1 Multiple-choice test

a)

We define AKA the event of Adam knows the answer and CA the event of Adam chooses the correct answer. So the probability we need to calculate is $Pr(AKA|CA)$. If Adam know the answer with probability p, it means $Pr(AKA) = p$ and $Pr(\overline{AKA}) = 1 - p$. Furthermore, if Adam does not have a clue then he answers correctly by choosing uniformly and randomly over m choices, so $Pr(CA|\overline{AKA}) = \frac{1}{m}$. Based on the previous input and with the help of Bayes law we can calculate the $Pr(AKA|CA)$ as following:

$$\begin{aligned}
Pr(AKA|CA) &= \frac{Pr(CA|AKA) * Pr(AKA)}{Pr(CA|AKA) * Pr(AKA) + Pr(CA|\overline{AKA}) * Pr(\overline{AKA})} \\
&= \frac{Pr(CA|AKA) * p}{Pr(CA|AKA) * p + \frac{1}{m} * (1 - p)} \\
&= \frac{1 * p}{1 * p + \frac{1}{m} * (1 - p)}
\end{aligned}$$

b)

Since $m = 5$ and $p = 0.6$ we evaluate the result from (a) as following:

$$\begin{aligned}
Pr(AKA|CA) &= \frac{1 * p}{1 * p + \frac{1}{m} * (1 - p)} \\
&= \frac{1 * 0.6}{1 * 0.6 + \frac{1}{5} * (1 - 0.6)} \\
&= 0.88
\end{aligned}$$

c)

We define BKA the event of Bella knows the answer, EA the event of Bella eliminate all but two answers and NC the event of Bella not know a clue and CA the event of Bella chooses the correct answer. So the probability we need to calculate is $Pr(BKA|CA)$. If Bella knows the answer with probability p_1, it means $Pr(BKA) = p_1$, while if she can eliminate all but two answers it means $Pr(EA) = p_2$ and if she does not have a clue then it means $Pr(NC) = 1 - (p_1 + p_2)$. Furthermore, if Bella does not have a clue then she answers correctly by choosing uniformly and randomly over m choices, so $Pr(CA|NC) = \frac{1}{m}$, while if Bella can eliminate all but two answers then she answers correctly by choosing uniformly over the 2 choices so $Pr(CA|EA) = \frac{1}{2}$. Based on the previous input and with the help of Bayes law we can calculate the

$Pr(BKA|CA)$ as following:

$$\begin{aligned} Pr(BKA|CA) &= \frac{Pr(CA|BKA) * Pr(BKA)}{Pr(CA|BKA) * Pr(BKA) + Pr(CA|EA) * Pr(EA) + Pr(CA|NC) * Pr(NC)} \\ &= \frac{Pr(CA|BKA) * p_1}{Pr(CA|BKA) * p_1 + \frac{1}{2} * p_2 + \frac{1}{m} * (1 - (p_1 + p_2)))} \\ &= \frac{1 * p_1}{1 * p_1 + \frac{1}{2} * p_2 + \frac{1}{m} * (1 - (p_1 + p_2)))} \end{aligned}$$

d)

Bella knows the answer with probability p_1, it means $Pr(BKA) = p_1$. If we assume that $Pr(BKA)$ is neither higher nor lower but it has a value as (b) subquestion equals to $Pr(BKA) = p = 0.6$. Furthermore, the probability of not knowing the answer is described through two events. Either she can eliminate all but two answers $Pr(EA)$ or she has no clue and answers uniformly and randomly above m questions $Pr(NC)$,so $Pr(\overline{BKA}) = Pr(EA) + Pr(NC) = 1 - p = 0.4$.Also we know that:

$$Pr(CA) = Pr(CA|BKA) * Pr(BKA) + Pr(CA|\overline{BKA}) * Pr(\overline{BKA})$$

However, the probability of answering correctly given she does not know the answer $Pr(CA|\overline{BKA})$ will be higher compared to $Pr(CA|\overline{AKA})$ since right now she either answer randomly over m or 2 left answers, while Adam just chooses randomly and uniformly over m answers when he has no clue. So, the probability of answering correctly when she knows the answer $Pr(BKA|CA)$ should be decreased since we assumed that $Pr(BKA)$ remained the same. Nevertheless, the subquestion refers that $Pr(AKA|CA) = Pr(BKA|CA)$, which means that our initial assumption of $Pr(BKA)$ remains the same was wrong and the only way for the equation $Pr(AKA|CA) = Pr(BKA|CA)$ to be true is when $Pr(BKA)$ is higher than it was before, so $Pr(BKA) = p_1 > 0.6$. We can prove it if we use the supposed information about $m = 5$ and $p_2 = 0.1$:

