Exercise Set 7: 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 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 $\frac{512}{2'048} = \frac{1}{4}$, 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 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 *Effect of imperfections in some gates in Shor's algorithm*

(a) After the Hadamard gates, the state is

$$\begin{aligned}\widetilde{H}_0 \otimes \widetilde{H}_1 \otimes \mathbb{I} \otimes \mathbb{I}(|0\rangle \otimes |0\rangle \otimes |0\rangle \otimes |0\rangle) \\ &= \left(\frac{1}{\sqrt{2}}\right)^2 (|0\rangle + e^{i\varphi_0}|1\rangle) \otimes (|0\rangle + e^{i\varphi_1}|1\rangle) \otimes |0\rangle \otimes |0\rangle \\ &= \frac{1}{\sqrt{4}}(|00\rangle + e^{i\varphi_0}|10\rangle + e^{i\varphi_1}|01\rangle + e^{i(\varphi_0+\varphi_1)}|11\rangle) \otimes |00\rangle \\ &= \frac{1}{\sqrt{4}}(|0\rangle + e^{i\varphi_1}|1\rangle + e^{i\varphi_0}|2\rangle + e^{i(\varphi_0+\varphi_1)}|3\rangle) \otimes |0\rangle\end{aligned}$$

(b) After the oracle U_f, we obtain the state

$$\frac{1}{\sqrt{4}}(|0\rangle \otimes |f(0)\rangle + e^{i\varphi_1}|1\rangle \otimes |f(1)\rangle + e^{i\varphi_0}|2\rangle \otimes |f(2)\rangle + e^{i(\varphi_0+\varphi_1)}|3\rangle \otimes |f(3)\rangle)$$

Since $f(x) = f(x+2)$, we have:

$$\frac{1}{\sqrt{4}}(|0\rangle + e^{i\varphi_0}|2\rangle) \otimes |f(0)\rangle + \frac{1}{\sqrt{4}}(e^{i\varphi_1}|1\rangle + e^{i(\varphi_0+\varphi_1)}|3\rangle) \otimes |f(1)\rangle$$

Applying the QFT to each term:

$$\frac{1}{4}\sum_{y=0}^{3}(1 + e^{i(\varphi_0+\frac{\pi}{2}2y)})|y\rangle \otimes |f(0)\rangle + \frac{1}{4}\sum_{y=0}^{3}(e^{i(\varphi_1+\frac{\pi}{2}y)} + e^{i(\varphi_0+\varphi_1+\frac{\pi}{2}3y)})|y\rangle \otimes |f(1)\rangle$$

(c) The state right after the measurement is

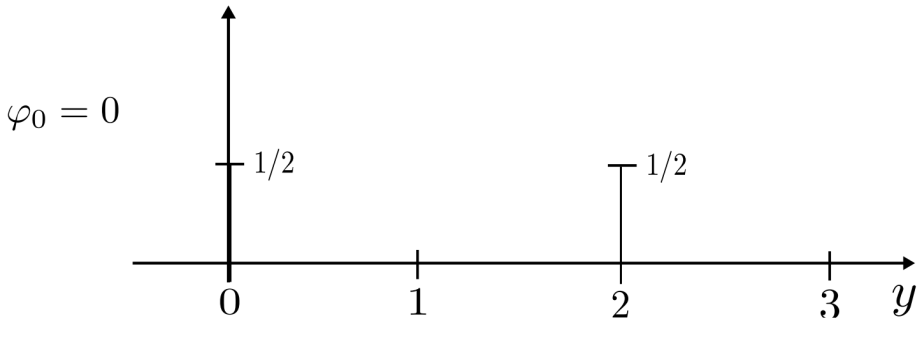
$$|\psi_4\rangle = \frac{1}{4}(1 + e^{i(\varphi_0+\pi y)})|y\rangle \otimes |f(0)\rangle + \frac{1}{4}e^{i(\varphi_1+\frac{\pi}{2}y)}(1 + e^{i(\varphi_0+\pi y)})|y\rangle \otimes |f(1)\rangle.$$

