CS 1511/2110 Midterm 2
Spring 2018

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 or two sentences. 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.
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. If there is sufficient time, you may then start filling in the details.

PART B Questions

1. Consider the proof from the text and from class to show that TQBF was in IP, and the following TQBF formula:

$$\exists x \forall y \exists z \ (\neg x \vee y \vee z) \wedge (x \vee \neg y \vee \neg z)$$

   (a) The non-quantified part:

$$(\neg x \vee y \vee z) \wedge (x \vee \neg y \vee \neg z)$$

   was converted into a polynomial. State this polynomial. You do not need to simply the polynomial in any way. Just write the polynomial in the most natural way.

   (b) The interactive protocol started with the prover sending the verifier an integer. Give the integer that would be sent in this case. Show your work.

2. The problem of deciding whether two graphs are isomorphic is probably the most famous problem in NP that is neither known to have a polynomial-time algorithm, nor known to be NP-complete. The discovery of interactive proofs lead to some circumstantial evidence that probably graph isomorphism is not NP-complete. State what this evidence is.

3. (a) Explain the bit commitment protocol that we discussed in class and in the book, which is based on the existence of a one-way permutation f. To explain the protocol it is sufficient to describe the messages that are sent between Alice and Bob.

   (b) Informally explain why neither Alice nor Bob can cheat.

4. (a) Informally define pseudo-random generator.

   (b) Formally define pseudo-random generator.

   (c) Informally define unpredictable generator.

   (d) Formally define unpredictable generator.

   (e) Is a pseudo-random generator necessarily an unpredictable generator? You need not justify your answer.

   (f) Is an unpredictable generator necessarily a pseudo-random generator? You need not justify your answer.

5. Consider the half-silvered mirrors experiment that we discussed in class.

   (a) What matrix represents a horizontally moving photon?

   (b) What matrix represents a vertically moving photon?

   (c) What matrix represents a full-silvered mirror?

   (d) What matrix represents a half-silvered mirror?

   (e) Show the sequence of matrices that are multiplied to determine the state of the photon after the second half silvered mirror, assuming the particle entered horizontally.

6. (a) In class and in the text and in class we discussed how to produce two entangled qubits from one qubit in state $(|0\rangle + |1\rangle)/\sqrt{2}$ and one reversible gate. Explain how this is accomplished. That is, state what the gate is, what the inputs to the gate are, and then what the resulting output will be.

(b) In the quantum algorithm for the Parity Game (EPR Experiment) discussed in class and in the text, Alice and Bob initially each took one of two entangled bits with them when they started traveling. In some situations, Alice would later perform a particular operation on her entangled bit. State in English what this operation was.

(c) Give the matrix that represents this operation.

7. (a) Define what it means for a randomized algorithm to be a 1/2-approximation (or 2-approximation depending on how one does the ratio) for MAX-SAT

   (b) Give a randomized algorithm that produces a 1/2-approximation (or 2-approximation depending on how one does the ratio) for the MAX-SAT problem.

   (c) Prove that there is no polynomial time algorithm A that can guarantee that that the number of clauses it satisfies in a MAX-SAT instance is at least the optimal number of clauses that are simultaneously satisfiable minus 10.

8. Consider the probabilistically checkable proof, verifiable by a $(poly(n), O(1))$-verifier, given in the text and in class for the language QUADEQ, which asked whether a collection of quadratic equations had a 0/1 solution. For a QUADEQ instance with n variables, the book/proof consisted of two parts, the first part had 2^n bits and the second part had 2^{n^2} bits. This question focuses on the second part of the book. Assume for the purpose of this question that the prover has correctly encoded an assignment of the variables in the book, although this assignment may not satisfy all equations.

   (a) Assume $n = 2$. For the assignment $u_1 = 1$, and $u_2 = 1$, give the $2^4 = 16$ bits in the second part of the book. Show your work.

   (b) Explain which page in the book the verifier will look at to determine the value of the equation $u_1u_1 + u_2u_2$.

   (c) Explain how the verifier checks that the assignment to the variables indeed solves all the equations in the QUADEQ instance.

   (d) If the assignment does not satisfy all equations, what is the probability that the above check will catch the error?

PART A Questions

1. Prove that the language GNI, the language of pairs of non-isomorphic graphs, is in AM. Start with a definition of AM.

   Hint: Be careful. Not every interactive protocol is an AM protocol. In particular, the first interactive protocol that we learned for GNI is not an AM protocol.

2. Let $f(x)$ be a one-way permutation that maps n bits to n bits. Recursively define $f^{(1)}(x) = f(x)$ and for $i > 1$ define $f^{(i)}(x) = f(f^{(i-1)}(x))$. Prove that $f^{(n)}(x)$ is a one-way permutation.

3. State the problem that Simon's algorithm solves. State Simon's algorithm.

4. Consider the following problem. The input is a collection of linear equalities with rational coefficients. For example,

   $$2x + y/3 + 2z/7 = 7/6$$

   $$2y - 4z/3 = 11/3$$

   The objective is to find an assignment to the variables that satisfies as many equations as possible. Prove that there exists a δ such that it is NP-hard to approximate this within a factor of $1 + \delta$. Use the fact that there exists a ϵ such that it is NP-hard to approximate MAX-SAT within a factor of $1 + \epsilon$.