ADVANCED QUANTUM INFORMATION THEORY

Exercise sheet 2

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

1. **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: $D(U_1U_2, V_1V_2) \leq D(U_1, V_1) + D(U_2, V_2)$.

      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 $\text{poly}(n)$ 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.

2. **Shor's algorithm.**

   (a) Suppose we would like to factorise $N = 85$ and we choose $a = 3$. Follow the steps of the integer factorisation algorithm to factorise 85 using this value of a (calculating the order of a classically!). You might like to use a computer.

   (b) Suppose we want to factorise $N = 35$ using Shor's algorithm, we have chosen $M = 2048$ and $a = 9$, and we receive a measurement result of 1365. Calculate the required continued fraction expansion and hence determine the claimed period of a output by the algorithm. Is the answer correct?

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