EECS 70 Discrete Math and Probability Spring 2020 UC Berkeley — Midterm 2

1. Fun with Letters (10 pts)

(a) (5 pts) **How many ways are there to arrange m A's, n B's and 1 C in a circle on a piece of paper?** Two letter arrangements are equivalent if and only if one can be rotated to obtain the other *without* flipping the paper over. **Clearly and concisely explain how you got your answer.**

Solutions: Fix C at the top so we don't overcount rotations. There are $\binom{m+n}{n}$ ways to choose n spots for B out of the $m+n$ remaining total slots. The m A's are forced to go in the rest of the spots. Any circle of letters can be rotated to have the single C at the top, so we are counting all unique configurations.

So there are $\binom{m+n}{n}$, or equivalently $\binom{m+n}{m}$, total ways.

Alternate approach: There are $(m+n+1)!$ total ways to to permute the $m+n+1$ total letters. To avoid overcounting, we need to divide by the number of ways to permute the A's ($m!$) and B's ($n!$). Finally, to account for rotations, we divide by $m+n+1$, as each unique circle has $m+n+1$ distinct rotations.

So there are $\frac{(m+n+1)!}{m!n!(m+n+1)} = \frac{(m+n)!}{m!n!}$ ways.

(b) (5 pts) Oski Bear is working on the above problem for $m = 3$ and $n = 2$ and says: "We can fix one of the B's at top of the cycle. We have 5 ways to choose a spot for the second B, and then 4 ways to choose a spot for C. Three A's go in the remaining 3 spots. So there are a total of $5 \times 4 = 20$ ways to arrange the letters." **Explain why Oski's approach does not work. In particular, is he undercounting or overcounting? If he is undercounting, give a specific instance that Oski's method didn't account for; if he is overcounting, give a specific example of an instance that is counted multiple times and briefly explain why it is counted more than once.**

Solutions: Oski is overcounting. When choosing spots for the second B, the same arrangement can be counted twice. For example, listing the arrangement clockwise, B_1B_2CAAA and B_1CAAAB_2 are counted as different arrangements but can be obtained from each other with rotation.

Knowing the previous part's solution can help you see that Oski is overcounting. After all $\binom{5}{3} = \frac{5 \cdot 4}{2} = 10$ which is less than 20 by a factor of two. This not only tells you that Oski is overcounting, it suggests that Oski is double counting. Where is this extra factor of two coming from? Are there two of anything? Yes! There are two Bs. This way, the numbers themselves can help you zero in on what the underlying issue is.

2. Independence (14 pts)

(a) (8 pts) The villagers of Bararah want to select exactly *one* of their top-performing gymnasts to compete in the regional competitions next fall. The four gymnasts who have made it to the top are Audra, Bibi, Kirk, and Babak.

After intense deliberation, the villagers decide to select one of the four gymnasts uniformly at random, since the candidates are equally capable. That is, each candidate is as likely as any other candidate to be selected.

Let A denote the event, "the letter 'a' appears in the name of the selected gymnast." That is, $A = \{\text{Audra}, \text{Babak}\}$.

Let B denote the event, "the letter 'b' appears in the name of the selected gymnast." That is, $B = \{\text{Bibi}, \text{Babak}\}$.

And let K denote the event, "the letter 'k' appears in the name of the selected gymnast." That is, $K = \{\text{Kirk}, \text{Babak}\}$.

Determine whether the events A, B, and K are mutually independent. Explain your answer clearly using the definition of mutual independence.

Solutions: The definition of mutual independence for three events requires the events to be pairwise independent as well as the probability of the intersection of all three of them being the product of their individual probabilities.

The individual probabilities of the three events are

$$\Pr(A) = \Pr(B) = \Pr(K) = \frac{2}{4} = \frac{1}{2}$$

since each of the candidates is equally likely to be chosen.

We note that the pairwise intersections of these events are identical. That is,

$$A \cap B = A \cap K = B \cap K = \{\text{Babak}\}.$$

It's now straightforward to see that the three events A, B, and K are *pairwise* independent:

$$\Pr(A \cap B) = \Pr(\{\text{Babak}\}) = \frac{1}{4} = \underbrace{\Pr(A)}_{1/2}\underbrace{\Pr(B)}_{1/2}$$

$$\Pr(A \cap K) = \Pr(\{\text{Babak}\}) = \frac{1}{4} = \Pr(A)\Pr(K)$$

$$\Pr(B \cap K) = \Pr(\{\text{Babak}\}) = \frac{1}{4} = \Pr(B)\Pr(K).$$

However, note that

$$A \cap B \cap K = \{\text{Babak}\},$$

so

$$\Pr(A \cap B \cap K) = \frac{1}{4} \neq \Pr(A)\Pr(B)\Pr(K) = \frac{1}{8}.$$

Therefore, the three events are *not* mutually independent.

(b) (6 pts) Consider two events A and B defined on a random experiment whose sample space is denoted by Ω. We know $\Pr(A \cap B) = \Pr(A)\Pr(B)$. Let A^c denote the complement of event A and B^c denote the complement of event B.

True or False? $\Pr(A^c \cap B^c) = (1 - \Pr(A))\Pr(B^c)$.

If you claim the assertion is true, provide a proof based on what is given. If you claim the assertion is false, provide a counterexample.