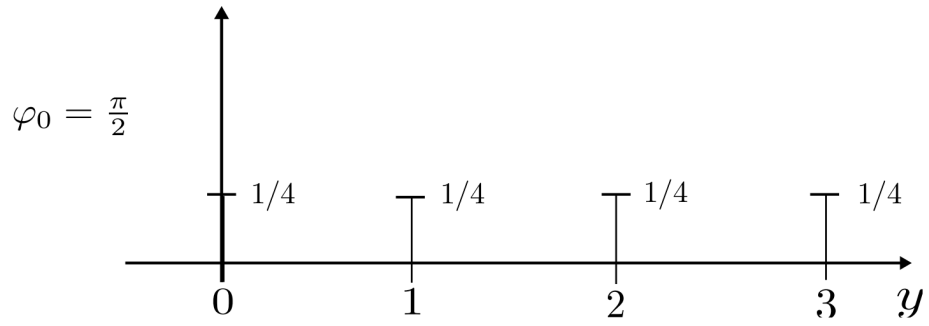
The probability of obtaining y is then given by

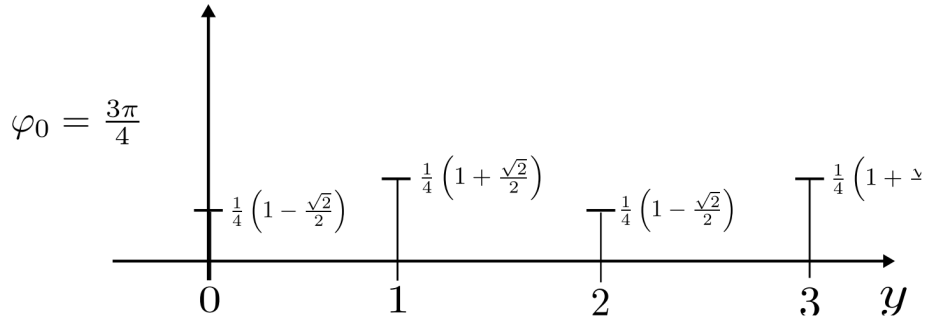
$$\begin{aligned}\text{Prob}(y|\varphi_0,\varphi_1) &= \frac{1}{16}\left\{|1 + e^{i(\varphi_0+\pi y)}|^2 + |1 + e^{i(\varphi_0+\pi y)}|^2\right\} \\ &= \frac{1}{8}\left((1 + \cos(\varphi_0 + \pi y))^2 + \sin^2(\varphi_0 + \pi y)\right) \\ \Rightarrow \quad \text{Prob}(y|\varphi_0,\varphi_1) &= \frac{1}{4}\left(1 + \cos(\varphi_0 + \pi y)\right)\end{aligned}$$

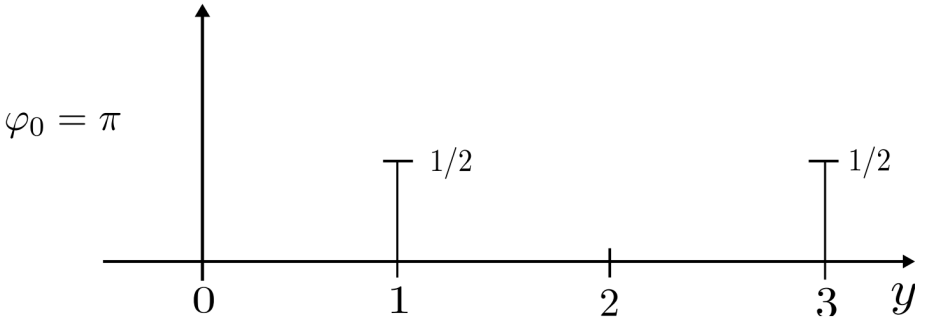
We see that, curiously, this probability does not depend on φ_1. Therefore, Shor's algorithm appears robust to this phase shift.

