CSCI0220 Practice Final Exam

Please read in full:

The following practice exam will look somewhat different from the one you receive on exam day. This practice exam is derived from last year's final, which was an untimed takehome. The in-class exam this year will cover similar information and be of similar difficulty in questions, but will be designed and formatted for an in-class exam. *You should not draw any conclusions about the length of the exam from this practice exam.*

It's a good idea to try the exam first by yourself, and then read over the solutions.

Problem 1

Let G be a graph with vertices V and edges E. Let R be a binary relation on V, such that $R(x, y)$ holds if and only if $\{x, y\} \in E$.

a. We are going to write down formulas in predicate logic (using quantifiers) that describe properties of G. For instance, $\forall x R(x, x)$ expresses that "every vertex has an edge to itself." (Note, this can't be true, since our definition of graphs does not allow "loop" edges.) For each of the following properties, write down a formula that is true if and only if G has that property.

   i. G is not a complete graph.

   ii. There is a path of length 3 between every pair of vertices in G.

   iii. Not every vertex of G has positive degree.

b. Is property (iii) above the same as saying "G is connected"? Explain why, or provide a counterexample.

c. Draw a graph with at least five vertices that has a Hamiltonian tour but does not have an Eulerian tour. Explain why your graph satisfies both of these properties.

Problem 2

a. Use the extended Euclidean algorithm to compute the GCD of 46 and 108 and express it as a linear combination of these values. Show us all your work.

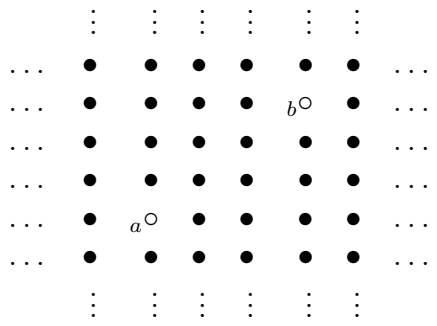
b. Encode a message using RSA for us: Choose values p and q (between 10 and 30—let's keep it simple) that determine the modulus $n = p \cdot q$, a public key e, a private key d, and a message m. Produce the encrypted message m^*. Show us all of these values, and any work that went in to producing them. (Outside of a CS22 exam, you should never share your public key!)

   We are not looking for a complex example. We just want to see you demonstrate the RSA scheme.

Problem 4

a. Consider a grid of dots that is infinite in all directions. Pick one dot and label it a; find the dot three steps above and three steps right and label it b.

How many paths of length 8 connect a to b? Explain your answer. The length of a path is the number of "hops" between points on that path. A hop can be a move one dot up, down, left, or right—no diagonal hops, and no skipping points.



b. Now suppose that b is n steps above and k steps right of a. What is the minimum length of a path from a to b? How many paths are there with this length? Why?

c. Prove that if $|k - n| > 1$ then there will be at least two consecutive up steps or two consecutive right steps in every path with minimal length.

Problem 5

Let A be a set, and $B = (B_1, \ldots, B_k)$ be a sequence of subsets of A. We say that B is a *nested* sequence of subsets of A if $B_i \subset B_{i+1}$ for each $i < k$. (We use the strict subset relation $\subset$ which implies $B_i \neq B_{i+1}$.) For example, $(\{\}, \{2\}, \{1, 2, 3\})$ is a nested sequence of subsets of $\{1, 2, 3\}$.

a. What is the maximum length of a nested sequence of subsets of $\{1, 2, \ldots, n\}$? Describe what such a nested sequence must look like. Prove that there can not be any longer nested sequence.

b. How many nested sequences of subsets of $\{1, 2, \ldots, n\}$ are there with this maximum length? Why?

c. I pick two subsets $B_1, B_2 \subseteq \{1, 2, \ldots, n\}$ uniformly at random. What is the probability that the sequence (B_1, B_2) is nested? You may express your solution symbolically (with a summation, binomial coefficients, or anything else you need), but explain how you got to that answer.

Problem 6

Ringo loves to shout out numbers between 1 and 12 (inclusive). He thinks he's good at doing this, but in fact, he's twice as likely to shout out an even number than an odd one. (Any two even numbers are equally likely, as are any two odd numbers.) We'll use probability theory to analyze the numbers he shouts out.

a. In scenario 1, you walk up to Ringo and ask him to shout out exactly one number.

   i. Let's model this as a probability space. What is the sample space? What is the probability of each outcome?

   ii. Remember that an *event* is a set of outcomes. Write down (as a set) the event that the square of Ringo's response is less than 10 or greater than 100. What is the probability of this event?

b. In scenario 2, you ask Ringo to keep shouting numbers until he shouts 12, writing down the sequence of numbers as he goes.

   i. Again, what is the sample space? (You do not need to write down the probability of each outcome here!)

   ii. What is the probability that Ringo shouts at least three numbers and at least one of the first three numbers is 4?

c. In scenario 3, you ask Ringo to shout exactly six numbers. What is the expected value of the sum of the numbers he shouts?

d. After all this testing, Ringo has improved: When you ask him to choose numbers between 1 and 6, he now chooses with uniform probability. In scenario 4, you ask him for three numbers, this time between 1 and 6. Is it more likely that the sum of the three numbers will be 11 or 12? Why?

