CS 4390/5353, Quantum Computing, Test 2

October 21, 2004

Name: .....

Conditions: No books allowed; you can use 5 pages of handwritten notes.

1. Grover's algorithm.

   1a. Describe what problem is solved by the Grover's algorithm, i.e., what is the input and what is the desired output.

   1b. Explain in what sense this algorithm is better than non-quantum algorithms for solving the same problem.

   1c. Describe the main steps of Grover's algorithm.

2. Show, on the example of looking for an element with the desired property in a 4-element array, that Grover's algorithm indeed finds the desired element *fast*. Show it on the example when the desired element is the element 01.

4. Suppose that we are solving a problem for which it is easy to check whether a candidate is indeed a solution, and we have a probabilistic algorithm that solves this problem with the probability $p_0 = 90\%$. How many times do we need to repeat this algorithm to achieve the probability $p_d = 99.9\%$ of the correct solution? Describe a general formula for the number of repetitions as a function of p_0 and p_d.

5–6. Describe the main steps of the RSA algorithm. On the example of the message $M = 10$ and of the public code (n, e), with $n = 21$ and $e = 5$, show, step by step, how we generate the secret code, how we encode the message, and how we decode the message.

7. Shor's algorithm.

   7a. Describe what problem is solved by the Shor's algorithm, i.e., what is the input and what is the desired output.

   7b. Describe why this problem is practically important.

   7c. Explain in what sense this algorithm is better than non-quantum algorithms for solving the same problem.

   7d. Describe the main steps of Shor's algorithm.

8. Briefly describe what progress you have made so far on your project.

9. *For extra credit:* Use geometry to describe how many iterations we need for Grover's algorithm.