Quantum Computing Exercises # 9

Ronald de Wolf

April 5, 2011

(to be handed in before or at the start of the lecture on Apr 12)

1. The following problem is a decision version of the factoring problem:

   Given positive integers N and k, decide if N has a prime factor $p \in \{k, \dots, N-1\}$.

   Show that if you can solve this decision problem efficiently (i.e., in time polynomial in the input length $n = \lceil \log N \rceil$), then you can also find the prime factors of N efficiently. *Hint: use binary search, running the algorithm with different choices of k to "zoom in" on the largest prime factor.*

2. (a) Let U be an S-qubit unitary which applies a Hadamard gate to the kth qubit, and identity gates to the other $S-1$ qubits. Let $i, j \in \{0,1\}^S$. Show an efficient way to calculate the matrix-entry $U_{i,j} = \langle i|U|j\rangle$ (note: even though U is a tensor product of 2×2 matrices, it's still a $2^S \times 2^S$ matrix, so calculating U completely isn't efficient).

   (b) Let U be an S-qubit unitary which applies a CNOT gate to the kth and ℓth qubits, and identity gates to the other $S-2$ qubits. Let $i, j \in \{0,1\}^S$. Show an efficient way to calculate the matrix-entry $U_{i,j} = \langle i|U|j\rangle$.

3. Consider a circuit C with $T = \text{poly}(n)$ elementary gates (only Hadamards and Toffolis) acting on $S = \text{poly}(n)$ qubits. Suppose this circuit computes $f : \{0,1\}^n \to \{0,1\}$ with bounded error probability: for every $x \in \{0,1\}^n$, when we start with basis state $|x, 0^{S-n}\rangle$, run the circuit and measure the first qubit, then the result equals $f(x)$ with probability at least 99/100.

   (a) Consider the following quantum algorithm: start with basis state $|x, 0^{S-n}\rangle$, run the above circuit C without the final measurement, apply a Z gate to the first qubit, and reverse the circuit C. Denote the resulting final state by $|\psi_x\rangle$. Show that if $f(x) = 0$ then the amplitude of basis state $|x, 0^{S-n}\rangle$ in $|\psi_x\rangle$ is in the interval $[1/2, 1]$, while if $f(x) = 1$ then the amplitude of $|x, 0^{S-n}\rangle$ in $|\psi_x\rangle$ is in $[-1, -1/2]$.

   (b) **PP** is the class of computational decision problems that can be solved by classical randomized polynomial-time computers with success probability $> 1/2$ (however, the success probability could be exponentially close to 1/2, i.e., **PP** is **BPP** without the 'B' for bounded-error). Show that **BQP** $\subseteq$ **PP**.

   Hint: use part (a). Analyze the amplitude of $|x, 0^{S-n}\rangle$ in the final state $|\psi_x\rangle$, using ideas from the proof of **BQP** $\subseteq$ **PSPACE** *that we saw in the lecture. You may assume* **BQP***-algorithms have error at most 1/100 instead of the usual 1/3. Note that you cannot use more than polynomial time.*