$$\begin{aligned} Pr(BKA|CA) &= \frac{1 * p_1}{1 * p_1 + \frac{1}{2} * p_2 + \frac{1}{m} * (1 - (p_1 + p_2)))} \\ &= \frac{1 * p_1}{1 * p_1 + \frac{1}{2} * 0.1 + \frac{1}{5} * (1 - (p_1 + 0.1)))} \end{aligned} \tag{1}$$

Based on the fact that the result of (b) equals (c):

$$Pr(AKA|CA) = Pr(BKA|CA) = 0.88 \tag{2}$$

So from (1) and (2) equations:

$$\frac{1 * p_1}{1 * p_1 + \frac{1}{2} * 0.1 + \frac{1}{5} * (1 - (p_1 + 0.1)))} = 0.88 \Leftrightarrow p_1 = 0.6873$$

2 Random subsets

a)

We define E_i the event of successful inserting element i to set X and G_i the probability of generating the subset i of all the 2^n subsets of set $[n]$. The generation of each subset X of set $[n]$ is produced based on n tosses of a fair coin. In particular, every element is going to be added based on the toss of a fair coin. Since the coin is fair we suppose that $Pr(E_i) = \frac{1}{2}$. Moreover, each toss is independent from all the other $n-1$ tosses. So, the probability of generating each subset i of X is the following:

$$Pr(G_i) = \prod_{i=1}^{n} Pr(Ei) = (\frac{1}{2})^n \tag{3}$$

Intuitively, for each element i we toss a coin and we submit it to our generating subset. We run n tosses and each time since it is independent events we multiply the probabilities of the tosses of the previous elements. Since each subset is going to be generated with the same probability then the resulting set X is equally likely to be each of all the 2^n subsets of the set $[n]$.

b)

We define E_y the elements of set Y. The set X is a subset of Y when every element of X is also an element of Y. So the probability of $Pr(X \subseteq Y)$ is the probability of choosing all the possible subsets you can produce from the e_y elements out of the 2^n possible subsets of [n].In particular, since we choose independently and uniformly both X and Y sets the final probability is the following:

$$Pr(X \subseteq Y) = \frac{2^{E_y}}{2^n}$$

c)

We define E the event that each element from $X \cup Y \cup Z$ appears in at least two of the three sets. The number of elements for $X \cup Y \cup Z$ set could be minimum 1 or maximum n. Looking for one element of the union set we need to find all the permutations in which it belongs to at least two sets and then we generalize this idea for all the possible elements of the union set. So $Pr(E)$ is calculated as:

$$Pr(E) = \prod_{i=1}^{n} Pr(\text{"each element } x_i \text{ from } X \cup Y \cup Z \text{ belongs to at least two sets"})$$

We define the notation that XYZ is the event that the element i belongs to all X,Y and Z while $\overline{X}YZ$ is the event that the element i belongs to Z,Y and not X. So:

$$\begin{aligned} &Pr(\text{"each element } x_i \text{ from } X \cup Y \cup Z \text{ belongs to at least two sets"}) = \\ &\quad = Pr(XYZ) + Pr(\overline{X}YZ) + Pr(X\overline{Y}Z) + Pr(XY\overline{Z}) \end{aligned}$$

From 2(a) we know that each element is chosen by a fair coin in each set X,Y or Z respectively and we fip the coin independently for each set. So:

$$Pr(XYZ) = Pr(\overline{X}YZ) = Pr(X\overline{Y}Z) = Pr(XY\overline{Z}) = \frac{1}{8}$$

