CS3236: Tutorial 0
(Probability Review)

1. **[Expectation, Independence, and Variance]**

   Let V and W be discrete random variables defined on some probability space with a joint probability mass function (PMF) $P_{V,W}(v, w)$

   (a) Prove that $\mathbb{E}[V + W] = \mathbb{E}[V] + \mathbb{E}[W]$. Do not assume independence.

   (b) Prove that if V and W are independent random variables, then $\mathbb{E}[VW] = \mathbb{E}[V]\mathbb{E}[W]$.

   (c) Let V and W be independent rv's and σ_V^2 and σ_W^2 are their respective variances. Find the variance of $Z = V + W$.

2. **[Modulo-2 Sum]**

   Let $X_1, X_2, \ldots, X_n$ be a sequence of n binary independent and identically distributed (i.i.d.) random variables. Assume that $\Pr(X_m = 1) = \Pr(X_m = 0) = 1/2$ for all $1 \leq m \leq n$. Let Z be a parity check on $X_1, \ldots, X_n$, i.e. $Z = X_1 \oplus \ldots \oplus X_n$ (where $0 \oplus 0 = 0, 0 \oplus 1 = 1$ and $1 \oplus 1 = 0$).

   (a) Is Z independent of X_1? (Assume $n > 1$)

   (b) Are $Z, X_1, \ldots, X_{n-1}$ independent?

   (c) Are $Z, X_1, \ldots, X_n$ independent?

   (d) Is Z independent of X_1 if $\Pr(X_m = 1) \neq 1/2$? (You may take $n = 2$ here)

3. **[Coin Flips]**

   Flip a fair coin four times. Let X be the number of Heads obtained, and let Y be the position of the first Heads (e.g., if the sequence of coin flips is TTHT, then $Y = 3$; if it is THHH, then $Y = 2$). If there are no heads in the four tosses, then we define $Y = 0$.

   (a) Find the joint PMF of X and Y;

   (b) Using the joint PMF, find the marginal PMF of X

4. **[Probability Properties and Bounds]**

   (a) For a nonnegative integer-valued rv N, show that $\mathbb{E}[N] = \sum_{n>0} \Pr(N \geq n)$.

(b) Derive the Markov inequality, which says that for any $a > 0$ and nonnegative X, $\Pr(X \geq a) \leq \mathbb{E}[X]/a$. *(Hint: Let $\mathbf{1}\{\cdot\}$ be the indicator function, which equals one if the condition inside is true and zero otherwise. Use the inequality $\mathbf{1}\{x \geq a\} \leq x/a$ for any $x \geq 0$, which is easily verified by checking the cases $x \geq a$ and $x < a$ separately.)*

(c) Derive the Chebyshev inequality, which says that $\Pr(|Y - \mathbb{E}[Y]| \geq b) \leq \sigma_Y^2/b^2$.

(d) **Weak Law of Large Numbers**: Let $X_1, \ldots, X_n$ be a sequence of i.i.d. rvs with zero-mean and finite variance σ^2. Show that for any $\epsilon > 0$, $\Pr\left[\frac{1}{n}(X_1 + \ldots + X_n) > \epsilon\right] \leq \sigma^2/(n\epsilon^2)$.

(Hint: What can we say about the variance of the random variable $\frac{1}{n}(X_1 + \ldots + X_n)$ as n becomes large?)

5. **[Modulo-M Sum]**

Let X be a random variable uniformly distributed over $\{0, 1, 2, \ldots, M-1\}$. Let Y be a random variable arbitrarily distributed over $\{0, 1, 2, \ldots, M-1\}$, and independent of X. Show that the sum of X and Y modulo M is uniformly distributed and independent of Y.

6. **[Presidential Poll]**

A couple of weeks before the presidential election, ECC News conducts a poll on the three candidates h, t, and j, based on two criteria: winning the election E via the electoral college, and winning the popular votes V. The joint probability distribution of the result is given below:

$$P_{EV}(E = h, V = h) = 0.154$$
$$P_{EV}(E = h, V = t) = 0.179$$
$$P_{EV}(E = h, V = j) = 0.092$$
$$P_{EV}(E = t, V = h) = 0.254$$
$$P_{EV}(E = t, V = t) = 0.134$$
$$P_{EV}(E = t, V = j) = 0.016$$
$$P_{EV}(E = j, V = h) = 0.028$$
$$P_{EV}(E = j, V = t) = 0.001$$
$$P_{EV}(E = j, V = j) = 0.142$$

where E and V are the random variables; and h, t and j are the outcomes.

(a) Determine the marginal probability P_V.

(b) Are the events candidate j winning the election ($E = j$), but candidate h winning the popular votes ($V = h$) independent? Give the reason

(c) Are the random variables E and V independent?

