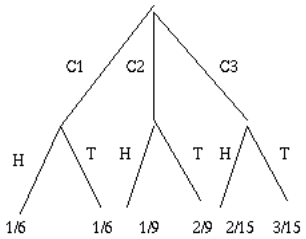
Midterm 2 Solutions

Note: These solutions are not necessarily model answers. Rather, they are designed to be tutorial in nature, and sometimes contain more explanation (occasionally much more) than an ideal solution. Also, bear in mind that there may be more than one correct solution. The maximum total number of points available is 60.

1. Quick Questions [12pts]

(a) The probability space is as follows: *4pts*



Almost all students got this question right.

(b) $\Pr[\overline{\text{genius}} \cap \overline{\text{love chocolate}}] = \Pr[\overline{\text{genius} \cup \text{love chocolate}}] = 1 - \Pr[\text{genius} \cup \text{love chocolate}]$. By the inclusion-exclusion principle, $\Pr[\text{genius} \cup \text{love chocolate}] = \Pr[\text{genius}] + \Pr[\text{love chocolate}] - \Pr[\text{genius} \cap \text{love chocolate}] = 0.6 + 0.7 - 0.4 = 0.9$. Therefore, $\Pr[\overline{\text{genius}} \cap \overline{\text{love chocolate}}] = 1 - \Pr[\text{genius} \cup \text{love chocolate}] = 1 - 0.9 = 0.1$. *4pts*

Almost all students got this question right. Some students drew a Venn diagram instead of algebraically invoking the inclusion-exclusion principle.

(c) There are only 11 ways to place the five adjacent spaces, corresponding to the situations of having 0-10 cars to the left of the spaces. There are $\binom{15}{5}$ ways to place the spaces if they are not required to be adjacent. Since all arrangements of the cars are equally probable, we can just take the ratio of these numbers to get the probability. Thus the desired probability is *4pts*

$$\frac{11}{\binom{15}{5}} = \frac{11 \times 10! \times 5!}{15!}.$$

.

There were many varied answers to this part. It is also possible, though more difficult, to solve this problem by considering the cars to be labeled and then finding the ratio of number of arrangements of labeled cars with five adjacent spaces to the total number of possible arrangements of labeled cars. Of course, the answer is the same as above. One of the common mistakes seemed to be mixing these two sample spaces, by taking the number of arrangements of distinct cars in the numerator and the number of ways of placing the spaces in the denominator.

2. Which key? [10pts]

Let A_k be the event that the kth key is the one that opens the door. Then *10pts*

$$\begin{aligned} p_k &= \Pr[A_{k+1}, \mid \overline{A_1} \cap \overline{A_2} \cap \ldots \cap \overline{A_k}\,] \\ &= \frac{\Pr[A_{k+1} \cap \overline{A_1} \cap \overline{A_2} \cap \ldots \cap \overline{A_k}]}{\Pr[\overline{A_1} \cap \overline{A_2} \cap \ldots \cap \overline{A_k}]} \\ &= \frac{\Pr[A_{k+1}]}{1 - \Pr[A_1 \cup A_2 \cup \ldots \cup A_k]} \\ &= \frac{\Pr[A_{k+1}]}{1 - (\Pr[A_1] + \Pr[A_2] + \ldots + \Pr[A_k])} \\ &= \frac{0.05}{1 - 0.05k} = \frac{1}{20 - k}. \end{aligned}$$

In the second line here we used the definition of conditional probability. In the fourth line we used the fact that the events A_i are disjoint, and in the fifth line we used the fact that $\Pr[A_i] = 0.05$ for each i.