Solutions: The assertion is true. This problem is fundamentally about complements and inclusion/exclusion as well as the definition of independence.

$$\begin{aligned}\Pr(A^c \cap B^c) &= \Pr(\Omega \setminus (A \cup B)) \\ &= 1 - \Pr(A \cup B) \\ &= 1 - (\Pr(A) + \Pr(B) - \Pr(A \cap B))\end{aligned}$$

But we know that A and B are independent, so $\Pr(A \cap B) = \Pr(A)\Pr(B)$.

$$\begin{aligned}&= 1 - \Pr(A) - \Pr(B) + \Pr(A)\Pr(B) \\ &= (1 - \Pr(A))(1 - \Pr(B)) \\ &= (1 - \Pr(A))\Pr(B^c)\end{aligned}$$

which concludes the proof.

3. Babak's sneaky attempt to sneak into Cory Hall (30 pts)

On a typical day, the State of California hosts 40 million people ("Californians").

Of that population, 2,000,000 have a persistent cough.

Among those who have a persistent cough, 1,000 have muscle ache.

Another 4,000 have muscle ache that is *not* accompanied by a persistent cough.

Of those who have a persistent cough *and* muscle ache, 900 are infected with, and carry, the influenza (flu) virus.

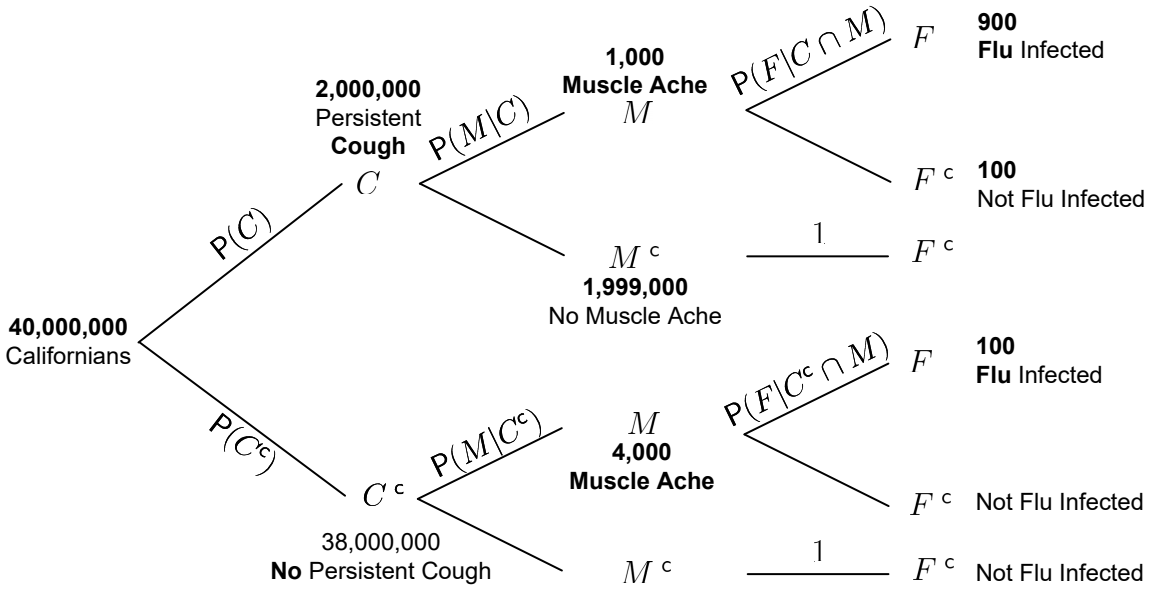
Anyone infected with the flu virus also suffers from muscle ache.

The number of Californians who are infected with, and carry, the flu virus, but who do *not* suffer from a persistent cough, is 100.

For convenience, we define the following events for a typical day in California:

- Event C denotes "A randomly-selected Californian suffers from a persistent cough."
- Event M denotes "A randomly-selected Californian suffers from muscle ache."
- Event F denotes "A randomly-selected Californian is infected with, and carries, the flu virus."

The diagram shown displays *part* of the statistics about a typical day in California. (Some relevant numbers might not be shown.)



The EECS Department at UC Berkeley has banned any person from entering EECS premises if they're likelier than not to carry the flu virus. In particular, a security guard has been assigned to each entrance of Cory Hall. The role of the guard is to assess the status of each prospective entrant and enforce department policy.

On the way to his office, Babak exhibits not only a persistent cough but also unmistakable signs of muscle ache. "You may not enter Cory Hall, Babak, because you're a likely carrier of the flu virus," the guard says.

Babak floods the guard with the California statistics and then says:

> *Fewer than the infinitesimal fraction of 1 in 2,000 Californians who suffer from a persistent cough are actually infected with, and carry, the flu virus. So, my persistent cough must not preclude me from entry into Cory Hall. Allow me in, please.*

Babak's trick succeeds. The guard — untrained in probability theory and intimidated by the numbers hurled at him — admits Babak into Cory Hall.

(a) (6 pts) **Explicitly evaluate** $\Pr(C)$**,** $\Pr(M)$**, and** $\Pr(C|M)$**.**

Solutions: By inspecting the diagram, we can see:

$$\Pr(C) = \frac{2,000,000}{40,000,000} = \frac{1}{20}$$
$$\Pr(M) = \frac{1,000+4,000}{40,000,000} = \frac{5,000}{40,000,000} = \frac{1}{8,000}$$
$$\Pr(C|M) = \frac{1,000}{1,000+4,000} = \frac{1}{5}$$

(b) (6 pts) **Explicitly evaluate** $\Pr(F)$, the probability that a randomly-selected Californian is infected with, and carries, the flu virus.

