CS 537: *Randomness in Computing* — Prof. Sofya Raskhodnikova
Boston University — January 27, 2020

Homework 2 – Due Friday, January 31, 2020 at noon

Submit solutions to problems 1-5 on separate sheets. They will be graded by different people.

Page limit You can submit **at most** 1 sheet of paper per problem, even if the problem has multiple parts. If you submit a longer solution for some problem, only the first sheet of paper will be graded.

Reminder Collaboration is permitted, but you must write the solutions *by yourself without assistance*, and be ready to explain them orally to the instructor if asked. You must also identify your collaborators and whether you gave help, received help, or worked something out together. Getting solutions from outside sources such as the Web or students not enrolled in the class is strictly forbidden.

Exercises Please practice on exercises in Chapter 1 of Mitzenmacher-Upfal.

Problems

1. **(Chess board)** Consider an 8×8 chess board in which the rows are numbered from 1 to 8, and likewise for the columns. And, as is usual for a chess board, the squares are alternately colored black and white. The squares of this chess board form the elements of a sample space in which all of the 64 squares on the chess board are equally likely; that is, all have probability $\frac{1}{64}$.

   For each of the following pairs of events A and B, determine if the two events are independent and **prove your answer is correct**:

   (a) A is the event that a white square is chosen and B is the event that a black square is chosen.

   (b) A is the event that a square from an even numbered row is chosen and B is the event that a square from an even numbered column is chosen.

   (c) A is the event that a white square is chosen and B is the event that a square from an even numbered column is chosen.

   Determine if the following three events A, B and C are mutually independent and **prove your answer is correct**:

   (d) A is the event that a square from an even numbered row is chosen, B is the event that a square from an even numbered column is chosen, and C is the event that a white square is chosen.

2. (**Multiple-choice test**) Adam and Bella are taking a multiple choice test, where each question has m choices.

   (a) For each question, Adam either knows the answer or has no clue. If he has no clue, he picks one of the m choices uniformly at random. Let p be the probability that Adam knows the answer. What is the conditional probability that Adam knows the answer to a question, given that he answered it correctly? **Express your answer in terms of m and p.**

   (b) Evaluate the expression you got in part (a) for $m = 5$ and $p = .6$.

(c) For each question, Bella either (i) knows the answer, (ii) can eliminate all but 2 answers, or (iii) has no clue. If she can eliminate all but 2 answers, she pick among the remaining 2 answers uniformly at random. If she has no clue, she picks one of the m choices uniformly at random. Let p_1 be the probability that Bella knows the answer and p_2 be the probability that she can eliminate all but 2 answers. What is the conditional probability that Bella knows the answer to a question, given that she answered it correctly? **Express your answer in terms of m, p_1 and p_2.**

(d) Suppose $m = 5$ and $p_2 = .1$. If your expression in part (c) evaluates to the same value as what you got in part (b), what is p_1? (Think, but do not hand in: Is it higher or lower than .6? Can you explain why?)

3. (**Random subsets**)

(a) We generate a subset X of set $[n]$ as follows: a fair coin is flipped independently for each element of the set; if the coin lands heads then the element is added to X, and otherwise it is not. Argue that the resulting set X is equally likely to be any one of the 2^n possible subsets.

(b) Suppose that two sets X and Y are chosen independently and uniformly at random from all the 2^n subsets of $[n]$. Determine $\Pr[X \subseteq Y]$. *Hint: Use part (a).*

(c) Suppose that three sets X, Y and Z are chosen independently and uniformly at random from all the 2^n subsets of $[n]$. Let E be the event that each element from $X \cup Y \cup Z$ appears in at least two of the three sets. Determine the probability of E.

4. (**Verifying matrix multiplication**)

(a) Recall that in the problem of verifying matrix multiplication, we are given $n \times n$ matrices A, B, C, and we want to check whether $A \cdot B = C$. Your friend Max proses the following algorithm for the problem: *Let $D = A \cdot B - C$. Pick i and j uniformly and independently from $[n]$ and compute D_{ij}. Accept if D_{ij} is 0 and reject otherwise.*

i. Give the best upper bound you can on the probability that this algorithm accepts incorrectly (for a worst-case input).

ii. Give the best upper bound you can on the number of independent runs of this algorithm you need to ensure that the error probability is at most 1/3.
Hint: Use the inequality $1 - x \leq e^{-x}$.

iii. State the running time of the resulting algorithm (with the number of runs you specified) using asymptotic notation.

(b) In the algorithm from class for verifying matrix multiplication, we chose a uniformly random vector $\bar{r}$ from $\{0, 1\}^n$. Suppose we choose $\bar{r}$ from $\{0, 1, \ldots, v - 1\}^n$ instead. Prove a better bound (than 1/2) on the probability of success of one check performed by the algorithm.

(c) Suppose your prior belief is that a given matrix multiplication identity is correct with probability 1/2. The analysis that starts at the bottom of page 11 of the textbook demonstrates how your prior belief about the probability that the identity is correct changes after i runs of the algorithm that do not find any mistakes. Modify this analysis to work with your bound from part (b).

5* **(Optional, no collaboration)** We pick a uniformly random permutation $a_1, a_2, \ldots, a_n$ of the numbers in $[n]$. What is the probability that this permutation satisfies $a_i \geq i - 3$ for all i?