(d)

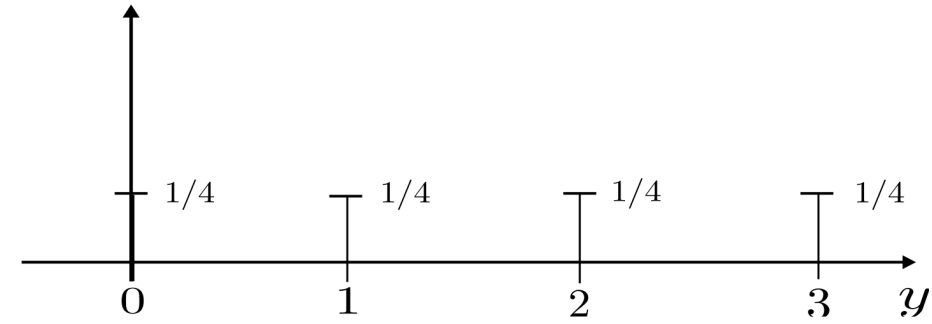








$$\mathrm{Prob}(y) = \int \mathrm{d}\varphi_0 \,\mathrm{Prob}(y|\varphi_0)\,\mathrm{Prob}(\varphi_0) = \int_0^{2\pi} \frac{\mathrm{d}\varphi_0}{2\pi}\,\mathrm{Prob}(y|\varphi_0) = \frac{1}{4}$$



In an NMR experiment, these spectra are obtained. In the cases when $\varphi_0 = 0, \frac{\pi}{4}, \frac{3\pi}{4}$ or π, we can read the period.

Exercise 3 *Simon's algorithm*

(a) Define the given vector as $s_1 = (1, 1, 0, 0)$ and define $s_2 = (0, 1, 1, 1)$. The function f is invariant under the transformations defined by them, as well as by their sum, $s_3 = (1, 0, 1, 1)$. You can verify that these are all the non-trivial vectors with this property. We conclude that the set of required vectors is

$$H = span\{s_1, s_2\} \; . \tag{1}$$

(b) The state of Simon's Algorithm, just before the measurement is:

$$|\psi\rangle = \frac{1}{2^4} \sum_{x,y \in \{0,1\}^4} (-1)^{x \cdot y} \, |y\rangle \otimes |f(x)\rangle \tag{2}$$

For every string in the image of f fix a preimage x. The term that is held in the first register (preceeding $|f(x)\rangle$) is

$$\sum_y (-1)^{x \cdot y} \left(\sum_{s \in H} (-1)^{s \cdot y} \right) |y\rangle \; . \tag{3}$$

Denote the space of all vectors orthogonal to H by $H^\perp$. With the same reasoning as seen in class, if $y \in H^\perp$ then

$$\sum_{s \in H} (-1)^{y \cdot s} = 4 \; . \tag{4}$$

Otherwise, the sum vanishes. We conclude that in the output distribution, all of the strings that are orthogonal to H are distributed uniformly, with probability $1/4$.

(c) By repeating the algorithm, we can recover the list of all vectors in $H^\perp$. The ones that are perpendicular to $H^\perp$ are the requested output.

Exercise 4 *The action of basic circuits*

(a)

$$|\psi_1\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \, |0\rangle \, |0\rangle = |+\rangle \, |0\rangle \, |0\rangle \; , \tag{5}$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}} (|000\rangle + |101\rangle) \; , \tag{6}$$

$$|\psi_3\rangle = \frac{1}{\sqrt{2}} (|000\rangle + |111\rangle) \; . \tag{7}$$

(b)

$$|\psi_3\rangle = \frac{1}{2} \left(|+++\rangle + |+--\rangle + |-+-\rangle + |--+\rangle \right) \; . \tag{8}$$

(c) Measuring in the standard basis, $(0, 0, 0)$ and $(1, 1, 1)$ are given with probability $1/2$ for each. The rest of the outcomes are given with probability 0.