Solutions: There are a total of $900+100 = 1000$ Flu infected, so:

$$\Pr(F) = \frac{1,000}{40,000,000} = \frac{1}{40,000}$$

(c) (6 pts) **True or False? Events** M **and** C **are *conditionally independent*, given Event** F**.** Explain your answer.

Hint: Evaluate $\Pr(M|F)$ *and* $\Pr(M|F \cap C)$*. This should not involve much work.*

Solutions: By inspecting the diagram, we can see:

$$\Pr(M|F) = 1$$
$$\Pr(M|F \cap C) = 1$$

Since $\Pr(M|F) = \Pr(M|F \cap C)$, we can conclude that events M and C are conditionally independent, given Event F.

(d) (6 pts) **Explicitly evaluate** $\Pr(F|C)$, the fraction of those afflicted with a persistent cough who are actually infected with, and carry, the flu virus. **Explain why this probability figure, an approximate upper bound for which Babak presented to the guard, should actually be irrelevant to the guard's decision.**

Solutions: By inspecting the diagram, we can see:

$$\Pr(F|C) = \frac{\Pr(F \cap C)}{\Pr(C)} = \frac{900}{2,000,000} = \frac{9}{20,000}$$

The guard should ignore this upper bound because it does not account for the fact that Babak has a muscle ache, which increases the probability that he has the flu.

(e) (6 pts) **Explicitly evaluate** $\Pr(F|C \cap M)$ **and explain why this is the probability figure that the guard should have taken into account while deciding.**

Solutions: By inspecting the diagram, we can see:

$$\Pr(F|C) = \frac{\Pr(F \cap C \cap M)}{\Pr(C \cap M)} = \frac{900}{1,000} = \frac{9}{10}$$

The guard should have used this number because it accounts for both of Babak's symptoms, cough and muscle ache.

4. Probabilistic Cycles (20 pts)

Suppose the random undirected graph G is constructed as follows. G starts off as n distinct vertices, where n is even. Independently for each of the possible pair of vertices, we add an undirected edge between them with probability p. (i.e. We toss a biased coin with probability p of coming up heads for each distinct pair of vertices — if it comes up heads, an edge is introduced between them. If it comes up tails, there is no edge there. The different coin tosses are independent of each other.)

(a) (2 pts) Let $v_1, v_2, \ldots, v_n$ be the vertices of G.

What is the probability that the sequence $[v_1, v_2, v_3, \ldots, v_n, v_1]$ corresponds to a cycle in the graph? Clearly and concisely explain how you got your answer.

(HINT: How many distinct edges are involved in this cycle?)

Solutions: For this cycle to exist, we need the edges $(v_1, v_2), (v_2, v_3), \ldots, (v_{n-1}, v_n), (v_n, v_1)$ to exist. As this is a set of n distinct edges, and each edge independently has probability p of existing, the probability that they all exist is $p \cdot p \cdot p \cdots p = p^n$.

(b) (10 pts) Using the union bound, **provide an upper bound on the probability that G has a Hamiltonian cycle.** Recall that a Hamiltonian cycle is a cycle which visits all the vertices of a graph exactly once.

Use Stirling's approximation ($n! \approx \sqrt{2\pi n}(\frac{n}{e})^n$) to argue about how small p has to be (as a function of n) for this bound to be nontrivial — i.e. for the bound to not be something bigger than 1. Feel free to make further approximations like $n - 1 \approx n$, etc. if that helps simplify what is going on.

Clearly explain how you got your answers by showing all work.

Solutions: We've already computed the probability of a specifc Hamiltonian cycle in the previous part. To apply the union bound, we need to count the number of distinct possible Hamiltonian cycles. There are $n!$ ways to permute all n vertices into a specific list (we need all vertices for the cycle to be Hamiltonian). We divide by n to account for rotations of the same cycle. The edges are undirected and so we need to further divide by 2 to account for potentially double counting reversed cycles for a total of $n!/(2n) = \frac{(n-1)!}{2}$ cycles.

Note: For purposes of a finding an upper bound as we will below, we accepted approximations of this expression such as $n!$ or $(n-1)!$. Those are valid upper bounds.

The event that G has a Hamiltonian cycle is the union of the events of each distinct possible Hamiltonian cycle existing. As there are $(n-1)!/2n$ such events, each with probability p^n of occurring, we find that an upper bound is:

$$\frac{(n-1)!}{2} \cdot p^n \leq n! p^n$$

Any valid upper bound using this train of thought, and reasonable approximations, should receive full credit.

Plugging in Stirling's approximation, the loosest version of the bound above becomes:

$$\sqrt{2\pi n}\left(\frac{n}{e}\right)^n \cdot p^n$$

If we set the above bound to be less than one and simplify we see that we need $p < (e/n)$ for the upper bound to be non-trivial.

