CS 2110 Final Exam and Theory of Computation Preliminary Exam
Fall 2008

Directions

1. The test is closed book and closed notes.
2. Answer at most 8 part B questions. Part B questions are worth 20 points each.
3. Answer at most 2 part A questions. Part A questions are worth 40 points each.
4. One quarter credit will be given for unanswered questions. Answers that are way off the mark will get no credit.
5. For the part A questions, usually it is then a good idea to have a paragraph giving an overview of the proof strategy/technique that you will use, and what the key ideas are, before launching into the details.

PART B Questions

1. The following sentence is essentially from a paper on the P vs. NP problem from the arXiv archive, "It has been previously demonstrated by the present author that the DNA string concatenation problem can be reduced to the problem of finding a large clique in a graph, and therefore the DNA concatenation problem is NP-Complete." Explain the error with this reasoning.

2. Explain the famous result of Baker, Gill and Soloway from the 1970's. Explain the relevance of this result for resolving the P vs. NP question.

3. Explain Nash's famous theorem about games. Start with a definition of a game that is appropriate for this setting.

4. Consider the following situation. Alice needs to flip a fair coin until she gets a heads. Let k be the number of flips until Alice sees a heads. Alice needs to send some bits to Bob over a network connection in order to communicate k to Bob. Alice and Bob can communicate a priori to determine their protocol. Give an expression for the expected number of bits that Alice must send to Bob. Explain why you know that approximately this many bits is necessary and sufficient.

   Note that I am not asking for a protocol, or a proof that a certain number is necessary. I am looking for you to cite and explain well known theorem that we covered in class.

5. For which of the following two complexity classes is it likely easier to find a complete problem. Explain your answer. PP is the class of languages L for which which there exists a probabilistic polynomial time Turing machine M such that if $x \in L$ then M accepts x with probability $> 1/2$, and if $x \notin L$ then M accepts x with probability $< 1/2$. QQ is the class of languages L for which which there exists a probabilistic polynomial time Turing machine M such that if $x \in L$ then M accepts x with probability $\geq 1/2$, and if $x \notin L$ then M accepts x with probability $< 1/2$.

6. Consider the following language: $\{(G, k)$: The largest simple cycle in graph G contains exactly k edges $\}$. Show that this language is in Σ_2^p. Start with a definition of Σ_2^p.

7. Is P is a subset of $P/poly$? Is $P/poly$ is a subset of P? Start with Definitions of P and $P/poly$. Then give one sentence justifications for your answer to each question.

8. Results by Soloway and Strassen in the mid 1970's and by Shor in the mid 1990's had analogous effects on computer scientists understanding of efficient computation. In one sentence, state each result. Then explain what the analogous effect of each result was.

9. Define what a "perfect zero knowledge" protocol is.

10. Explain why BPP is contained in $P/poly$. Start with a definition of BPP and $P/poly$.

11. State a problem that is complete for the class P with respect to NC reductions. Define NC.

12. Explain why the existence of a really good pseudo-random generator would allow one to conclude that $BPP = P$. Start with definitions of BPP and pseudo-random generator.

13. Give the interactive protocol for the graph nonisomorphism problem from the book and class. You need not argue about the correctness of the protocol, just try to state it clearly.

14. Explain the setup of experiment with the 1/2 silvered mirrors that we discussed in class when we first discussed quantum computation. What is unexpected outcome when one carries out this experiment. Briefly explain why this outcome occurs.

15. You have two entangled qubits in state: $a|00> + b|01> + c|10> + d|11>$. Answer the following questions. You need not justify your answers.

    - What must be true about the relationship of the values a, b, c, and d?
    - If you measure the first qubit, what is the probability that you observe a 0?
    - If you measure the first qubit and observe a 0, what is the resulting state of the two bits?
    - If $b = c = 0$, and you rotated the first bit by $\pi/4$ radians, what be the resulting state of the bits. You can write an expression for the state, you need not simplify.

16. The PCP theorem gives an alternative characterization of the complexity class NP. State the PCP theorem, and give a definition of the type of machine/protocol/system in the alternative characterization.

PART A Questions

1. Prove from first principles that there are languages that can be accepted in exponential time that can not be accepted in polynomial time.

2. State Gödel's incompleteness theorem, and show that it follows as a logical consequence of the fact that the halting problem is not computable/decidable.

3. Give the perfect zero-knowledge protocol for graph isomorphism from the book and prove that the protocol is perfect zero knowledge.

4. Prove from first principles that the circuit satisfiability problem is NP-hard. The circuit satisfiable problem takes as input a circuit and asks whether there is any inputs to the circuit that cause a particular output to be 1. So basically I am asking you to give a proof of Cook's theorem here.

5. Prove that if NP has polynomial time circuits then the polynomial time hierarchy collapses.

6. Prove that if graph isomorphism is NP-hard then the polynomial time hierarchy collapses.

7. State what problem Simon's algorithm solves. Give Simon's algorithm. Prove that it solves this problem. Prove that Simon's algorithm runs in polynomial time.

8. Prove that there exists some constant γ, such that it is NP-hard to approximate MAXSAT to within a factor of γ. You may assume the PCP theorem.