ADVANCED QUANTUM INFORMATION THEORY

Exercise sheet 3

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

1. **Factoring via phase estimation.** 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, for arbitrary integer $n \ge 0$, $U_x^{2^n}$ can be implemented in time polynomial in n and $\log N$ (not polynomial in 2^n!).

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

   (d) Show that
$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\psi_s\rangle = |1\rangle.$$

   (e) 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 $s \in \{0, \dots, r-1\}$ picked uniformly at random, with probability lower bounded by a constant.

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

2. **More efficient quantum simulation.**

   (a) Let A and B be Hermitian operators with $\|A\| \le K$, $\|B\| \le K$ for some $K \le 1$. Show that
$$e^{-iA/2} e^{-iB} e^{-iA/2} = e^{-i(A+B)} + O(K^3)$$
   (this is the so-called *Strang splitting*). Use this to give a more efficient approximation of k-local Hamiltonians by quantum circuits than the algorithm given in the notes, and calculate its complexity.

   (b) Let H be a Hamiltonian which can be written as $H = UDU^\dagger$, where U is a unitary matrix that can be implemented by a quantum circuit running in time poly(n), and $D = \sum_x d(x)|x\rangle\langle x|$ is a diagonal matrix such that the map $|x\rangle \mapsto e^{-id(x)t}|x\rangle$ can be implemented in time poly(n) for all x. Show that e^{-iHt} can be implemented in time poly(n).