To compute q_k we proceed similarly as follows:

$$\begin{aligned} q_k &= \Pr[A_{k+1} \cup A_{k+2} \cup \ldots \cup A_{18} \mid \overline{A_1} \cap \overline{A_2} \cap \ldots \cap \overline{A_k}] \\ &= \frac{\Pr[(A_{k+1} \cup A_{k+2} \cup \ldots \cup A_{18}) \cap \overline{A_1} \cap \overline{A_2} \cap \ldots \cap \overline{A_k}]}{\Pr[\overline{A_1} \cap \overline{A_2} \cap \ldots \cap \overline{A_k}]} \\ &= \frac{\Pr[A_{k+1} \cup A_{k+2} \cup \ldots \cup A_{18}]}{1 - \Pr[A_1 \cup A_2 \cup \ldots \cup A_k]} \\ &= \frac{\Pr[A_{k+1}] + \Pr[A_{k+2}] + \ldots + \Pr[A_{18}]}{1 - (\Pr[A_1] + \Pr[A_2] + \ldots + \Pr[A_k])} \\ &= \frac{(0.05)(18 - k)}{1 - 0.05k} = \frac{18 - k}{20 - k}. \end{aligned}$$

Most students had difficulty with this problem. Many simply guessed a formula intuitively and then tried to explain why their guess should be correct. Some thought that the probability of a key working was independent of the probabilities of the other keys working and tried to multiply probabilities. (Note that if, e.g., the first key does not work, then the conditional probability of the second key working is higher.) Others seemed to have few ideas for approaching the problem.

3. Go Bears! [12pts]

(a) The number of distinct arrangements is $\boxed{\frac{11!}{3!2!2!}}$. *4pts*

There are 11 letters, so there are 11! arrangements if all letters are different. However, since there are three l's, two a's, and two o's, we must divide 11! by 3!2!2! (the number of ways of permuting these sets of equivalent letters) to count the distinct arrangements.

An alternative (messier) solution is: $\binom{11}{3}\binom{8}{2}\binom{6}{2}\binom{4}{1}\binom{3}{1}\binom{2}{1}\binom{1}{1}$, which if you expand out all the binomial coefficients and cancel you will see evaluates to the same value as above. This is derived as follows:

1. Choose three spots from 11 spots for the letter l
2. Choose two spots from the remaining 8 spots for the letter a
3. Choose two spots from the remaining 6 spots for the letter o
4. Choose one spot from the remaining 4 spots for the letter f
5. Choose one spot from the remaining 3 spots for the letter c
6. Choose one spot from the remaining 2 spots for the letter t
7. Choose one spot from the remaining 1 spots for the letter b

Almost everybody got this part right.

(b) The number of distinct arrangements is $\boxed{\frac{11!}{3!2!2!} - \frac{9!}{3!2!}}$. *4pts*

We first count the number of distinct arrangements that do contain the substring *tab* : treating *tab* as a super-letter, we see that there are 9! such arrangements if we regard all letters as different; however, as in part (a) we must divide by 3!2! to account for the repeated l's and o's. Finally, we subtract the result from the total number of arrangements computed in part (a).

Alternative solution: $9 \times \binom{8}{3}\binom{5}{2}\binom{3}{1}\binom{2}{1}\binom{1}{1}$ (which after some arithmetic can be seen to be equal to the above expression). This is derived in similar fashion to the alternative solution for part (a).

A common mistake here was to overlook the fact that tab already contains an a, and hence to incorrectly divide the number of arrangements containing tab by an extra 2!.

(c) The number of distinct arrangements is $\boxed{\frac{11!}{3!2!2!} - \frac{10!}{2!2!} + \frac{9!}{2!2!}}$. *4pts*

Similar to part (b), think of a pair of l's as a super letter; we will then have $\frac{10!}{2!2!}$ arrangements that contain a pair of l's next to each other. However, notice that this number includes the arrangements with three adjacent l's counted *twice*! (Think of how a sequence of three l's contains two pairs of adjacent l's.) Therefore, we have to add back in the number of arrangements with three adjacent l's, which is $\frac{9!}{2!2!}$. (This is really an application of the inclusion-exclusion principle.) This gives us the final answer above.

Many students partially solved this problem but overlooked the fact about the number of arrangements with three l's next to each other.

Alternative solution (which in this case is actually neater): $\boxed{\binom{9}{3}\frac{8!}{2!2!}}$.

