

CS 4390/5353
Quantum Computing
Test 1

Tuesday, September 29, 2009

Name:

5 pages of notes allowed.

1. Describe negation and disjunction (“or”) as Toffoli gates; write down the truth tables for these gates.
2. Compute the probability of 0 and 1 for the following state:

$$\frac{\sqrt{3}}{\sqrt{7}}|0\rangle - \frac{2 \cdot i}{\sqrt{7}}|1\rangle.$$

Check that it is a physically valid state.

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

$$\frac{\sqrt{3}}{\sqrt{7}}|0\rangle - \frac{2 \cdot i}{\sqrt{7}}|1\rangle$$

with the same state of the second qubit.

7. Show, in detail, how the state

$$\frac{1}{3}|00\rangle - \frac{1}{3}|01\rangle + \frac{i}{3}|10\rangle + \frac{\sqrt{2}}{\sqrt{3}}|11\rangle$$

will change when we measure the first 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: 1101 1010 1100 0010 0110 1001 1100 0011 1100 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 $p = 3$ and $q = 5$, and that the public key is $e = 5$. Use the general algorithms to compute the private key, to encode the message $M = 7$, and to decode the encoded message E .