

1

a. To vote for one candidate out of three, a voter can encrypt three different times. The voter encrypts a 1 for the candidate they want and a 0 for the other two, posts these 3 votes, and gives a zero knowledge proof that exactly one of the 3 values is an encryption of a 1, and the other two are encryptions of 0. Then, we add up all the votes for each candidate. The third party decrypts each candidate's total, and proves that this decryption is correct.

b. To compute the number of "yes" votes, simply compute $n_1 + n_2 - 9N$. To make sure this works, note that if we denote k as the number of "yes" votes, then $N - k$ represents the number of "no" votes. Then $n_1 + n_2 = 10 \cdot k + 9(N - k) = 10k + 9N - 9k = k + 9N$, so $n_1 + n_2 - 9N = k$ as desired.

c. Yes, we can. Note that TP_1 , if he receives some $n \in [0, 9]$, has no idea what the other number is and therefore has a 50% chance of guessing the right vote. Because the numbers are picked at random, there is a $\frac{1}{11}$ chance that someone voting "yes" will pick a 10. Since each person votes yes with probability $\frac{1}{2}$, TP_1 will get a 10 with probability $\frac{1}{22}$. Since there are presumably many more than 22 voters, TP_1 will probably get at least one 10 and can therefore be absolutely certain that this person voted "yes." Therefore, he can tip the balances in his favor by having a 50% chance if he gets a number that is not 10, but having a 100% chance for all the 10s he receives.

Now his success probability on guessing each vote is:

$$\begin{aligned} \Pr[\text{Success}] &= \Pr[\text{Success}|n = 10] * \Pr[n = 10] + \Pr[\text{Success}|n \neq 10] * \Pr[n \neq 10] \\ &= 1 * \frac{1}{22} + .5 * \frac{21}{22} \\ &= \frac{23}{44} \end{aligned}$$

Alternatively, when TP_1 gets a value $n \in [0, 9]$, he can always guess that the vote was a no. Intuitively, since we know yes votes have some chance of being encoded as a 10, we know yes votes are slightly less likely to be encoded as 0 - 9 (only with probability $\frac{10}{11}$), whereas all no votes will be encoded as 0 - 9. Since yes and no votes are equally likely, this means 0 - 9 is more likely to come from a no vote.

In this case, the success probability on guessing each vote is:

$$\begin{aligned} \Pr[\text{Success}] &= \Pr[\text{Success}|yes vote] * \Pr[yes vote] + \Pr[\text{Success}|no vote] * \Pr[no vote] \\ &= \Pr[n = 10|yes vote] * \Pr[yes vote] + \Pr[\text{Success}|no vote] * \Pr[no vote] \\ &= \frac{1}{11} * \frac{1}{2} + 1 * \frac{1}{2} \\ &= \frac{12}{22} \end{aligned}$$

d. Again, we can. If we expand the range from 1 to 10,000 (or even higher), then TP_1 will

only receive one number (10,000) every 10,001 votes of which he can be absolutely certain. If we make our number for the “yes” vote much higher than the number of voters, TP_1 will most likely not be able to guess Alice’s vote with probability higher than 50%.

2

a. To check that the graph is represented correctly, Bob can ask Alice to remove all the paper cups next to the edges (the ones showing the two endpoints of each edge) and the paper cups covering the green numbers. This will allow him to check that she is using the right graph.

Note that if we do not remove the cups covering the green numbers, then the verifier would have to solve the graph isomorphism problem to verify that the graph with the blue labelling is equivalent to the original graph. That would be hard.

b. He comes back in after Alice has rearranged everything and looks under all the paper cups covering the C and Not C marks. This will allow him to see how many vertices are in the cover.

c. Bob will ask Alice to show all the information surrounding one edge (so he sees the endpoints of the edge and the arrow pointing to the one in the vertex cover). Then, he can ask to confirm that the endpoint to which the arrow is pointing has a C under its corresponding paper cup. Since he is looking at one edge, he will catch Alice with probability $\frac{1}{E}$, where E represents the number of edges in the graph.

d. Bob should always pick completely at random. There are three ways to check whether Alice is cheating: (1) check that the graph is correct, (2) check that the size of the alleged cover is correct, and (3) check one edge at a time to make sure each edge is covered. Therefore, whenever Bob comes back in the room, he should randomly pick one of these ways of checking. Suppose, he ends up picking each method with probability $\frac{1}{3}$. If he picks to verify the graph, he will know with probability 100% if Alice is using the wrong graph. Likewise, if he picks to verify the size of the cover, he will know with probability 100% if the number of C s is not the same as what Alice claimed. If he picks to verify edges, we determined in part (c) that he has a $\frac{1}{E}$ chance of catching Alice, where he again picks his edge to check completely at random. Therefore, if Alice cheats by messing up the graph, she will be caught with probability $\frac{1}{3}$, if she cheats by adding extra vertices to the cover, she will be caught with probability $\frac{1}{3}$, and if she cheats by not covering some edges, she will be caught with probability at least $\frac{1}{3E}$. Since these are the only 3 ways she can cheat, this means Bob will catch her with probability at least $\frac{1}{3E}$.

