CDT in Quantum Engineering **Spring 2015**

ADVANCED QUANTUM INFORMATION THEORY

Exercise sheet 1

Ashley Montanaro, University of Bristol
`ashley@cs.bris.ac.uk`

1. **Smulation of various kinds.**

   (a) 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 for sampling from the probability distribution on the final measurement outcomes.

   (b) 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 $K = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & i \\ i & 1 \end{smallmatrix}\right)$.

   (c) 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 output.

2. **Grover's algorithm.**

   (a) Let $N = 4$ and consider the case where there is one marked element. 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?

   (b) 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.

   (c) 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?

   (d) 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.

3. **Quantum oracle interrogation.** In this question, you will prove the following result of Wim van Dam.

Theorem 1. *Given oracle access to bits of an unknown n-bit string x, there is a quantum algorithm that learns x completely with success probability at least* 0.999 *using* $n/2 + O(\sqrt{n})$ *queries, for any x.*

This success probability can in fact be taken to be any constant strictly less than 1. Of course, classically we need precisely n queries to learn x with this worst-case success probability.

(a) Show that, for any $x \in \{0,1\}^n$, given the n qubit state

$$|\psi_x\rangle := \frac{1}{2^{n/2}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle,$$

there is a quantum algorithm that determines x with certainty using no additional queries to the bits of x. (Here $x \cdot y = \sum_i x_i y_i$ is the inner product of x and y modulo 2.)

(b) For any $0 \leq r \leq n$, consider the state

$$|\psi_x^r\rangle := \frac{1}{\sqrt{R}} \sum_{y \in \{0,1\}^n, |y| \leq r} (-1)^{x \cdot y} |y\rangle,$$

where $R = \sum_{i=0}^{r} \binom{n}{i}$. Show that, for some $r = n/2 + O(\sqrt{n})$, $|\langle \psi_x | \psi_x^r \rangle|^2 \geq 0.999$ (hint: look up Chernoff bounds).

(c) Show that the state $|\psi_x^r\rangle$ can be produced using r queries to bits of x.

(d) Use parts (a)-(c) to prove Theorem 1.

4. **The QFT.**

(a) Write down the circuit for the QFT on 2 qubits. Multiply out the matrices in the circuit and check that the result is what you expect.

(b) This part is about approximately implementing the QFT, proving a claim made in the lecture notes. Define the distance $D(U,V)$ between unitary operators U and V as the maximum over all states $|\psi\rangle$ of $\| U|\psi\rangle - V|\psi\rangle \|$.

i. Show that $D(\cdot,\cdot)$ is subadditive: $D(U_1 U_2, V_1 V_2) \leq D(U_1, V_1) + D(U_2, V_2)$.

ii. Give a quantum circuit for an operator $\widetilde{Q}_{2^n}$ on n qubits such that $\widetilde{Q}_{2^n}$ uses $O(n \log n)$ gates and show that $D(\widetilde{Q}_{2^n}, Q_{2^n}) \leq 1/p(n)$ for any desired polynomial $p(n)$.

iii. Consider an arbitrary quantum circuit which has poly(n) gates in total, starts with the state $|0\rangle^{\otimes n}$ and finishes with a measurement in the computational basis, followed by some classical postprocessing. Argue that any uses of Q_{2^n} within the circuit can be replaced with $\widetilde{Q}_{2^n}$ without significantly affecting the output of the algorithm.

5. **Shor's algorithm.**

(a) Suppose we would like to factorise $N = 85$ and we choose $a = 3$. Show that a and N are coprime (without factorising N) using Euclid's algorithm. Follow the steps of the integer factorisation algorithm to factorise 85 using this value (calculating the order of a classically!). You might like to use a computer.

(b) Imagine we want to factorise $N = 21$ and we choose $a = 4$. Does the integer factorisation algorithm work or not?