(Again, with some arithmetic this can be seen to have the same value as the solution above.) To see this alternative solution, let's use X to denote any non-l letter. To count all arrangements in which no pair of l's appear next to each other, we will introduce the notion of "separators", which, in order of appearance in the arrangement, are: $\boxed{\text{LX}}$, $\boxed{\text{LX}}$, $\boxed{\text{L}}$. All of the other six letters (all non-l's) are placed between the separators. Here are some possible example placements:

- XX $\boxed{\text{LX}}$ XX $\boxed{\text{LX}}$ XX $\boxed{\text{L}}$ X
- XXXXXX $\boxed{\text{LX}}$ $\boxed{\text{LX}}$ $\boxed{\text{L}}$
- $\boxed{\text{LX}}$ XXX $\boxed{\text{LX}}$ $\boxed{\text{L}}$ XXX

Since we force the first two separators to consist of an l followed by a non-l, any placement of these nine symbols with the separators in the given order guarantees that no pair of l's are next to each other. Moreover, any arrangement in which no pair of l's are next to each other corresponds to exactly one such placement (since each of the first two l's to occur must have at least one non-l letter following it). Thus, we can just count such placements. First, we choose 3 locations out of 9 for the separators. Once the separators are placed, there are 8 spots (each denoted by X) to be filled in; this gives us 8! possibilities. However, since we have two o's and two a's, this number must be divided by 2!2!. This gives us the alternative solution above.

4. Euler and Hamilton [14pts]

(a) Clearly BB_n has $2n$ vertices. For the number of edges, note first that the number of edges in a complete graph on n vertices is $\binom{n}{2}$, so the number of edges in BB_n is $2\binom{n}{2} + 1 = n(n-1) + 1$. *2pts*

Almost everybody got this part right.

(b) BB_n does not have a Hamiltonian cycle for any value of n. To see this, suppose without loss of generality that the cycle starts in the left-hand copy of K_n (the one containing s). At some point the cycle must visit the right-hand copy of K_n, which it can only do by taking the edge $\{s, t\}$. But now the cycle cannot return to its starting point because there is no route back to the left-hand side without revisiting s and t. *3pts*

Again, almost everybody got this right.

(c) BB_n has a Hamiltonian path for all values of n. To get such a path, let u and v be arbitrary vertices on the left and right sides, with $u \neq s$ and $v \neq t$. Starting at u, follow a Hamiltonian path on the left-hand side to s; this is always possible since every vertex is connected to every other. Then follow the edge $\{s, t\}$, and finally follow a Hamiltonian path in the right-hand side from t to v; this exists for the same reason as above. The result is a Hamiltonian path in BB_n from u to v. *3pts*

Most people correctly said that a path exists for all n. However, quite a lot of people lost one or two points for the explanation. The most common error was to not explain how the paths in each of the two sides are glued together into a single path.

(d) BB_n does not have an Eulerian tour for any value of n. One way to see this is by the same argument as in part (b): any cycle would necessarily have to cross the "cut" between the two copies of K_n twice, but there is only one edge $\{s, t\}$ between them. *3pts*

An alternative way is to use Euler's Theorem: an Eulerian tour exists if and only if all vertex degrees are even. But clearly the degrees of s and t are one larger than those of all other vertices, so it is not possible for all vertex degrees to be even.

Most people got this right, using one of the above two arguments.

(e) For $n \geq 3$, BB_n has an Eulerian path if and only if n is odd. To see this, we use a criterion discussed in class and in HW6: a connected graph G has an Eulerian path from vertex u to vertex v *if and only if* u, v have odd degree and all other vertices have even degree. When n is odd, all vertices of BB_n except s and t have even degree, so we have an Eulerian path. When n is even all vertices except s and t have odd degree, so we have no Eulerian path (unless $n = 2$, when there are only two such vertices; but this case is excluded by the assumption $n \geq 3$). *3pts*

An alternative argument is to say that, because of the single "cut" edge $\{s, t\}$, any Eulerian path must consist of an Eulerian tour (starting and ending at s) in the left-hand side, followed by the edge $\{s, t\}$, followed by an Eulerian tour (starting and ending at t) in the right-hand side. But by Euler's Theorem these two Eulerian tours exist *if and only if* all degrees within each K_n are even, which holds if and only if n is odd.

