CDT in Quantum Engineering **Spring 2016**

ADVANCED QUANTUM INFORMATION THEORY

Exercise sheet 1

Ashley Montanaro, University of Bristol
ashley.montanaro@bristol.ac.uk

1. **Big-O notation and quantum circuits.**

   (a) In each of the following cases, write down whether $f(n) = O(g(n))$, $f(n) = \Omega(g(n))$, both, or neither.

   i. $f(n) = n$, $g(n) = n^2$.

   ii. $f(n) = 100n^3 + 50n^2 + 76$, $g(n) = 0.01n^3$.

   iii. $f(n) = e^{2n}$, $g(n) = e^n$.

   (b) Give examples of functions f, g such that neither $f(n) = O(g(n))$, nor $f(n) = \Omega(g(n))$.

   (c) For each of the following sets of quantum gates, determine whether or not the set is universal for quantum computation. You may assume that $\{H, X, \text{CNOT}, T\}$ is universal.

   i. $\{H, \text{CNOT}, T\}$.

   ii. $\{X, \text{CNOT}, T\}$.

   iii. (harder) $\{CZ, K, T\}$, where CZ is a controlled-Z gate and $K = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & i \\ i & 1 \end{smallmatrix}\right)$.

   (d) Imagine we are given a quantum circuit on n qubits which consists of poly(n) gates picked from the (universal) set $\{H, X, \text{CNOT}, T\}$, followed by a final measurement of all the qubits. Assume that at each step in the computation the quantum state is unentangled (i.e. is a product state of the n qubits). Show that the circuit can be simulated efficiently classically: that is, there is an efficient classical algorithm which determines the final quantum state produced by the circuit.

2. **Oracles and Grover's algorithm.**

   (a) Show that the phase oracle U_f as defined in the lecture notes cannot be used to implement the bit oracle O_f, even if f only has 1 bit of output.

   (b) Consider unstructured search for one marked element with $N = 4$. Write down and multiply out all the matrices and vectors occurring for one step of Grover's algorithm, to verify the claim in the lecture notes that the algorithm finds the marked element with certainty. What is the final state if another step is made?

   (c) Write down an expression for the (x, y)'th matrix entry of the matrix $-H^{\otimes n} U_0 H^{\otimes n}$ occurring in Grover's algorithm.

   (d) Let N be arbitrary and consider the case of Grover search for one marked element. What is the probability that the marked element is found if the qubits are measured after only one step of the algorithm?

   (e) (Harder.) Consider Grover search for k marked elements, where $k = \epsilon N$ is known in advance. Describe how to modify Grover's algorithm so that it finds a marked element with *certainty* using $O(1/\sqrt{\epsilon})$ queries. This can be seen as "quantum de-randomisation", a process with no classical analogue.