $f(n) = o(n^2)$?
3. Let $f(n) = 2.5^n$. Is $f(n) = o(3.5^n)$?
4. Let $f(n) = 500 \log n^{100}$. Is $f(n) = O(0.5 \log n)$?
5. Let $f(n) = 1.01^{n/100}$. is $f(n) = \omega(n^{900})$?