PhD Comprehensive examination in Quantum Computation

Department of C&O
University of Waterloo

Examiners: Michele Mosca and Ashwin Nayak
Spring term, July 2, 2003

Instructions

Answer any **six** out of the following seven questions. All questions carry equal weight.

Questions

1. **Quantum key exchange.**

   Describe the steps of the BB84 quantum key exchange protocol, and give the formal statement of its unconditional security.

2. **BQP $\subseteq$ PSPACE.**

   Show that every decision problem that can be solved with bounded error in polynomial time by a quantum algorithm can also be solved by a deterministic classical algorithm that uses polynomial space. How much time and space does your classical algorithm use in terms of the time and space used by the quantum algorithm for the problem?

3. **The nine-qubit Shor code.**

   In the 9-qubit Shor quantum error correcting code, the basis states are encoded as:

$$\begin{aligned} |0\rangle &\mapsto \left(\frac{|000\rangle + |111\rangle}{\sqrt{2}}\right)^{\otimes 3} \\ |1\rangle &\mapsto \left(\frac{|000\rangle - |111\rangle}{\sqrt{2}}\right)^{\otimes 3}. \end{aligned}$$

   (a) Explain how an unknown one qubit superposition can be protected against an arbitrary error in a single qubit using this code.

   (b) Give circuits that implement a logical NOT gate and a logical Z-gate on a qubit encoded with the Shor code.

4. **Universal sets of gates.**

   A *two-level* unitary operator on n qubits is a unitary operator whose restriction to the space spanned by all but two classical basis states is the identity. Show how we can implement any given two-level unitary operator by a quantum circuit consisting of CNOT and single qubit gates.

   (You may assume that every single qubit unitary operator can be decomposed as $AXBXC$, up to an overall phase, where A, B, C are unitary operators such that $ABC = I$.)

5. **Lower bound for quantum search.**

   For a function $f : \{1, 2, \ldots, n\} \to \{0, 1\}$, the search problem consists of determining if there is an index $i \in \{1, 2, \ldots, n\}$ such that $f(i) = 1$. Prove that every quantum algorithm with oracle (or black-box) access to the function f that solves the search problem with bounded error makes $\Omega(\sqrt{n})$ queries to the oracle. What is the implication of this lower bound for quantum algorithms for NP-complete problems?

6. **Communication complexity of Inner Product.**

   The inner product function $\mathrm{IP}_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is defined as

$$\mathrm{IP}_n(x, y) \quad = \quad \sum_{i=1}^{n} x_i \cdot y_i \pmod 2.$$

   Suppose there is a one-message quantum protocol for computing the inner product of two arbitrary n-bit inputs x, y given to Alice and Bob, respectively. Further, suppose that in this protocol Alice sends a pure state $|\phi_x\rangle$ over m qubits (the lone message) to Bob, who can then compute the inner product exactly, i.e., with probability 1.

   (a) Show how Bob can modify his computation so that he can learn Alice's input x from $|\phi_x\rangle$.

   (b) State and justify a non-trivial lower bound for the length m of the message $|\phi_x\rangle$.

7. **Discrete logarithms.**

   Let $G \subseteq \{0,1\}^n$ be a cyclic group of order k generated by an element g. Suppose that G is presented as a black-box. In other words, you are given oracles that implement the multiplication operation, the inverse, and the test for the identity element. You may also assume oracles that can perform controlled versions of these group operations.

   (a) Describe an efficient (polynomial-time) quantum algorithm to compute the discrete logarithm of a specified element $h \in G$, given g and k.

   (b) Devise an efficient algorithm to generate a quantum state that approximates with high fidelity the uniform superposition over all elements of G. Justify its correctness and efficiency.