Quantum Information and Quantum Computing, Problem set 8

Assistant : sara.alvesdossantos@epfl.ch, clemens.giuliani@epfl.ch, khurshed.fitter@epfl.ch

Problem 1 : The quantum counting algorithm

We wish to write an algorithm to estimate the number M of solutions of a search problem in a database of size $N = 2^n$, using quantum phase estimation (possibly not looking it up on the Nielsen and Chuang or on the Qiskit textbooks!). Suppose you are given the operator corresponding to Grover's search oracle $\hat{G}$ for the given search problem, and that you are also given the code to perform a controlled-$\hat{G}$ gate. For this problem we assume that $|\psi\rangle = \hat{H}^{\otimes n}|0\rangle$ is the constant superposition state of the vectors of the computational basis, and $|\alpha\rangle = (N-M)^{-1/2}\sum_x'' |x\rangle$ and $|\beta\rangle = M^{-1/2}\sum_x' |x\rangle$ are respectively the superpositions of all the non-solutions and of all the solutions in the computational basis.

1. Write the operator $\hat{G}$ as a matrix in the subspace spanned by $|\alpha\rangle$ and $|\beta\rangle$. What are its eigenvalues $e^{i\theta}$ and how are they related to the number of solutions M?
2. Write a QPE circuit that estimates M using t qubits in the estimate register. How do you prepare the initial state of the n-qubit register so that the QPE always gives a good estimate of M?
3. Suppose we wish to estimate θ to within 2^{-m} with probability $p = 1 - \epsilon$. Prove that, by setting ϵ small and $m \sim n$, the accuracy on the estimate of M is $O(\sqrt{M})$.

Problem 2 : Code Grover's search algorithm

Explicitly write the quantum circuit for carrying out Grover's search for $f(x) : \{0,1\}^3 \to \{0,1\}$ (always without looking it up!). Assume that $f(x) = 1$ for $x = 101$ and $x = 110$. Write the oracle circuit first, the rest of the $\hat{G}$ operator next. Then write the remaining part of the circuit and execute it on the QASM simulator. Determine first how many times the Grover iteration must be applied.