Notice that if we used the tighter union bound, we would have had

$$\sqrt{\frac{\pi}{2}(n-1)}\left(\frac{n-1}{e}\right)^{n-1} \cdot p^n$$

which to some might feel different. However notice that:

$$\sqrt{\frac{\pi}{2}(n-1)}\left(\frac{n-1}{e}\right)^{n-1}\cdot p^n = \sqrt{\frac{\pi}{2}(n-1)}(\frac{e}{n-1})\left(\frac{n-1}{e}\right)^{n} p^n$$
$$= \sqrt{\frac{\pi e^2}{2(n-1)}}\left(\frac{(n-1)p}{e}\right)^{n}$$

For this to be less than one:

$$(n-1)\frac{p}{e} < (\frac{2(n-1)}{\pi e^2})^{\frac{1}{2n}}$$

which implies

$$p < \frac{e}{n}\left(\frac{n}{n-1}(\frac{2(n-1)}{\pi e^2})^{\frac{1}{2n}}\right)$$

and we can see that the entire term in parentheses goes to 1 as n gets large.

(c) (8 pts) After the construction of G, we see that it has e edges in total. Given this information, what is the probability that the vertices v_1, v_2, and v_3 form a triangle? **In other words, what is the probability that v_1, v_2, and v_3 form a cycle within G given that there are e total edges in the graph.** Clearly and concisely explain how you got your answer.

(HINT: You know where three of the e edges have to go, how many ways are there for the other $e-3$ edges to be placed?)

Solutions: We note that there are $\binom{n}{2}$ possible edges. This means there are a total of $\binom{\binom{n}{2}}{e}$ ways to place all the edges, and a total of $\binom{\binom{n}{2}-3}{e-3}$ ways to first fix three edges to (v_1, v_2, v_3) and place the remaining $e-3$ edges.

Let T be the event that the triangle exists and E be the event that there are e total edges. We then have:

$$\Pr(E) = \binom{\binom{n}{2}}{e}\cdot p^e(1-p)^{\binom{n}{2}-3}$$
$$\Pr(T\cap E) = \binom{\binom{n}{2}-3}{e-3}\cdot p^e(1-p)^{\binom{n}{2}-3}$$

Note that finding $\Pr(E)$ is a straightforward application of the probability that a $\text{Binom}(\binom{n}{2}, p)$ random variable is equal to e. Finding $\Pr(T\cap E)$ just tweaks that probability so we don't include the probability of configurations in which the triangle does not exist.

Thus we can find the final conditional probability:

$$\Pr(T|E) = \frac{\Pr(T\cap E)}{\Pr(E)} = \frac{\binom{\binom{n}{2}-3}{e-3}}{\binom{\binom{n}{2}}{e}} = \frac{e(e-1)(e-2)}{\binom{n}{2}(\binom{n}{2}-1)(\binom{n}{2}-2)}$$

Note: If you did a straight counting approach without justification on why the situation lended itself to a uniform probability space, you received most, but not all, of the credit.

5. Combinatorial Fun (16 pts)

(a) (6 pts) **Write the simplest expression potentially involving n, k, j that could go in the blank, and then prove the equality using a combinatorial proof.** You must give a combinatorial proof for full credit — algebra alone won't do it, even if it might help you figure out what is going on...

Assume $n > k > j$:

$$\text{\_\_\_\_\_} = \binom{n}{k-j}(k-j)!\binom{n-k+j}{j}j!$$

Solutions: There are two candidate expressions for being "simplest:" either $\binom{n}{k}k!$ or $\frac{n!}{(n-k)!}$.

We expected most people to get the expression by just working out the algebra:

$$\begin{aligned}\binom{n}{k-j}(k-j)!\binom{n-k+j}{j}j! &= \frac{n!}{(k-j)!(n-k+j)!}(k-j)!\frac{(n-k+j)!}{j!(n-k)!}j! \\ &= \frac{n!}{(n-k)!}\end{aligned}$$

and then noticing that this is just $\binom{n}{k}k!$.

The term involving the "choose" is easier for some to immediately interpret to give a combinatorial proof, while others might have felt that $\frac{n!}{(n-k)!} = n\cdot(n-1)\cdots(n-k+1)$ was easier to interpret since that is naturally a product of k different terms.

Either way, we are led to the following combinatorial proof:

We want to count the number of ways to pick an ordered list of k items out of n total choices. There are two ways of doing so.

LHS: First pick the k items that are going to be in our list, of which there are $\binom{n}{k}$ ways. Then there are $k!$ ways to permute them. This gives a count of $\binom{n}{k}k!$.

Alternative LHS: We pick k things out in order. There are n choices for the first item, $n-1$ choices for the second, and so on going to $n-k+1$ choices for the final k-th item. This gives $\frac{n!}{(n-k)!} = n\cdot(n-1)\cdots(n-k+1)$ for the left hand side.

RHS: First pick $k-j$ items to be the *first* $k-j$ items, and permute them (similar to LHS, there are $\binom{n}{k-j}(k-j)!$ ways to do this). Then pick j more items out of the $n-(k-j)$ remaining items (so we have chosen a total of k items), permute them, and put the entire permuted sequence *after* the first $k-j$ items we chose and permuted already. There are $\binom{n-k+j}{j}j!$ ways to complete this second step, and consequently $\binom{n}{k-j}(k-j)!\binom{n-k+j}{j}j!$ total ways to fully order k items out of n total choices.

Since we've counted the same thing two different ways, the LHS and RHS must be equal.

(b) (10 pts) Let $n \geq 2k$. **Write down the combinatorial identity that is proved by the following story.** *Some parts of the story are redacted and left for you to figure out.* Consequently, **you must explain your answer for full credit.**

There are n humans each with their dog. We want to select a party of $2k$ creatures from the n humans and n dogs to go on a hike, with the constraint that a dog cannot go without their owner, but an owner can go without their dog.