Again, most people obtained the correct range of values of n, but the explanations here were generally weaker than in the other parts. Many people seemed to be confused about the difference between Eulerian tour (which starts and ends at the same vertex) and Eulerian path (which starts and ends at different vertices). Some people just said that the vertices of each K_n all have even degree when n is odd; this misses the key point that s and t also have odd degree. Many people used the alternative argument (gluing together Eulerian tours in the two sides), but as in part (c) some were not precise about how the tours are glued together. Finally, almost nobody gave a convincing argument for why the path exists only *for odd values of n: this requires using the "only if" parts in the two arguments above. We did not deduct points for this omission, but you should be aware of it.*

5. Secret sharing [12pts]

(a) From the secret sharing scheme given in class, we know that the secret is given by $P(0)$, where $P(x)$ is a polynomial over $GF(7)$ satisfying $P(1) = 3$, $P(2) = 2$, and $P(3) = 3$. To find the secret, we first reconstruct $P(x)$. For that, we use *Lagrange Interpolation* over $GF(7)$. We have: *6pts*

$$\Delta_1(x) = \frac{(x-2)(x-3)}{(1-2)(1-3)} = \frac{(x-2)(x-3)}{2}$$
$$\Delta_2(x) = \frac{(x-1)(x-3)}{(2-1)(2-3)} = \frac{(x-1)(x-3)}{-1}$$
$$\Delta_3(x) = \frac{(x-1)(x-2)}{(3-1)(3-2)} = \frac{(x-1)(x-2)}{2}$$

Thus the polynomial $P(x)$ is given by

$$P(x) = \left(3 \times \frac{(x-2)(x-3)}{2}\right) + \left(2 \times \frac{(x-1)(x-3)}{-1}\right) + \left(3 \times \frac{(x-1)(x-2)}{2}\right).$$

Working over $GF(7)$, we know that the inverse of 2 is $2^{-1} = 4$. Replacing it in the expression for $P(x)$, we obtain

$$\begin{aligned} P(x) &= 3 \times 4 \times (x-2)(x-3) - 2(x-1)(x-3) + 3 \times 4 \times (x-1)(x-2) \\ &= 3 \times 4 \times (x^2 - 5x + 6 + x^2 - 3x + 2) - 2x^2 + 8x - 6 \\ &= 22x^2 - 88x + 90 = x^2 + 3x + 6 \pmod 7. \end{aligned}$$

Thus the secret is $s = P(0) = 6$.

(b) First notice that since we are working over $GF(q)$, *a priori* the secret might be any number in $\{0, 1, \ldots, q-1\}$. Now suppose that two people get together to recover the secret. This means they know two points, say, (x_1, y_1) and (x_2, y_2), on the degree-2 polynomial P. Also, the secret is the value $s = P(0)$. But now notice that *any* of the q possible values for the secret s gives us a third point on the polynomial, of the form $(0, s)$. And each of these q possibilities corresponds to a *different* polynomial P (because there is a *unique* polynomial P through any three given points). Hence the information that the two people have is consistent with every possible value of the secret. Thus the scheme is 2-secure. *3pts*

There were a lot of partial responses to this question. Many students just stated the fact that with only two points one cannot uniquely interpolate a degree-2 polynomial. Although this is true, it does not imply that the scheme is 2-secure.

(c) The scheme described above gives the shares $P(i)$ for $1 \leq i \leq 5$ to five people, and the secret is $P(0)$. If we are working over $GF(5)$, this means that one person gets the value $P(5) = P(0)$, which is the secret! So the secret is in fact directly revealed to one person. *3pts*

More generally, if we give *any* five shares to the five people (not necessarily the values $P(1)$, $P(2)$, $P(3)$, $P(4)$ and $P(5)$), then *either* we must give one person the secret $P(0)$, *or* we must give at least two people the same value $P(x)$ for some $x \in GF(5)$. (This is because there aren't enough distinct values in $GF(5)$ to ensure that everybody gets a different share that is also different from the secret.) But in this second case, when those two people get together with a third person, the group has only two distinct points on the polynomial P so they cannot interpolate to find P.

There were a lot of partial responses to this question. Also, many students claimed that the scheme is not effective because the secret found in part (a) was 6, which is larger than q in $GF(5)$. But this is irrelevant because the answer to part (a) assumed we were working over $GF(7)$, not over $GF(5)$. Some students claimed that the polynomial could not be interpolated over $GF(5)$; this is in some cases true, but is a much less precise answer than the one above, which identifies a concrete problem with the scheme.