CS 2200 Assignment - 1

Instructor Avah Banerjee
Due Date. Sep 16 12:00 Noon

Your answers should not contain any handwritten parts. All relevant written sections should be typed and compiled into a single PDF, including screenshots, code, and figures where applicable.

Problem 1, (15 x 3 = 45 Pts) Go to the Lean Game Server. There, you will find three interactive games about natural numbers, set theory, and logic. Your goal is to play and complete all three games. You do not need to play the game titled "Robo" (it's about interactive proof). When you play a game, in the left window pane of the game UI, there will be a transcription of the various moves you made, along with how many times you used hints to figure out the next steps. You need to submit this transcript as part of your evidence that you have completed all the levels of the three games. The fewer hints you use, the higher your score will be.

Problem 2, (25 Pts) In a complex political landscape, a diplomat is navigating the intricate corridors of power in a foreign nation. The diplomat finds herself at a critical juncture, needing to choose the right policy path that will lead to a successful negotiation with the government. In this delicate situation, she encounters three political advisors, each from a different faction within the government: one who always tells the truth, one who always lies, and one who gives completely unpredictable answers. Unfortunately, the diplomat doesn't know which advisor belongs to which faction.

To make matters more complicated, the diplomat is permitted to ask only two yes-or-no questions, and each question must be directed to a single advisor. Can the diplomat figure out which policy path will lead to a successful negotiation?

Bonus question (10 Pts) Describe the situation using first-order logic and formally prove that your strategy is valid.

Problem 3, (30 Pts) We can think of a proof (particularly in the context of computer science) more generally as some evidence that proves a hypothesis. Now suppose there are two parties, Alice and Bob. Alice works at Property Testing Inc., where she is given an object X (in this case, a pair of labeled graphs G_1, G_2) and has to determine if the object has some property T (whether the graph G_1 is non-isomorphic to the graph G_2).

Bob also works at Property Testing Inc. and has developed a reputation over several years. Instead of testing properties using the standard property testing methods employed by the company, Bob simply guesses whether a given object has the property. Normally,

someone like that would get fired pretty quickly, but in Bob's case, he seems to always guess correctly. Bob insists that he doesn't just guess but has a way to generate a valid proof, though he has declined to share his proofs so far.

Alice has observed Bob for some time now and wants to get to the bottom of Bob's bag of tricks. She believes that if Bob can always generate a valid proof, there must be a systematic way for Bob to convince Alice of this without revealing his proof. So, Alice comes up with the following game that she wants to play with Bob:

Alice is given two graphs, G_1 and G_2, and needs to determine if they are non-isomorphic, meaning that no relabeling of vertices in G_1 will make it identical to G_2. Bob claims he can prove that the two graphs are non-isomorphic without revealing any specific details about how he knows this.

To test Bob's claim, Alice devises the following protocol:

1. Alice randomly chooses one of the two graphs, G_1 or G_2, and gives Bob a randomly permuted version of that graph, G', without revealing which graph she chose or how the vertices were relabeled.

2. Alice then asks Bob to identify whether G' is the permuted version of G_1 or G_2, effectively proving that he can distinguish between the two graphs.

3. If Bob correctly identifies which graph G' corresponds to, Alice can conclude that Bob knows the graphs are non-isomorphic. However, Bob must do this without revealing any details about the specific differences (thus revealing a part of his secret proof) between G_1 and G_2.

4. Bob can convince Alice by consistently identifying the correct graph, thereby demonstrating that he knows the two graphs are non-isomorphic, even though Alice never sees the actual proof.

Alice repeats this process multiple times, each time randomly choosing one of the two graphs and permuting it. If Bob can consistently identify the correct graph, Alice will be persuaded that the graphs G_1 and G_2 are indeed non-isomorphic. Can Bob successfully demonstrate that the two graphs G_1 and G_2 are non-isomorphic without revealing any specific details of his proof, using the above protocol?