Based on that result the previous equation is equal to:

$$Pr(\text{"each element } x_i \text{ from } X \cup Y \cup Z \text{ belongs to at least two sets"}) =$$
$$= Pr(XYZ) + Pr(\overline{X}YZ) + Pr(X\overline{Y}Z) + Pr(XY\overline{Z}) = \frac{1}{2}$$

So the wanted probability $Pr(E)$ is:

$$\begin{aligned} Pr(E) &= \prod_{i=1}^{n} Pr(\text{"each element } x_i \text{ from } X \cup Y \cup Z \text{ belongs to at least two sets"}) \\ &= \prod_{i=1}^{n} \frac{1}{2} = (\frac{1}{2})^n \end{aligned}$$

3 Verifying matrix multiplication

a)

a).1

We define as E the event of accepting incorrectly the algorithm. The algorithm picks one cell D(i,j) and accepts incorrectly if the cell's number is not zero, in other words if the identity does not hold. In order to pick this one cell, it picks randomly the i coordinate over n choices and j coordinate as well randomly over n choices. Intuitively, the best this algorithm can do is to check 1 over the n^2 choices and accept or reject the matrix multiplication based only on that. So Pr(E) has an upper bound as the following:

$$Pr(E) \geq \frac{1}{n^2}$$

a).2

We define k to be the number of all independent runs of the algorithm. Also, we define $Pr(Error)$ the error probability of the previous algorithm.The $Pr(error)$ after we run it k times is given as follows:

$$Pr(error) = (1 - Pr(E))^k$$

Since we want to bound $Pr(error)$ to be at most $\frac{1}{3}$ then the previous equation is transformed as follows:

$$Pr(error) = (1 - Pr(E))^k \leq \frac{1}{3} \Longrightarrow$$

$$
\begin{aligned}
(1-\frac{1}{n^2})^k &\leq \frac{1}{3} \xrightarrow{1-x\leq e^{-x}} \\
e^{\frac{-k}{n^2}} &\leq \frac{1}{3} \xrightarrow{ln()} \\
\frac{-k}{n^2} &\leq ln(\frac{1}{3}) \Longrightarrow \\
k &\geq n^2 \cdot ln(3)
\end{aligned}
$$

a).3

In order to answer about running time we should think first what is the running time for the initial algorithm and then multiply this time over k iterations. Initially, the algorithm only calculates a cell of the matrix so it need to make calculations over all the vector $A[i,m], m = [1,...,n]$ and vector $B[m,j], m = [1,...,n]$ then apply a subtraction with $C[i,j]$ and a comparison with zero. The calculations needs at least $O(n)$ time since it is a vector by vector multiplication. Based on subquestion (b) if we run this algorithm at least over $n^2 \cdot ln(3)$ iterations then the final running time will be with asymptotic notation $O(ln(3) \cdot n^2 \cdot n) \approx O(n^3)$

b)

We define $\overline{r} \in [0,..,v-1]^n$ as a random vector. For our proof, we will use the following lemma: *Choosing r* $= \overline{r} \in [0,..,v-1]^n$ *uniformly at random is equivalent to choosing each* r_i *independently and uniformal from* $[0,...,v-1]$. The proof behind the lemma is that if each r_i is chosen independently and randomly then each of all 2^n possible subsets of $\overline{r}$ have a probability $(\frac{1}{v})^n$. Following the same process as for verifying matrix multiplication using a vector $r \in [0,1]^n$. We suppose $D = AB - C \neq 0$ and multiply each part with the random vector $\overline{r}$. So $D\overline{r} \neq 0$. Without error of generality we investigate one cell of D since it has a non zero value, for example D$_{nn}$:

$$D_{nn} = \sum_{j=1}^{n} d_{n,j} \cdot r_j \Longrightarrow r_n = \frac{\sum_{j=1}^{n-1} d_{n,j} \cdot r_j}{d_{nn}}$$

Now using the lemma, choosing each r_k from the vector $\overline{r}$ can be done independently and uniformly at random from $[0,..,v-1]$. So if we considered all the other r_k values of $\overline{r}$ vector have been set in a fixed value then in our case only r_n has not yet been chosen. Returning back to the previous equation the right part has a fixed deterministic value since all factors have been calculated. On the left part, r_n has not been calculated and through lemma it has v equally possible values to take. So, the equality holds with a probability at most $\frac{1}{v}$ and hence the probability that $AB\overline{r} = C\overline{r}$ is at most $\frac{1}{v}$.

