C&O 781 / QIC 890 Topics in Quantum Information
Recent advances in Quantum Information
University of Waterloo, Fall 2013
Instructor: Ashwin Nayak
Assignment 3, Nov. 17, 2013
Due: by noon, Nov. 29, 2013

Question 1. Show, from first principles, 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?

Question 2. We say a decision problem (language) L is in QRG(1) if there is a uniform sequence (C_n) of polynomial-size quantum circuits with the following properties. The circuit C_n operates on $n + 2\,p(n)$ input qubits, for some polynomial p, and is such that

- for every input $x \in L$ of length n, we have $\max_\rho \min_\sigma \Pr[C_n(x, \rho, \sigma) = 1] \geq 2/3$, and
- for every input $x \notin L$ of length n, we have $\max_\rho \min_\sigma \Pr[C_n(x, \rho, \sigma) = 1] \leq 1/3$,

where ρ and σ range over $p(n)$-qubit quantum states, and $C_n(x, \rho, \sigma)$ denotes the outcome of a measurement of the first qubit in the standard basis, after the circuit has been applied on input $|x\rangle\langle x| \otimes \rho \otimes \sigma$.

Show how we can use the MMWU algorithm to decide whether a given input x is in L.

Question 3. Using ideas from the QIP(3) protocol for Quantum Circuit Distinguishability, and the characterization of the maximum acceptance probability of a QIP(3) proof system we saw in class, prove that the completely bounded trace norm of the difference of two quantum operations Φ_1, Φ_2 can be expressed in terms of the maximum output fidelity $\max_{\rho,\sigma} \mathrm{F}(\Psi_1(\rho), \Psi_2(\sigma))$ (where ρ, σ are quantum states over appropriate spaces) of two related quantum operations Ψ_1, Ψ_2. Describe the operations Ψ_1, Ψ_2 explicitly in terms of Φ_1, Φ_2.

Question 4. Show that we cannot compute the XOR of *three* or more bits with one quantum query with probability greater than 1/2. Therefore, the Kerenidis-de Wolf lower bound method does not directly extend to q-query LDCs for $q \geq 3$.