(d) What is the probability that the candidate t wins the election, given that he does not win the popular vote?

7. **[Sending Files Over a Noisy Channel]**

You are given a huge set of files. Your job is to send those to the ISS (International Space Station). Each of the files is encoded using one of the three different encoding algorithms: A, B, and C. Unfortunately, your lab partner forgot to annotate those encoded files based on the algorithms used after encoding them. All you know is one-third of the files are encoded using algorithm A, half using B, and one-sixth using C. It is known that using algorithm A, the chance that a file is received corrupted is 0.35. Similarly, if algorithm B or C is used, the probability is 0.32 and 0.13, respectively.

(a) You pick a file and send it to the ISS. What is the probability that the file is received uncorrupted?

(b) ISS reports that they successfully received an uncorrupted file. What is the probability that the file is encoded using algorithm B?

8. **(Advanced) [Proving Existence Properties Using Probability]**

   (a) Let $\mathcal{M} = \{0, 1, \ldots, N^2 - 1\}$ for some positive integer N, and let $\mathcal{A}$ be a subset of $\mathcal{M}$ of size N. Show that there exists a subset $\mathcal{B}$ of $\mathcal{M}$ of size at most N such that the set $\mathcal{C} = \{a+b \mod N^2 | a \in \mathcal{A}, b \in \mathcal{B}\}$ has cardinality at least $\frac{N^2}{2}$.
   (Hint: Place N items in the set $\mathcal{B}$ uniformly at random with replacement, and study the average number of integers in $\mathcal{M}$ but not $\mathcal{C}$. The inequality $(1 - 1/n)^n < \frac{1}{e}$ is also useful, as is linearity of expectation.)

   (b) Let $x_1, x_2, \ldots, x_n$ be real numbers (not all zero) such that $x_1 + \cdots + x_n = 0$. Show that there is a permutation $y_1, \ldots, y_n$ of $x_1, \ldots, x_n$ such that $y_1 \cdot y_2 + y_2 \cdot y_3 + \cdots + y_n \cdot y_1 < 0$.
   (Hint: Choose a random permutation and consider the expectation $\mathbb{E}[y_k \cdot y_{k+1}]$ of the product of a consecutive pair. Again use linearity of expectation.)

9. **[Repetition Repetition Repetition Code]**

   Consider the repetition code R_4 over the alphabet $\mathcal{A} = \{1, 2, 3\}$, and the majority-vote decoder (maximum likelihood decoder).

   (a) List all the received codewords that will be uniquely decoded as 2222. (Here the "unique" requirement means that neither 1111 nor 3333 are equally far from the received sequence compared to 2222)

   (b) Suppose the probability of each symbol being flipped to another symbol is f, equally likely for each symbol. An error is said to occur when a codeword is incorrectly decoded. If we adopt a pessimistic viewpoint and assume that an error always occurs when there is a tie in decoding (e.g., 1122 is received, which is equally close to 1111 and 2222), then what is the probability of error p_b of R_4?

Hints

1. Can be done fairly directly via definitions of expectation and variance.

2. Try to check whether $p_{Z|\ldots}(0|\ldots)$ depends on the variables being conditioned on.

3. Can directly count outcomes.

4. In (a) write $\mathbb{E}[N] = \sum_{n=0}^{\infty} nP_N(n)$, note that $nP_N(n) = P_N(n) + \ldots + P_N(n)$ (n times), and try to re-arrange. (c) is a special case of (b). In (d) note $\mathsf{Var}[cX] = c^2 \mathsf{Var}[X]$, and also $\mathsf{Var}[A + B] = \mathsf{Var}[A] + \mathsf{Var}[B]$ for independent RVs.

5. Compare the joint distribution P_{ZY} to the product of marginals $P_Z \times P_Y$.

6. Mostly basic given the definitions of marginals, independence, conditioning, etc.

7. Start with $P(A) \cdot P(U|A) + P(B) \cdot P(U|B) + P(C) \cdot P(U|C)$ and make the relevant substitutions.

8. In (a) let X be the number of integers in $\mathcal{M} \setminus \mathcal{C}$ and let X_j be the indicator random variable for the event that $j \notin \mathcal{C}$, and show that $\mathbb{E}[X_j] < 1/e$ using the hint, and then that $\mathbb{E}[X] < N^2/e$. In (b) let $y = y_1, \ldots, y_n$ be a uniformly random permutation of $x_1, x_2, \ldots, x_n$, define $Y = y_1 \cdot y_2 + y_2 \cdot y_3 + \cdots + y_n \cdot y_1$, and write $\mathbb{E}[Y]$ in terms of the pairwise averages $\mathbb{E}[y_k \cdot y_{k+1}]$.

9. In part (b) the binomial distribution may help.