c)

Suppose E be the event that the identity is correct, and assume B be the event that the test returns that the identity is correct. We start with $Pr(E) = \frac{1}{v}$ and $Pr(\overline{E}) = \frac{v-1}{v}$, and since test has a one-slide error bounded by $\frac{v-1}{v}$ it is true that $Pr(B|E) = 1$ and $Pr(B|\overline{E}) \leq \frac{v}{v-1}$. So using Bayes's law we get:

$$Pr(E|B) \geq \frac{Pr(B|E) \cdot Pr(E)}{Pr(B|E) \cdot Pr(E) + Pr(B|\overline{E}) \cdot Pr(\overline{E})} \Longrightarrow Pr(E|B) \geq \frac{\frac{1}{v}}{\frac{1}{v} + \frac{v-1}{v} \cdot \frac{v-1}{v}} = \frac{v}{v+(v-1)^2}$$

Suppose now that after running the randomized test again and again it returns that the identity is correct. After the first test, we may naturally have revised our prior model, so that we believe $Pr(E) = \frac{v}{v+(v-1)^2}$ and $Pr(\overline{E}) = 1 - Pr(E) = \frac{(v-1)^2}{v+(v-1)^2}$.Moreover, let B be the event that the new test returns that the identity is correct; since the tests are independent, as before we have $Pr(B|E) = 1$ and $Pr(B|E) \leq \frac{v}{v-1}$. So using Bayes's law we get:

$$Pr(E|B) \geq \frac{Pr(B|E) \cdot Pr(E)}{Pr(B|E) \cdot Pr(E) + Pr(B|\overline{E}) \cdot Pr(\overline{E})} \Longrightarrow Pr(E|B) \geq \frac{\frac{v}{v+(v-1)^2}}{\frac{v}{v+(v-1)^2} + \frac{v-1}{v} \cdot \frac{(v-1)^2}{v+(v-1)^2}} = \frac{v^2}{v^2 + (v-1)^3}$$

Based on the previous two examples we can formalize that in general if our prior model (before running the test) is that $Pr(E) \geq \dfrac{v^i}{v^i + (v-1)^{i+1}}$ and if the test returns that the identity is correct (event B), then:

$$Pr(E|B) \geq \frac{Pr(B|E) \cdot Pr(E)}{Pr(B|E) \cdot Pr(E) + Pr(B|\overline{E}) \cdot Pr(\overline{E})} \Longrightarrow Pr(E|B) \geq \frac{\frac{v^i}{v^i+(v-1)^{i+1}}}{\frac{v^i}{v^i+(v-1)^{i+1}} + [1 - \frac{v^i}{v^i+(v-1)^{i+1}}]} = \frac{v^{i+1}}{v^{i+1} + (v-1)^{i+2}}$$

4 Generalized Randomized Min-Cut

a)

The small modification to Karger's algorithm so that it outputs a 3-way cutset is to stop the basic algorithm one step earlier. By doing so, the algorithm will continue to cut an edge in each iteration but since it stops one step earlier the number of nodes will be 3 and as a result we receive the set of edges connecting the three remaining vertices.In particular the 3-way Karger's algorithm will be the following:

```
Algorithm 1: 3-way Karger's algorithm.
  input  : undirected graph G=(V,E)
  output: The set of edges connecting the three remaining vertices.
  while $\|V\| > 3$ do
      choose $e \in E$ uniformly random.
      $G \leftarrow$ graph obtained by contracting $e \in G$
  end
  Return the set of edges connecting the three remaining vertices.
```

b)