We can count the number of distinct valid parties in two ways: picking dogs first or picking people first.

If we select j of the dogs, then by the constraint, their owners have to be selected, so we only need to select $2k-2j$ more people from the remaining humans. The number of dogs selected ranges from 0 to k since at most half of the party can be dogs.

Alternatively, we could start with people. We select i people, then by the constraint, the dogs selected need to be owned by one of the i people. So there are *[redacted]* ways to pick the $2k-i$ dogs that are going to come along with the people we already selected. There clearly must be at least as many people as dogs selected, so we need to sum over i ranging from *[redacted]* to *[redacted]*.

Solutions:

$$\sum_{j=0}^{k} \binom{n}{j}\binom{n-j}{2k-2j} = \sum_{i=k}^{2k} \binom{n}{i}\binom{i}{2k-i}$$

LHS sums over the number of dogs we select: There are $\binom{n}{j}$ ways to choose j dogs and $\binom{n-j}{2k-2j}$ to choose the remaining $2k-2j$ humans whose dogs were not chosen. We sum over j from 0 to k as stated, as we cannot have more dogs than people (thus there are at most k dogs).

RHS sums over the number of people we select: There are $\binom{n}{i}$ ways to choose i people. All the dogs chosen must belong to one of those i people, so we have to choose $2k-i$ dogs out of the i dogs whose owners have already been chosen- that's $\binom{i}{2k-i}$ ways. We must have at least k people so that we have enough dogs to fill out the group of size $2k$ (if we only chose $k-1$ people, for example, we'd end up with at most $2(k-1) < 2k$ beings in the group in total). We can choose up to $2k$ people (the whole group could be humans).

6. Hotel Rooms and Beyond: Error-and-erasure correction leveraging the CRT (58 pts)

Note: for this entire problem, you can use properties of the Chinese Remainder Theorem that we discussed in lecture, notes, homework, and discussion without proof and without having to specify all the details.

Alice is staying at a hotel and she wants to share her room number with Bob by leaving a sequence of notes in a list of pre-arranged locations.

i) There are only 100 possible hotel rooms, labeled 0 to 99.

ii) Alice takes her room number p and computes the remainders $y_i = p \bmod p_i$. The specific p_i that she uses are $p_1 = 3, p_2 = 5, p_3 = 7, p_4 = 11$, and $p_5 = 13$.

iii) She writes y_i on the i-th note and places the note in location i. (Both Alice and Bob know which location corresponds to which numbers i and p_i.)

This sequence of notes can be viewed as a codeword $\vec{y}(p)$. For example, if Alice is in room 51, she sends the codeword $\vec{y}(51) = (0,1,2,7,12)$ since $51 \bmod 3 = 0$, $51 \bmod 5 = 1$, $51 \bmod 7 = 2$, $51 \bmod 11 = 7$, $51 \bmod 13 = 12$.

(a) (3 pts) Unfortunately, there is a chance that some of Alice's notes get blown away by the wind. Those missing notes will be treated as erasures and denoted by X.

It turns out that Alice is in room 51 as above, so she sends the codeword $(0,1,2,7,12)$. Bob gets the received symbols $(0,1,2,X,X)$. **Explain how Bob can leverage the CRT to identify Alice's room number.**

Solutions: Bob gets the codeword $(0,1,2,X,X)$, which corresponds to the following table:

3	5	7	11	13
0	1	2	X	X

He can then set up the following congruences:

$$p \equiv 0 \pmod 3$$
$$p \equiv 1 \pmod 5$$
$$p \equiv 2 \pmod 7$$

Through a straightforward application of the Chinese Remainder Theorem, we find:

$$\begin{aligned} p &\equiv (0)(35)[35^{-1}]_3 + (1)(21)[21^{-1}]_5 + (2)(15)[15^{-1}]_7 \pmod{3*5*7} \\ &\equiv (0)(35)[2^{-1}]_3 + (1)(21)[1^{-1}]_5 + (2)(15)[1^{-1}]_7 \pmod{105} \\ &\equiv (0)(35)(2) + (1)(21)(1) + (2)(15)(1) \pmod{105} \\ &\equiv 0 + 21 + 30 \pmod{105} \\ &\equiv \boxed{51} \end{aligned}$$

So Bob thinks Alice is in room $\boxed{51}$.

(b) (6 pts) Generalizing the previous part, **prove that in the case of up to two erasures anywhere, your scheme will always correctly identify the room number.** For this part, feel free to just use the properties of the CRT along with the following facts.

- $p_1 < p_2 < \cdots < p_5$.
- The number of rooms is less than $\prod_{i=1}^{3} p_i$.

Solutions: Assume the received message has ≤ 2 erasures. We show that the room number can be uniquely identified.

Select some three pairs of received (prime, residue) as $(p_i, r_i), (p_j, r_j), (p_k, r_k)$. The decoding algorithm is:

i. Use the CRT to find the message x with: He can then set up the following congruences:

$$x \equiv r_i \pmod{p_i}$$
$$x \equiv r_j \pmod{p_j}$$
$$x \equiv r_k \pmod{p_k}$$

This x will be unique $\bmod p_i p_j p_k$.

ii. Since the original message x (the room number) was chosen within $0 \leq x < \prod_{i=1}^{3} p_i \leq p_i p_j p_k$, knowing the message uniquely $\bmod p_i p_j p_k$ is sufficient to decode the exact message. Notice in this step, it was important the message was chosen to be less than the product of the three smallest primes – so any other set of 3 primes (corresponding to the non-erased locations) has a larger product.

