CS 4390/5353
Quantum Computing
Final Exam

Thursday, December 10, 2009, 4-6:45 pm

Name:

10 pages of notes allowed.

1. Describe negation and conjunction ("and") as Toffoli gates; write down the truth tables for these gates.

2. Compute the probability of 0 and 1 for the following state:

$$\frac{3}{5}|0\rangle - \frac{4 \cdot \mathrm{i}}{5}|1\rangle.$$

Check that it is a physically valid state.

3. Show, step by step, that the Deutsch-Josza algorithm works for $f(x) = x$.

4. Explain, in detail, why there are exactly four classical unary operations.

5. Prove that copying is not possible in quantum computing.

6. Compute the tensor product $s_1 \otimes s_2$ of the state

$$\frac{3}{5}|0\rangle - \frac{4 \cdot \mathrm{i}}{5}|1\rangle$$

with the same state of the second qubit.

7. Show, in detail, how the state

$$\frac{3}{5}|00\rangle - \frac{2}{5}|01\rangle + \frac{2 \cdot \mathrm{i}}{5}|10\rangle + \frac{2\sqrt{2}}{5}|11\rangle$$

will change when we measure the second bit.

8–9. Show how Alice and Bob use quantum cryptography to form a safe onetime pad. Assume that they start with 4 bits, and, for simplicity, that they do not take eavesdropping into account. In generating random message and random bases, and in simulating measurement results, use the bits from following sequence of random bits: 1001 1100 0011 1100 1101 1010 1100 0010 0110 Describe the resulting one-time pad. Show how this pad can be used to send a message consisting of all 1s, and how Bob can decode the resulting message.

10. Run a numerical example of RSA. Assume that we started with prime numbers $p = 11$ and $q = 5$, and that the public key is $e = 7$. Use the general algorithms to compute the private key, to encode the message $M = 9$, and to decode the encoded message E.

11. Show, step-by-step, that Grover's algorithm works on an example when among 4 elements of an array, only one element $a[2] = a[10_2]$ satisfies the desired property.

12. Prove, in detail, that Grover algorithm requires $\sim \sqrt{N}$ steps to find a desired element in an unsorted array of size N. For simplicity, assume that in this array, there is only one element with the desired property.

13. Show, in detail, how we can use Fast Fourier transform to compute the product of two polynomials:

$$A(x) = 1 + 3x + 9x^2 \text{ and } B(x) = 1 - 3x.$$

14. Explain what exactly Shor's algorithm does, and why it is important.

15. Describe, step by step, how computing without computing works.

16. Describe, step by step, how one can teleport a state $\frac{4}{5} \cdot |0\rangle - \frac{3 \cdot \mathrm{i}}{5} \cdot |1\rangle$. Assume that when Alice measures the values of the first two bits, she gets the result 10.

17. Explain why tensor methods are needed when we multiply two large matrices. Show, in detail, how the tensor method works, on the example of multiplying the following two 4×4 matrices:

$$A = \begin{pmatrix} 0 & 3 & 4 & 5 \\ 3 & 4 & 5 & 0 \\ 4 & 5 & 0 & 3 \\ 5 & 0 & 3 & 4 \end{pmatrix}, \quad B = \begin{pmatrix} 5 & 4 & 3 & 0 \\ 4 & 3 & 0 & 5 \\ 3 & 0 & 5 & 4 \\ 0 & 5 & 4 & 3 \end{pmatrix}$$

18. Briefly describe what you did as part of your project for this class.

19. (*For extra credit*) Describe the contents of someone else's project for this class.