We define E_1 as the event of we pick an edge not in C in the first iteration. So we need to calculate the following probability:

$$Pr(E_1) = 1 - Pr(\overline{E_1}) \tag{4}$$

The probability of picking an edge in C is the probability of choosing one of the k edges belonging to C out of all m edges.So the equation (4) turns out:

$$Pr(E_1) = 1 - \frac{k}{m}$$

We define two nodes of the graph u and v, with $u, v \in V$. When we pick an edge in the first iteration there are two separate situations for those two nodes. In the first situation they are not connected so in order to belong in the up coming minimum 3-way cut-set the sum of their degrees should be at least as the number of edges k,so :

$$deg(u) + deg(v) \geq k \tag{5}$$

In the second situation, nodes u and v are connected so in order to belong in the up coming minimum 3-way cut-set the following equation must be true:

$$deg(u) + deg(v) - 1 \geq k \tag{6}$$

We subtract one edge since we have double counted as the two edges are connected. In order to generalize those two forms we are going to take the sum of all the possible pairs of u and v and find a lower bound for them. So for the equation (5) the sum of all the possible pairs of u and v has the following lower bound.

$$\sum_{u,v \in V} deg(u) + deg(v) \geq \binom{n}{2} \cdot k. \tag{7}$$

The reason for this bound of the sum of all pairs of nodes is that the sum of degrees of one pair is at least k. If we calculate all the pairs then it is k times all the total combinations to choose two nodes. Now, for the equation (6) if we sum of the connected edges then the sum would be greater equal with the total number of edges.So :

$$\sum_{u,v \in V} deg(u) + deg(v) \geq m \tag{8}$$

Adding the equations (7) and (8) with give us an information about the degrees of all the pairs of nodes regardless if they are connected or not. If we sum all the degrees of all the pairs of nodes we will get:

$$\sum_{u,v \in V} deg(u) + deg(v) = 2 * m * (n-1) \tag{9}$$

The reason behind the above equation is that adding all the degrees of pairs of nodes we will get the number of edges m overcounted. Overcounted by 2 since we calculated the edges of connected nodes twice and we did that for each other node (n-1) of a pair for all the nodes. In other words, for each node we double counted all the edges between its connected nodes for all the combination with the rest of the nodes. So, adding all pairs of nodes through equations (7),(8) we get:

$$\begin{aligned}
\sum_{u,v \in V} deg(u) + deg(v) &\geq \binom{n}{2} \cdot k + m \xrightarrow{(9)} \\
2 * m * (n-1) &\geq \binom{n}{2} \cdot k + m \Longrightarrow \\
m &\geq \frac{\binom{n}{2} \cdot k}{2(n-1) - 1} \Longrightarrow \\
1 - \frac{k}{m} &\geq 1 - \frac{1 - 2(n-1)}{\binom{n}{2}} \Longrightarrow \\
Pr(E_1) &\geq 1 - \frac{1 - 2(n-1)}{\binom{n}{2}} \Longrightarrow \\
Pr(E_1) &\geq \frac{(n-2)(n-3)}{n(n-1)}
\end{aligned}$$

c)

We define F_i the event of no contracted edges belongs in C after i iterations. Based on that $Pr(E_1) = Pr(F_1)$. If we run the algorithm for a second iteration then we should make the same analysis as we did in (b) but this time the nodes are n-1 since we contracted two into one in the first iteration. So $Pr(E_2|F_1) = \frac{((n-1)-2)((n-1)-3)}{(n-1)((n-1)-1)} = \frac{(n-3)(n-4)}{(n-1)(n-2)}$. If we generalize then:

$$Pr(E_i|F_{i-1}) = \frac{(n-i-1)(n-i-2)}{(n-i+1)(n-i)}$$

So to run one iteration of the whole algorithm based on previous equation:

$$\begin{aligned} Pr(F_{n-3}) &= Pr(E_{n-3} \cap F_{n-4}) = Pr(E_{n-3}|F_{n-4}) * Pr(F_{n-4}) \implies \\ &= Pr(E_{n-3}|F_{n-4}) \cdot Pr(E_{n-4}|F_{n-5}) ... Pr(E_2|F_1) \cdot Pr(F_1) \implies \\ &\geq \prod_{i=1}^{n-3} \frac{(n-i-1)(n-i-2)}{(n-i+1)(n-i)} \implies \\ &\geq \frac{(n-2)(n-3)}{n(n-1)} \cdot \frac{(n-3)(n-4)}{(n-1)(n-2)} ... \frac{12}{30} \cdot \frac{6}{20} \cdot \frac{1}{6} \implies \\ &\geq \frac{12}{n(n-1)^2(n-2)} \end{aligned}$$