School of Mathematics **Spring 2019**

QUANTUM COMPUTATION

Exercise sheet 4

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

1. **Shor's algorithm.** In this question you will work through the final steps of the integer factorisation algorithm. You might like to use a calculator or computer for some of the parts. Suppose we would like to factorise $N = 33$.

   (a) What value do we choose for M?

   (b) Now suppose we randomly choose $a = 2$. What is the order r of a mod N?

   (c) Now suppose we get measurement outcome $y = 614$. Is this a "good" outcome of the form $\lfloor \ell M/r \rceil$ for some integer ℓ?

   (d) Write $z = y/M$ as a continued fraction.

   (e) Write down the convergents of this continued fraction and hence show that the algorithm correctly outputs the order of a mod N.

2. **A simple case of phase estimation.** Consider the phase estimation procedure with $n = 1$, applied to a unitary U and an eigenstate $|\psi\rangle$ such that $U|\psi\rangle = e^{i\theta}|\psi\rangle$.

   (a) Write down a full circuit for the quantum phase estimation algorithm in this case.

   (b) By tracking the input state through the circuit, write down the final state at the end of the algorithm. What is the probability that the outcome 1 is returned when the first register is measured?

   (c) Imagine we are promised that either $U|\psi\rangle = |\psi\rangle$, or $U|\psi\rangle = -|\psi\rangle$, but we have no other information about U and $|\psi\rangle$. Argue that the above circuit can be used to determine which of these is the case with certainty.

3. **Factoring via phase estimation (optional but interesting).** Fix two coprime positive integers x and N such that $x < N$, and let U_x be the unitary operator defined by $U_x|y\rangle = |xy \pmod N\rangle$. Let r be the order of x mod N (the minimal t such that $x^t \equiv 1$). For $0 \le s \le r-1$, define the states

$$|\psi_s\rangle := \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-2\pi i s k/r}\, |x^k \pmod N\rangle.$$

(a) Verify that U_x is indeed unitary.

(b) Show that each state $|\psi_s\rangle$ is an eigenvector of U_x with eigenvalue $e^{2\pi i s/r}$.

(c) Show that

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\psi_s\rangle = |1\rangle.$$

(d) Thus show that, if the phase estimation algorithm with n qubits is applied to U_x using $|1\rangle$ as an "eigenvector", the algorithm outputs an estimate of s/r accurate up to n bits, for $s \in \{0, \ldots, r-1\}$ picked uniformly at random, with probability lower bounded by a constant.

(e) Show that, for arbitrary integer $n \geq 0$, $U_x^{2^n}$ can be implemented in time polynomial in n and $\log N$ (not polynomial in 2^n!).

(f) Argue that this implies that the phase estimation algorithm can be used to factorise an integer N in $\text{poly}(\log N)$ time.