Exercise Set 10: Solution
Quantum Computation

Exercise 1 *Convergents in Shor's algorithm*

(a) Let us compute the convergents of $\frac{y}{M} = \frac{171}{2'048}$:

$$\frac{171}{2'048} = 0 + \frac{1}{2'048/171} \qquad \frac{2'048}{171} = 11 + \frac{167}{171} = 11 + \frac{1}{171/167}$$
$$\frac{171}{167} = 1 + \frac{4}{167} = 1 + \frac{1}{167/4} \qquad \frac{167}{4} = 41 + \frac{3}{4} = 41 + \frac{1}{4/3} \qquad \frac{4}{3} = 1 + \frac{1}{3}$$

So in the notation of the course, $\frac{171}{2'048} = [0, 11, 1, 41, 1, 3]$ and the values of the successive convergents of $\frac{171}{2'048} = 0.083496\ldots$ are

$$0 \qquad \frac{1}{11} = 0.\overline{09} \qquad \frac{1}{11 + \frac{1}{1}} = \frac{1}{12} = 0.08\overline{3} \qquad \frac{1}{11 + \frac{1}{1+\frac{1}{41}}} = \frac{42}{503} = 0.083499\ldots$$

We can stop here, as it can be checked directly that 12 is indeed the period of $f(x) = 3^x \bmod 35$. Note that the output $y = 171$ corresponds here to $k = 1$; one can check that

$$\left| \frac{y}{M} - \frac{k}{r} \right| \leq \frac{1}{2M}$$

(b) The computation of the convergents stops very quickly here, as $\frac{512}{2'048} = \frac{1}{4}$ (so in the notation of the course, $\frac{512}{2'048} = [4]$), but one can check that 4 is not a period of $f(x)$. We are actually in the unlucky situation where $k = 3$ and $\frac{k}{r}$ is not an irreducible fraction.

(c) Let us compute the convergents of $\frac{y}{M} = \frac{853}{2'048} = 0.4615\ldots$:

$$\frac{853}{2'048} = 0 + \frac{1}{2'048/853} \qquad \frac{2'048}{853} = 2 + \frac{1}{853/342} \qquad \frac{853}{342} = 2 + \frac{1}{342/169}$$
$$\frac{342}{169} = 2 + \frac{1}{169/4} \qquad \frac{169}{4} = 42 + \frac{1}{4}$$

so in the notation of the course, $\frac{853}{2'048} = [0, 2, 2, 2, 42, 4]$ and the corresponding convergents are

$$0 \qquad \frac{1}{2} = 0.5 \qquad \frac{1}{2 + \frac{1}{2}} = \frac{2}{5} = 0.4 \qquad \frac{1}{2 + \frac{1}{2+\frac{1}{2}}} = \frac{5}{12} = 0.41\overline{6} \qquad \ldots$$

and again, we can stop here, as 12 is the period of $f(x)$. Note that the output $y = 853$ corresponds to $k = 5$ and satisfies again

$$\left| \frac{y}{M} - \frac{k}{r} \right| \leq \frac{1}{2M}$$

Exercise 2 *Grover's algorithm for $N = 4$*

(a) The theory says that one query of the oracle in the quantum circuit suffices (as here, $M = 1 = N/4$). In other words, one "Grover operator" suffices.

(b) If P is any projector we have $(I - 2P)(I - 2P) = I - 4P + 4P^2 = I - 4P + 4P = I$. For the given U matrix this implies that $UU^\dagger = U^\dagger U = I$.

The entry $|00\rangle$ is mapped to

$$|00\rangle \to |11\rangle \to \frac{1}{\sqrt{2}}(|10\rangle - |11\rangle) \to \frac{1}{\sqrt{2}}(|11\rangle - |10\rangle)$$
$$\to \frac{1}{2}(|10\rangle - |11\rangle - |10\rangle - |11\rangle) = -|11\rangle \to -|00\rangle$$

The entry $|10\rangle$ is mapped to

$$|10\rangle \to |01\rangle \to \frac{1}{\sqrt{2}}(|00\rangle - |01\rangle) \to \frac{1}{\sqrt{2}}(|00\rangle - |01\rangle)$$
$$\to \frac{1}{2}(|00\rangle + |01\rangle - |00\rangle + |01\rangle) = |01\rangle \to |10\rangle$$

and we check also that $|01\rangle \to |01\rangle$ et $|11\rangle \to |11\rangle$.