Alternatively, if we check (1) with probability $\frac{1}{E+2}$ and (2) with probability $\frac{1}{E+2}$, and (3) with probability $\frac{E}{E+2}$, then if Alice cheats by messing up the graph, we will check (1) and catch her with probability $\frac{1}{E+2}$. Similarly, if she cheats by adding more than k vertices to her cover, we will check (2) and catch her with probability $\frac{1}{E+2}$. Finally, if Alice cheats by not covering at least 1 edge, we will check (3) with probability $\frac{E}{E+2}$, and then we will check the appropriate edge with probability $\frac{1}{E}$, so we will catch her with probability at least $\frac{1}{E+2}$. Thus, in all cases our minimum probability

of catching her is $\frac{1}{E+2}$.

e. Suppose we use the first strategy given in part d. Then Bob should repeat the process $3 \cdot E$ times. The probability that Alice can get away with cheating in each round is $(1 - \frac{1}{3E})$. The probability that Alice can get away with cheating in $3E$ rounds is $(1 - \frac{1}{3E})^{3E}$, which is approximately $\frac{1}{e}$ which is a constant.

3

a. This definition is equivalent to the original. To see this, we write $\Pr[c] = \Pr[c|m] = \frac{\Pr[m \cap c]}{\Pr[m]}$. Now, rearranging this equation to solve for $\Pr[m]$, we see that $\Pr[m] = \frac{\Pr[m \cap c]}{\Pr[c]} = \Pr[m|c]$ by definition. This we recognize as the Shannon definition, so this definition implies the Shannon definition. To see the converse, note that $\Pr[m] = \Pr[m|c] = \frac{\Pr[m \cap c]}{\Pr[c]}$. Again, we rearrange to see that $\Pr[c] = \frac{\Pr[m \cap c]}{\Pr[m]} = \Pr[c|m]$, so the two definitions are indeed equivalent.

b. By the Shannon definition, we know that $\Pr[m_1] = \Pr[m_1|c]$ and $\Pr[m_0] = \Pr[m_0|c]$. Therefore, if $\Pr[m_0|c] = \Pr[m_1|c]$, we have that $\Pr[m_1] = \Pr[m_0]$ and therefore M must have a uniform distribution (a distribution in which all messages are equally likely to be picked) since this is true for all pairs m_0, m_1 in M .

4

a. A function like $\nu(k) = 2^{-k}$ is certainly negligible, and also always positive.

b.

- This is not negligible. Look at something like $p(k) = 1$ for a counterexample.

- Yes, this is negligible.

Proof: Suppose that $\nu_1(k) * \nu_2(k)$ is not negligible. Then there exists a polynomial p such that at an infinite number of points k , $\frac{1}{p(k)} < \nu_1(k) * \nu_2(k)$. Then, since $\nu_1(k) \in [0, 1]$, we know that at all of these points k , $\frac{1}{p(k)} < \nu_2(k)$. But then there cannot exist k_0 such that for all $k > k_0$, $\nu_2(k) < \frac{1}{p(k)}$, so ν_2 is not negligible. This is a contradiction.

- Yes, this is negligible.

Proof: Suppose that $\nu(k) * p(k)$ is not negligible. Then there exists a polynomial q such that at an infinite number of points k , $\frac{1}{q(k)} < p(k) * \nu(k)$. Let $r(k) = q(k)p(k)$, and note that r is a polynomial. Then, we know that at all of these points k , $\frac{1}{q(k)p(k)} = \frac{1}{r(k)} < \nu(k)$. But then there cannot exist k_0 such that for all $k > k_0$, $\nu(k) < \frac{1}{r(k)}$, so ν is not negligible. This is a

contradiction.

- No, this is not necessarily negligible.

$$\text{Let } p(k) = k \text{ and } \nu_i(k) = \begin{cases} 1 & \text{for } k = i \\ 0 & \text{for } k \neq i \end{cases}$$

Now

$$\begin{aligned} \sum_{i=1}^{p(k)} \nu_i(k) &= \sum_{i=1}^k \nu_i(k) \\ &= \nu_k(k) + \sum_{i=1}^{k-1} \nu_i(k) \\ &= 1 + 0 \\ &= 1, \text{ which is not negligible.} \end{aligned}$$

Intuitively, if at every point k , we add in a function which is negligible in that it will eventually become very small (in this case 0), but which is large (in this case 1) at point k , we will have a sum which is large at all points k .

Note: this problem ended up being much subtler and more difficult than we intended, so we decided to give credit for both yes + no answers.

- This is clearly not negligible; just take $\nu_1 = \nu_2$ for a counterexample.
- This is not negligible, and $p(k) = k$ should provide a counterexample.

c. This does not follow. Since the problem doesn't ask for the function to be continuous, we can take a function like $\nu(k) = \begin{cases} \text{negligible} & \text{for } k \text{ even} \\ 1 & \text{for } k \text{ odd} \end{cases}$ as a counterexample.