CS 2110 Final Exam
Fall 2010

Directions

1. The test is closed book and closed notes.
2. The test consists of 10 questions, each with a part (a) and a part (b).
3. Answer at most 8 part (a) questions. These are worth 10 points each.
4. Answer at most 4 part (b) questions. These are worth 20 points each.
5. If you are not reaonably certain of your answers, please don't take random guesses. It is better just to leave it blank.
6. You don't need to give every single detail in your answers, just hit the main points. Part (a) questions should be answered in say 1 to 4 sentences.
7. Please concentrate on providing clear answers to the questions that you have time to answer, rather than on answering the maximum number of questions. It could well be that it is not reasonable to provide reasonable answers to the maximum number of questions within the allotted time.

1. (a) State Godel's Incompleteness Theorem.
   (b) Sketch the proof of Godel's Incompleteness Theorem that uses the fact that there is no algorithm for the Halting Problem. This proof involves the construction of a formula Φ. You do not need to explain how to construct Φ, you need only explain what properties Φ has.

2. (a) Define Kolmogorov complexity.
   (b) Prove that there is no algorithm that can determine the Kolmogorov complexity of a string.

3. (a) Draw a Venn diagram showing the inclusion relationship between the complexity classes: log space, polynomial time, Σ_1^p, Π_1^p, Σ_2^p, Π_1^p, and polynomial space. State which inclusions are known to be proper/strict.
   (b) Prove the strictness of these inclusions from first principles.

4. (a) Give an example of a "logic problem" that is known to be polynomial-time complete for the complexity class of polynomial space.
   (b) Prove from first principles that this problem is complete for polynomial space.

5. (a) Define $P/poly$, uniform NC, and non-uniform NC.
   (b) Show that if $NP \subset P/poly$ then $\Pi_2^p = \Sigma_2^p$.

6. (a) Define the randomized complexity classes RP, $co-RP$, ZPP and BPP.
   (b) Prove $ZPP = RP \cap co-RP$.

7. (a) Define $IP[k]$. That is, define what a k round interactive protocol is. How do you decide who sends the first message in such a protocol?
   (b) Give an $IP[10]$ protocol that takes as input a propositional Boolean formula F and an integer k, and accepts if the number of satisfying assignments to F is at least k and rejects if the number of satisfying assignments to F is less than $k/2$. The protocol may accept or reject if the number of satisfying assignments is in between $k/2$ and k. Give some intuition (not necessarily a formal proof) why this protocol is correct.

8. (a) Define what is meant by "semantic security" within the context of a cryptographic protocol.
   (b) Construct a direct acyclic graph where the nodes represent the following statements:
      i. One time pad private key cryptography with short keys is possible
      ii. BPP algorithms can be derandomized to give subexponential time deterministic algorithms
      iii. Public key cryptography is possible
      iv. One-way functions exist
      v. Pseudo-random generators exist

   where a directed edge (x, y) from a vertex x to a vertex y means that statement x logically implies statement y. If your graph contains edges $(x.y)$ and (y, z), then it shouldn't contain the edge (x, z) as this is a logical consequence. So in some sense your graph should have the minimal number of edges. Prove one of the implications (hint: Pick an easy implication. Some of these implications are very easy to prove and some are very hard to prove).

9. (a) Explain the EPR experiment. You can just explain what Alice can Bob are supposed to accomplish, not how they accomplish it. Why is this protocol famous? Or two ask the question a different way, what did the textbook want us to learn from this example?

   (b) Give Alice and Bob's protocol from the text. Calculate the probability of Bob and Alice winning given that they see different inputs. Show your work.

10. (a) When proving $NP \subset PCP(poly, 1)$, explain how error correcting codes come into the picture. Start with a definition of $PCP(poly, 1)$.

    (b) To prove that $NP \subset PCP(poly, 1)$ the book showed that an NP-complete problem was in $PCP(poly, 1)$. This NP-comlete problem involved showing that there were 0/1 solutions to a sequence of equations. Part of the protocol involved checking the 0/1 assignment to the variables. Explain how the assignment was encoded, using 011 as an example assignment. Explain what property of this encoding is checked, how it is checked, and why this check works.