So we can correctly decode with ≤ 2 erasures.

(c) (5 pts) Would your scheme *always* work if there were 3 erasures and only 2 received notes? **If so, argue that it always works. If not, give an explicit counterexample where your scheme doesn't work.** (i.e. construct an example where there is an ambiguity about which room is Alice's room.)

Solutions: It would not always work.

Assume for contradiction that this CRT code can tolerate any 3 erasures. Then we could erase the 3 largest primes, and only receive the message x mod 3 and mod 5. This only uniquely identifies the message mod 15, not mod 105, so we cannot decode uniquely. For example $x = 16$ and $x = 31$ both have the same residues mod 3 and mod 5.

Notice that if the first three locations were erased, we would in fact have enough information to uniquely decode, since $11 * 13 \geq 99$. But we are considering the worst-case pattern of erasures.

(d) (8 pts) Now assume that instead of the wind blowing away a note, somebody malicious finds a note before Bob and replaces it with a corrupted note. Now the received notes r_i could differ from the true $y_i = p \bmod p_i$ in at most one location.

For such a small message-space, Bob decides to simply try all possible messages $p \in \{0, 1, \ldots, 99\}$, and see which one's $\vec{y}(p)$ differs from the received notes $\vec{r}$ in at most one location. If there is a unique such p, Bob just picks that one.

Could there be two different legitimate room numbers whose encodings both differ from the received notes in only one note? If so, give an example. If not, prove it.

(HINT: If someone told you which note was corrupt, could you uniquely figure out the room? What if they told you that two specific notes were possibly corrupt? Could you do it then? How does that help you think about the above situation?)

Solutions: This is impossible. Fix some received codeword $(r_1, r_2, r_3, r_4, r_5)$. For contradiction, assume there were some two messages, $x_1 \neq x_2$ such that $\vec{y}(x_1)$ and $(r_1, r_2, r_3, r_4, r_5)$ differ at one position, and also $\vec{y}(x_2)$ and $(r_1, r_2, r_3, r_4, r_5)$ differ at one position. But then $\vec{y}(x_1)$ and $\vec{y}(x_2)$ differ from each other in at most two locations. Now consider sending the message x_1, encoded as $\vec{y}(x_1)$, and then erasing the locations of these two differences. Then a receiver can't determine if we encoded the message x_1 or x_2. But we have already proven that this code can tolerate 2 erasures and hence $x_1 = x_2$, which is a contradiction.

Note: In general, this reflects how any $2t$-erasure-correcting code can in principle be used as a t-error-correcting code.

You could also have essentially redone the proof of the previous part as a part of doing this part instead of just leaning on the previous part.

(e) (10 pts) Let's think about a more general case. Instead of 5 notes, assume that there are $n+2k$ of them. We have $n+2k$ large (think 100 binary digits or thereabouts) prime numbers $p_1 < p_2 < \cdots < p_n < p_{n+1} < \cdots < p_{n+2k}$. The message is the number p which is a natural number in the range $0 \leq p < \prod_{i=1}^{n} p_i$. Define the number $N = \prod_{i=1}^{n} p_i$ for this upper-bound quantity.

Suppose you receive a list $\vec{r}$ of received notes $r_1, r_2, \ldots, r_{n+2k}$.

At first, your friend is more relaxed than you about the possibility of corruptions. Your friend has a simple scheme in which she assumes that all $n+2k$ of the notes were not corrupted and just uses the Chinese Remainder Theorem to reconstruct a number r that satisfies all the $r_i = r \bmod p_i$ equations for all $i \in [1, n+2k]$. By the CRT construction, this r is always less than $M = \prod_{i=1}^{n+2k} p_i$. Your friend says that if there were no corruptions, then actually $r < N$ and she wouldn't have to think about anything and could just say that $p = r$.

Now your friend has received special information that the note in location ℓ might have been corrupted so that $r_\ell \neq y_\ell = p \bmod p_\ell$. Indeed your friend had already noticed that the r she naively reconstructed was in fact bigger than N.

She suggests the following scheme instead: she will take $e = p_\ell$ and multiply each of the r_i by e, taking the result mod p_i. In other words, she will compute $q_i = er_i \bmod p_i$ for all $i \in [1, n+2k]$. This way, $q_\ell = 0$ since she doesn't trust that corrupted note in location ℓ. Then, she will use the CRT to compute the unique non-negative integer q that satisfies all those equations and is less than M. With that q in hand, she will just divide q by e to get the original p.

Prove that your friend's scheme works if there is a corruption in the ℓ-th note. (You can assume that $k > 1$.)

Solutions: Since we want to recover p by computing $\frac{q}{e}$, what we need to show is that the recovered $q = pe$.

To show this, we invoke the CRT and the fact that it returns a unique integer less than M. If all the CRT equations are the same, then the solution to them is also the same mod M.

There are two categories of equations. Those that correspond to uncorrupted notes and the equation that corresponds to the corrupted note.

For the uncorrupted notes $i \neq \ell$, we know that $r_i = p \bmod p_i$ and this can be rewritten by the properties of modulo arithmetic as $er_i \bmod p_i = ep \bmod p_i$. This means that $q_i = ep \bmod p_i$ and so $q_i \equiv ep \pmod{p_i}$.