Exercise 5 *The Fourier Transform of a periodic vector (Optional)*

(a) Let us denote $\left|\tilde{\psi}\right\rangle = QFT\,|\psi\rangle$, such that

$$\left|\tilde{\psi}\right\rangle = (\tilde{\psi}_1, ..., \tilde{\psi}_{N-1})\ . \tag{9}$$

The coefficients are given by:

$$\tilde{\psi}_k = \frac{1}{\sqrt{N}}\sum_{z=0}^{N-1}\psi_z e^{\frac{2\pi i}{N}zk} = \frac{1}{\sqrt{N}}\sum_{s=0}^{m-1}e^{\frac{2\pi i}{N}srk} = \frac{1}{\sqrt{N}}\sum_{s=0}^{m-1}(e^{\frac{2\pi i}{N}rk})^s\ . \tag{10}$$

In the second step, we used the fact that $x_k = 1$ only for $k = sr$ with some $s \in \{0, ..., m-1\}$. Use now the following identitry for the geometric series:

$$\tilde{\psi}_k = \frac{1}{\sqrt{N}}\begin{cases} m & e^{\frac{2\pi i}{N}rk} = 1 \\ \frac{1-e^{\frac{2\pi i}{N}rkm}}{1-e^{\frac{2\pi i}{N}rk}} & otherwise \end{cases} \tag{11}$$

Now note that $e^{\frac{2\pi i}{N}rk} = 1$ only when k is a whole multiple of m, Namely when $k = j \cdot m$. Now since $N = m \cdot r$,

$$1 - e^{\frac{2\pi i}{N}kmr} = 1 - e^{2\pi ik} = 0\ . \tag{12}$$

Ultimately,

$$\tilde{\psi}_k = \begin{cases} \frac{m}{\sqrt{N}} & k = j \cdot m \\ 0 & otherwise \end{cases} \tag{13}$$

In other words, the Fourier Transform of the given periodic vector (sometimes named a "comb" or a "Lattice") with a period $r = N/m$ is another vector of the same type, with a period of $m = N/r$.

(b) In a similar manner, we use the fact that $\tilde{\psi}_k^{(a)}$ is 1 only when $k = sr + a$. The calculation now gives:

$$\tilde{\psi}_k^{(a)} = \frac{1}{\sqrt{N}}\sum_{s=0}^{m-1}e^{\frac{2\pi i}{N}(sr+a)k} = e^{\frac{2\pi i}{N}ak}\cdot\frac{1}{\sqrt{N}}\sum_{s=0}^{m-1}(e^{\frac{2\pi i}{N}rk})^s\ . \tag{14}$$

We get a similar expression, with the addition of a complex phase:

$$\tilde{\psi}_k = e^{\frac{2\pi i}{N}ak}\begin{cases} \frac{m}{\sqrt{N}} & k = j \cdot m \\ 0 & otherwise \end{cases} \tag{15}$$

(c) Any periodic vector $|\psi\rangle$ with a period r is fully determined by its first r entries. We can therefore write it as a linear combination of "combs" (vectors of the type given in section (b)).

$$|\psi\rangle = \sum_{s=0}^{r-1}\psi_s\left|\psi^{(s)}\right\rangle \tag{16}$$

here, ψ_s are complex numbers and $\left|\psi^{(s)}\right\rangle$ are combs with the same notation as in the last section. The Fourier Transform of any $\left|\psi^{(s)}\right\rangle$ has vanishing coefficients except for multiples of $m = N/r$, namely $\tilde{\psi}_k^{(s)} \neq 0 \iff k = j \cdot m$. The Fourier Transform is linear, so we conclude that the Fourier Transform of $|\psi\rangle$ vanishes except for whole multiples of m:

$$k \neq j \cdot m \Rightarrow \tilde{\psi}_k = 0 \; . \tag{17}$$