CS 1511/2110 Midterm 2
Spring 2017

Directions

1. The test is closed book and closed notes.
2. There are 8 part B questions. Answer at most 6 part B questions. Please try to limit your answers to one sentence. Part B questions are worth 10 points per question.
3. There are 4 part A questions. Answer at most 2 part A questions. Part A questions are worth 20 points per question.
4. Time will likely be an issue for most students. So use time wisely. Initially concentrate on the main ideas, and then fill in details with any remaining time.
5. In particular, for the part A questions, usually it is then a good idea for the start of your answer to define relevant terms, give an overview of the proof strategy/technique that you will use, and to explain the key ideas are. After this, you may launch into details.

PART B Questions

1. (a) Formally define the complexity class ZPP.
   (b) Formally define the complexity class co-RP.
   (c) Draw a Venn diagram fully illustrating all known inclusion relationships between the complexity classes BPP, RP, co-RP, and ZPP.

2. State the interactive set size protocol discussed in the text and in class. Recall that the goal of this protocol was to differentiate between that case that some set S had more than k elements from the case that S had less than $k/2$ elements. So you need to state what is sent in each message, and what computation is performed by the verifier to determine whether whether it accepts or rejects. You do not need to discuss the analysis of the protocol. For full credit, your protocol should only send a polynomially bounded number of bits.

3. (a) Informally define what a pseudo-random generator is.
   (b) Formally define pseudo-random generator. So I am looking for a definition in first order logic. The first thing that I will check is that you have the right quantifiers in the right order.

4. (a) Give a diagram to show which of the following statements imply other statements. So I'm looking for an organized list of implications, e.g. $(i) \Longrightarrow (iii)$, $(iv) \Longrightarrow (ii)$, etc.
      i. The existence of good pseudo-random generators
      ii. $P \neq NP$
      iii. The existence of computationally secure private key cryptography with small keys
      iv. The existence of secure public key cryptography
      v. The existence of one-way functions
   (b) Pick one of these implications, and explain why it is true. Make sure to identify the implication you are explaining, and define the relevant terms.

5. Assume two entangled qubits are in the state

$$a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle$$

   Here a, b, c and d are real numbers.
   (a) What must be true about a, b, c and d?
   (b) What is the probability that you observe a 1 if you measure the first qubit?
   (c) Conditioned on the fact that you observe a 1 when you measure the first qubit, what is the resulting state of the two qubits?

6. (a) State the problem solved by Simon's algorithm (recall that this algorithm is discussed in the quantum computing section in the text).
   (b) How many queries are required to solve this problem deterministically?
   (c) How many queries by are required to solve this problem with high probability using a randomized algorithm?
   (d) How many queries are required by Simon's algorithm to solve this problem with high probability?

7. (a) Describe an interactive proof for graph non-isomorphism. So you need to state what is sent in each message, and what computation is performed by the verifier to determine whether whether it accepts or rejects. You do not need to discuss the analysis of the protocol.

   (b) Explain how to convert this into a probabilistically checkable proof. So you need to describe how the prover determines what bits to put in the book, and how the verifier will use the book.

8. In class and in the text it was show that the NP-complete language QUADEQ was in $PCP(poly(n), 1)$. Assume that you have an instance of QUADEQ that has a solution $u_1 = 1$, $u_2 = 1$, $u_3 = 1$, and $u_4 = 0$. Calculate the number of bits in the resulting probabilistic proof (the bits written in the book for the verifier to read). Justify your answer, and show your work.

PART A Questions

1. Prove BPP is contained in Σ_2^p. Start by defining the terms. Then give an overview of the proof technique you will use.

2. Let (D, E) be a private key encryption scheme. So $D(E(x, y), y) = x$ for every possible message x and every possible key y. Prove that if the number of bits, let us denote this by m, is strictly greater than the number of bits in the key, let us denote this by k, then (D, E) does not achieve perfect secrecy. Of course you should start by defining perfect secrecy. Then give an overview of the proof technique you will use.

3. (a) Explain the Elitzur-Vaidman bomb testing experiment.

   (b) Assume that a real bomb is tested with the experiment. What is the probability that it will explode? What is the probability that it will not explode, but can be definitively identified as a real bomb? Show your work.

   (c) (5 points extra credit) Assume there are n bombs, half of which are duds, and half of which are working bombs. How many real bombs can be identified without exploding them. Show your work. This is extra credit because it was covered in the notes but not in class.

4. Consider the following problem: Given a system of linear equations in n variables with coefficients that are rational numbers, determine the largest subset of equations that are simultaneously satisfiable. Show that there is a constant $\rho < 1$ such that approximating the size of this subset to within a ρ factor is NP-hard. Use the fact that it is known that there is a constant $\sigma < 1$ such that approximating MAX-SAT to within a factor of σ is NP-hard. Start by explaining the proof technique you will use.

   Note that "equation" in this context means that the relation is equality. So one possible equation might be $1.5x + 2y + 2.5z = 10.5$. Note that rational solutions are allowed. So $x = 2$, $y = .5$ and $z = 3$ is an allowable solution.