(c) *Algorithmic steps:* We assume that $x_0 = 00$ without loss of generality.

1. Initial state $|001\rangle$
2. $H^{\otimes 3}|001\rangle = \frac{1}{(\sqrt{2})^3}\big(|00\rangle + |01\rangle + |10\rangle + |11\rangle\big) \otimes \big(|0\rangle - |1\rangle\big)$
3. After the oracle

$$\frac{1}{(\sqrt{2})^3}\big\{|00\rangle \otimes (|f(00)\rangle - |\overline{f(00)}\rangle) + |01\rangle \otimes \big(|f(01)\rangle - |\overline{f(01)}\rangle\big)$$
$$+ |10\rangle \otimes \big(|f(10)\rangle - |\overline{f(10)}\rangle\big) + |11\rangle \otimes \big(|f(11)\rangle - |\overline{f(11)}\rangle\big)\big\}$$

Because $f(00) = 1$ and $f(01) = f(10) = f(11) = 0$ we find

$$\frac{1}{(\sqrt{2})^3}\big\{|00\rangle \otimes (|1\rangle - |0\rangle) + |01\rangle \otimes \big(|0\rangle - |1\rangle\big)$$
$$+ |10\rangle \otimes \big(|0\rangle - |1\rangle\big) + |11\rangle \otimes \big(|0\rangle - |1\rangle\big)\big\}$$
$$= \frac{1}{(\sqrt{2})^3}\big\{-|00\rangle + |01\rangle + |10\rangle + |11\rangle\big\} \otimes (|0\rangle - |1\rangle)$$

Note that the solution $|00\rangle$ is marked here with a phase -1. This is sometimes called the "kickback phase" phenomenon (like in Deutsch-Josza's algorithm). Now we apply $H^{\otimes 2}$ to the first register and this gives:

$$\frac{1}{(\sqrt{2})^5}\big\{-|00\rangle - |01\rangle - |10\rangle - |11\rangle + |00\rangle - |01\rangle + |10\rangle - |11\rangle$$
$$+ |00\rangle + |01\rangle - |10\rangle - |11\rangle + |00\rangle - |01\rangle - |10\rangle + |11\rangle\big\} \otimes (|0\rangle - |1\rangle).$$

We apply the controlled sign change: only $|00\rangle$ changes sign:

$$\frac{1}{(\sqrt{2})^5}\big\{+|00\rangle - |01\rangle - |10\rangle - |11\rangle - |00\rangle - |01\rangle + |10\rangle - |11\rangle \\ - |00\rangle + |01\rangle - |10\rangle - |11\rangle - |00\rangle - |01\rangle - |10\rangle + |11\rangle\big\} \otimes (|0\rangle - |1\rangle).$$

Before proceeding, we simplify:

$$\begin{aligned}
&\frac{1}{(\sqrt{2})^5}\big\{-2|00\rangle - 2|01\rangle - 2|10\rangle - 2|11\rangle\big\} \otimes (|0\rangle - |1\rangle) \\
&\quad = -\frac{1}{(\sqrt{2})^3}\big\{+|00\rangle + |01\rangle + |10\rangle + |11\rangle\big\} \otimes (|0\rangle - |1\rangle) \\
&\quad = -\frac{1}{\sqrt{2}}(\underbrace{H^{\otimes 2}|00\rangle}_{\text{Ô surprise!}}) \otimes (|0\rangle - |1\rangle) = -H^{\otimes 3}(|001\rangle).
\end{aligned}$$

4. Now we apply the last series of Hadamard gates $H^{\otimes 3}$. Since $H^2 = 1$ we find the final state $-|00\rangle \otimes |1\rangle$. The measurement of the first register gives $x_0 = 00$ with probability 1.