Midterm 2

7:00-9:00pm, 15 November

Instructions

1. This is a closed-book exam; however, you may use one single-sided $8.5'' \times 11''$ sheet of notes. Electronic devices are not permitted.
2. There are **five** questions on this exam. Answer each question part in the space below it, using the back of the sheet to continue your answer if necessary. If you need more space, use the blank sheet at the end.
3. None of the questions requires a very long answer, so avoid writing too much! Unclear or long-winded solutions may be penalized.
4. Show all your work!
5. This is not an arithmetic test. For answers requiring a numerical value, you should simplify the expression as far as you can *without* doing heavy arithmetic.
6. The approximate credit for each question part is shown in the margin (total 60 points). Points are not necessarily an indication of difficulty!

Your Name: **Your Section:**

For official use; please do not write below this line!

Q1	
Q2	
Q3	
Q4	
Q5	
Total	

[exam starts on next page]

1. Quick Questions [12pts]

(a) You are given three coins: one is fair, one comes up Heads with probability 1/3 (and Tails with probability 2/3), and the third comes up Heads with probability 2/5 (and Tails with probability 3/5). You pick a coin uniformly at random and toss it once. Depict the sample space as a tree and show the probability of each sample point. *4pts*

(b) Of the students in a class, 60% are geniuses, 70% love chocolate, and 40% fall into both categories. What is the probability that a randomly selected student is *neither* a genius *nor* a chocolate lover? *4pts*

(c) In a parking lot, there are 15 spaces of which 10 are occupied. Assuming that the cars occupy randomly chosen spaces, what is the probability that there are five adjacent vacant spaces? [NOTE: You may leave your answer in terms of factorials.] *4pts*

[continued on next page]

2. Which key? [10pts]

10pts

You are trying to open the door of a storeroom in your office building, but you don't know which of the 18 keys on the office key-ring does the job. You judge the probability that any particular key is the right one as 5% (so there is a 10% chance that none of the keys works). Suppose that you start trying the keys systematically one at a time, and that you have not found the correct key after trying the first k keys (where $0 \leq k \leq 17$). Let p_k denote the probability that the next key you try is the correct one, and let q_k denote the probability that *some* subsequent key will be the correct one. Find formulas for p_k and q_k, as a function of k. Explain your calculation. [NOTE: You should *not* attempt to compute p_k and q_k for each k separately; instead, you should give a general formula for p_k and q_k, valid for all k.]

[continued on next page]

3. Go Bears! [12pts]

In this question you are asked to count various configurations. In all cases you should explain your answer. You may leave your answers in terms of factorials.

(a) How many *distinct* arrangements of the eleven letters in the word "*calfootball*" are there? [NOTE: In such arrangements, multiple occurrences of the same letter—such as the three "*l*"s—are indistinguishable; i.e., two arrangements of the letters that differ only by permutations of the "*l*"s are *not* distinct.] *4pts*

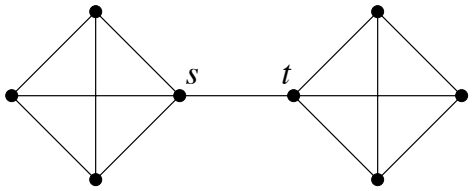
(b) How many distinct arrangements are there in which the substring "*tab*" does not occur? *4pts*

(c) How many distinct arrangements are there in which no pair of "*l*"s appear next to each other? *4pts*

[continued on next page]

4. Euler and Hamilton [14pts]

For each $n \geq 3$, the "barbell" graph BB_n consists of two copies of the *complete* graph K_n on n vertices, joined by a single edge $\{s, t\}$. [Recall that the complete graph is an undirected graph in which every pair of vertices is joined by an edge.] For example, here is a picture of BB_n for $n = 4$:



When answering the questions below, you may use without proof any result covered in class or a homework provided it is clearly stated.

(a) How many vertices and edges does BB_n have? *2pts*

(b) For which values of n does BB_n have a Hamiltonian cycle? Explain. *3pts*

(c) For which values of n does BB_n have a Hamiltonian path? Explain. *3pts*

(d) For which values of n does BB_n have an Eulerian tour? Explain. *3pts*

(e) For which values of n does BB_n have an Eulerian path? Explain. *3pts*

[continued on next page]

5. Secret sharing [12pts]

Consider the problem of sharing a secret s amongst five people so that any three people can determine the value of the secret but any two cannot. As discussed in class, we do this by choosing a degree-2 polynomial P over $GF(q)$ (for suitable q) so that $P(0) = s$, and distributing shares $P(i)$ to person i for $1 \leq i \leq 5$.

(a) Suppose $q = 7$ and the shares obtained by the first three people are $P(1) = 3$, $P(2) = 2$ and $P(3) = 3$. What is the secret? Show your working clearly. *6pts*

(b) A secret-sharing scheme as above is called *2-secure* if and only if any group of two or fewer people has *no information* about the secret, in the sense that every one of the q possible values for the secret is consistent with the information they have. Explain briefly why the above scheme is indeed 2-secure. *3pts*

(c) Suppose now that $q = 5$. Why would the above secret-sharing scheme not be effective with this value of q? Be as precise as you can. *3pts*

[The end]