For the corrupted notes, we know that $r_\ell e = r_\ell p_{ell}$ and so $r_\ell e \bmod p_\ell = 0$ since all multiples of p_ℓ are divisible by p_ℓ. Meanwhile, $pe = pp_\ell$ and so by the identical logic, $pe \bmod p_\ell = 0$. This means that once again, $q_i \equiv pe \pmod{p_\ell}$.

So all the $n+2k$ equations match and by the CRT, this means that $q \equiv pe \pmod{M}$. All that remains is verifying that $ep < M$ but this is clear since

$$\begin{aligned}
ep &< eN && \text{since } p < N \text{ by definition} \\
&< p_{n+2k} \prod_{i=1}^{n} p_i && \text{by definition of } N \text{ and how big } e \text{ can be} \\
&< \prod_{i=1}^{n+2k} p_i && \text{since } k \geq 1 \\
&= M && \text{by the definition of } M
\end{aligned}$$

which means that $q = ep$. So dividing by e indeed gives p.

(f) (6 pts) Continuing the setup of the previous part. Now suppose that your friend is told that there are corrupted notes in locations ℓ_1, ℓ_2, ℓ_3.

Show how you can adapt your friend's scheme to deal with this case. (You can assume that $k > 3$.) Explain briefly why this will work.

(HINT: You just have to change e to make everything work.)

Solutions: We just use the previous scheme except we make $e = p_{\ell_1} p_{\ell_2} p_{\ell_3}$.

The argument above only relied on a couple of facts. First, that indeed we zero out all the equations that correspond to corrupted notes. That still holds because any multiple of e is also a multiple of p_{ℓ_j} for $j = 1, 2, 3$. The uncorrupted notes give rise to valid equations that are solved by $q = pe$ just as above. This means that we know $q \equiv ep \pmod{M}$ just as in the previous part.

Notice that the argument used to show $ep < M$ continues to hold since $k > 3$ so there is plenty of headroom so the $ep < eN < M$ argument continues to hold with no modification.

(g) (12 pts) Now, nobody is going to tell you exactly which notes are corrupted. However, suppose that someone gives you a function that can magically find all integer solutions (e, q, z) to constrained equations of the form $ae + bq + gz = d$ where you get to pick interval constraints for the e, q, z of the form $e \in [0, e_u]$ and $q \in [0, q_u]$ while $z \in (-\infty, +\infty)$ is unconstrained. This function takes in integer arguments (a, b, g, d, e_u, q_u).

Describe how you could use this function exactly once to help you decode the underlying message p from a list of received notes $r_1, r_2, \ldots, r_{n+2k}$ where at most c of the notes have been corrupted away from their original values of $y_i = p \bmod p_i$. You know that $c < k$ in advance and if it helps, feel free to assume that both n and k are moderate sized numbers like 100 or 10, and think about c as being something like 3.

What arguments would you use for the integers a, b, g, d, e_u, q_u? How would you use the resulting integers e, q, z to find your p? (It is fine if you have to invoke calculations for these arguments, etc. Obviously, the received notes are going to be involved in some fashion.)

HINT: Think about what q and e mean in the previous part. What do you know about how big those q and e could be? Think about how you go back and forth between writing a system of CRT equations and writing something in mod math. Think about how you write an equality of the form $f \equiv g \pmod{M}$ in the form of an equality involving an unknown integer.

The numbers N and M defined in earlier parts might be useful as could the number $H = \prod_{i=n+2k-c+1}^{n+2k} p_i$.

Also, you might find it helpful to glance at the next part before starting this one.

Solutions: The key to understanding this is the realization that the previous parts were using the CRT as a way to calculate a $q \equiv pe \pmod{M}$ and making sure that the resulting q and pe were small enough so that neither would wrap around to cause trouble.

So, let's assume that we want the answer to be $e = \prod_{j=1}^{c} p_{\ell_j}$ where ℓ_j represents the location of the j-th corrupt note. Clearly, the biggest e could be is the product of the c biggest primes in our set, and that is represented by the number H above. Consequently, the upper bound $e_u = H$.

With an error-locating number e that big, the biggest that $q = pe$ could be is NH since $p < N$ and $e < H$. This means that we are safe using $q_u = NH$.

What remains is to find the linear equation itself. To do this, we can follow the hint and move back and forth between the CRT equations earlier and an expression in mod math. We know that the CRT equations earlier had er_i on the right hand side:

$$q \bmod p_i = er_i \bmod p_i$$

Viewing this as coming from the representation in CRT coordinates, and recognizing that scalar multiplication by an integer can be applied componentwise in the CRT representation, we know that all of these equations are simply expressing:

$$q \bmod M = er \bmod M$$

where the r is the unique CRT solution that is less than M and treats all the received notes as though they were valid. (Since that means $r \bmod p_i = r_i$.)

Taking the above expression and rewriting using mod equivalence we see:

$$q \equiv er \pmod{M}$$

which is the same as saying there exists an integer z so that

$$q = re + zM. \tag{1}$$

Bringing this into the form our magical function wants, we get $re - q + Mz = 0$ as the equation we want to solve for suitably small natural numbers e and q and arbitrary integer z.

So, we want to use $a = r, b = -1, g = M$ together with the $e_u = H$ and $q_u = NH$ we saw before.

