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?

   Answer: M is the smallest power of 2 larger than $N^2 = 1089$, so $M = 2048$.

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

   Answer: By explicit multiplication, the order is 10.

   (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?

   Answer: Yes: $3 \times 2048/10 = 614.4$, and the outcome is the closest integer to this.

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

   Answer: To start, we have $z = 307/1024$. So

$$\begin{aligned} z &= \frac{1}{\frac{1024}{307}} = \frac{1}{3+\frac{103}{307}} = \frac{1}{3+\frac{1}{\frac{307}{103}}} = \frac{1}{3+\frac{1}{2+\frac{101}{103}}} = \frac{1}{3+\frac{1}{2+\frac{1}{\frac{103}{101}}}} = \frac{1}{3+\frac{1}{2+\frac{1}{1+\frac{2}{101}}}} \\ &= \frac{1}{3+\frac{1}{2+\frac{1}{1+\frac{1}{\frac{101}{2}}}}} = \frac{1}{3+\frac{1}{2+\frac{1}{1+\frac{1}{50+\frac{1}{2}}}}}. \end{aligned}$$

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

   Answer: The convergents are obtained by truncating this expansion, i.e.

$$\frac{1}{3}, \quad \frac{1}{3+\frac{1}{2}} = \frac{2}{7}, \quad \frac{1}{3+\frac{1}{2+\frac{1}{1}}} = \frac{3}{10}, \quad \frac{1}{3+\frac{1}{2+\frac{1}{1+\frac{1}{50}}}} = \frac{152}{507}.$$

   We want to find a convergent that is within $1/(2N^2) = 1/2178$ of $z = 307/1024$ and has denominator at most $N = 33$. Doing the calculations shows that $1/3$ and

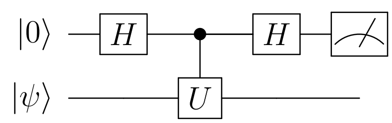
2/7 are not within 1/2178 of z, while 152/507 is ruled out because of its large denominator. So the only option is 3/10, which is indeed close enough. Therefore we output the denominator 10, which is indeed the order of a mod N.

Note that $a^{r/2} - 1 = 31$ and N are coprime, so the final step of the algorithm fails!

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.

   Answer:



   (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?

   Answer: We have

$$|0\rangle|\psi\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|\psi\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle+e^{i\theta}|1\rangle)|\psi\rangle \mapsto \frac{1}{2}((1+e^{i\theta})|0\rangle+(1-e^{i\theta})|1\rangle)|\psi\rangle$$

   so the probability that 1 is returned is $\frac{1}{4}|1 - e^{-i\theta}|^2 = \sin^2(\theta/2)$.

   (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.

   Answer: In the first case, we have $\theta = 0$, so the measurement returns 0 with certainty. In the second case, $\theta = \pi$, so the measurement returns 1 with certainty. Thus we can distinguish between the two cases as required.

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.

Answer: For U_x to be a permutation of basis states, we require $xy \equiv xz \pmod{N} \Leftrightarrow y = z$, i.e. taking $w = y - z$, we need that $xw \equiv 0 \Leftrightarrow w = 0$. But this holds because x is coprime to N.

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

Answer: By direct calculation,

$$\begin{aligned} U_x|\psi_s\rangle &= \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-2\pi isk/r}\, U_x|x^k\rangle = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-2\pi isk/r}\,|x^{k+1}\rangle \\ &= \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{-2\pi is(k-1)/r}\,|x^k\rangle = e^{2\pi is/r}|\psi_s\rangle. \end{aligned}$$

(c) Show that

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

Answer:

$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|\psi_s\rangle = \frac{1}{r}\sum_{k=0}^{r-1}\left(\sum_{s=0}^{r-1} e^{-2\pi isk/r}\right)|x^k\rangle = |1\rangle.$$

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

Answer: If $|\psi_s\rangle$ were input to the algorithm, we would get an estimate of s/r accurate up to n bits with probability lower-bounded by a constant. As we are using a uniform superposition over the states $|\psi_s\rangle$, we get each possible choice of s/r with equal probability.

(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!).

Answer: The operator $U_x^{2^n}$ simply performs the map $|y\rangle \mapsto |x^{2^n} y \pmod{N}\rangle$, i.e. multiplies y by x^{2^n}. To perform this multiplication, we can use repeated squaring:

$$x^{2^n} = (x^{2^{n-1}})^2 = ((x^{2^{n-2}})^2)^2 = \cdots = ((x^2)^2 \dots)^2,$$

where x is squared n times. Each squaring step takes time at most $\mathrm{poly}(n)$.

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

Answer: As we recall from Shor's algorithm, it suffices to compute the period r of a randomly chosen integer $1 < a < N$ to factorise N. Applying the phase estimation algorithm with $n = O(\log N)$ qubits to the operator U_a, we obtain an integer c such that $|c/2^n - s/r| < 1/2^{n+1}$, for randomly chosen s, in time poly($\log N$) time. Using the theory of continued fractions, we can go from this to determining s/r and hence r.