Once we call the magical function with these arguments, it must return to us a pair of small enough q, e that satisfy $q \equiv re \pmod{M}$. Whatever the true error-locator number $e_{true} = \prod_{j=1}^{c} p_{\ell_j}$ was, it together with $p_{true} = e_{true}p$ certainly solve the above equation while being small enough.

We didn't expect anyone to go beyond the above point. However, in reality, a question remains: could there could be any other such solutions that are small enough and for which we can't just divide the resulting q' by e' to get p?

Suppose there was another solution pair q', e' to (1). Now consider the difference $q_{true}e' - q'e_{true}$.

First, notice that:

$$q_{true}e' \equiv re_{true}e' \pmod{M}$$

and

$$q'e_{true} \equiv re'e_{true} \pmod{M}$$

and since both equal the same thing, their difference equals zero mod M. (Can you feel the complete parallels to the arguments we did in lecture and in the note?)

But we also know that

$$\begin{aligned} q'e_{true} - q'e_{true} &\equiv pe_{true}e' - q'e_{true} \pmod{M} \\ &\equiv e_{true}(e'p - q') \pmod{M} \end{aligned}$$

Putting these together, we see that

$$e_{true}(e'p - q') \equiv 0 \pmod{M} \tag{2}$$

Remember e_{true} is a product of (at most) c primes that mark the corrupt locations. So for (2) to happen, there must exist an integer w so that

$$e'p - q' \equiv w \prod_{e_{true} \bmod p_j \neq 0} p_j \pmod{M} \tag{3}$$

since M is the product of all these primes. Here, the fact that $e'p < NH$ and $q' < NH$ is enough to prevent (3) from happening in a nontrivial manner since there are at least $n + 2k - c > n + k + 1$

non-corrupt primes and there are only $n+c < n+k$ primes in the product that defines NH. Since all these primes are about equally sized, the only way (3) can happen is if $w = 0$, in which case we have $e'p - q' \equiv 0 \pmod{M}$. By the same argument of sizes, this means that $e'p - q' = 0$ and so we are done since that means that $\frac{q'}{e'} = p$.

Here, we have seen how everything is a direct parallel to what we did with polynomials down at the level of the proofs. Which is the moral of EECS 16A, 16B, and 70: for engineers in our field, the proofs matter more than the theorems or results or formulas. That is why we need you to work this hard in these courses and why our questions ask you to do things that you have never seen before in lecture or discussion. Because those are the skills that we are actually trying to get you to learn. Consequently, we need to have a few exam questions that you've never seen before too.

(h) (8 pts) **Describe the relationship of what is happening in this problem with the Berlekamp-Welch approach to dealing with up to k malicious errors in the polynomial-based error-correcting codes that you learned about in the course.**

- **What are analogous to the $P(x), Q(x), E(x)$ polynomials?**
- **What are analogous to evaluations of polynomials?**
- **What is analogous to the maximum degrees of $P(x), Q(x), E(x)$?**

HINT: This entire part can be viewed as a hint for the previous part.

Solutions: The analogies are almost complete.

- The quantities p, q, e are analogous to the $P(x), Q(x), E(x)$ polynomials. The natural number p contains the message itself, just as the polynomial $P(x)$ encodes the message in Reed-Solomon coding. The quantity e tells you where the corruptions are just as the error-locator polynomial $E(x)$ does in Reed-Solomon coding. And the quantity q is what you end up solving for using the appropriate linear equation, so that you can divide by e to get what you want. Just as we find $Q(x)$ and divide by $E(x)$ to get the message in Reed-Solomon decoding.
- Modding a number by the prime p_i is analogous to evaluating a polynomial at the point i. There are $n+2k$ primes just as there were $n+2k$ points to evaluate at for Reed-Solomon codes.
- The maximum possible sizes of the integers p, q, e play the role of the maximum degrees of $P(x), Q(x), E(x)$. The fact that $p < N$ plays the role of the fact that $P(x)$ has a maximum degree of $n-1$. The fact that $e < H$ plays the role of saying that $E(x)$ has a maximum degree of c if we expect c corruptions. The idea that we are looking for a suitably small $q < NH$ plays the role of the fact that we seek out a polynomial $Q(x)$ in Berlekamp-Belch decoding whose maximum degree is $n+c$ if there are c corruptions.

A tiny shade of difference comes from the fact that with polynomials, we could let c go all the way up to k while for this code, because the primes are only about the same size and not exactly the same size, we have to keep $c < k$ in our scheme.

But as you notice above, the proof works in a completely analogous way as the polynomial case. The properties given to us by the CRT allowing us to uniquely determine small enough numbers given that their mods agree at enough places.

It is out of the scope of this course, but it turns out that the "magic" techniques used to solve the constrained mod-math linear equation that we get are intimately connected to the EGCD algorithm, as we had you see that it works for real numbers too. These ideas are related to a concept called "continued fractions" (that are a staple of math contests, but otherwise not usually studied by students before 70) whose properties can be used to solve that equation through a very clever reduction to a specific continued fraction problem.

The beauty of mathematics comes from the deep interconnections between its various parts. This problem only hints at the spectacular vistas that exist within the mathematics related to what goes on in the EECS department.

Contributors:

- Yiming Ding.
- Jonathan Lin.
- Babak Ayazifar.
- Edward Im.
- Amin Ghafari.
- Anant Sahai.

