Exercise Set 9: Solution
Quantum Computation

Exercise 1 *Another algorithm involving the QFT*

(a) The matrix elements of V_f are

$$\langle y| V_f |x\rangle = e^{-\frac{2\pi i}{M} f(x)} \langle y|x\rangle = \begin{cases} e^{-\frac{2\pi i}{M} f(x)} & \text{if } x = y \\ 0 & \text{fi } x \neq y \end{cases}$$

i.e., the matrix is diagonal and one checks trivially that $V_f V_f^\dagger = V^\dagger V_f = I$. For the QFT matrix, we have

$$\langle y| QFT |x\rangle = \frac{1}{\sqrt{M}} \sum_{y'=0}^{M-1} e^{\frac{2\pi i}{M} xy'} \langle y|y'\rangle = \frac{1}{\sqrt{M}} e^{\frac{2\pi i}{M} xy} \quad \text{since } \langle y|y'\rangle = \delta_{y,y'}$$

The inner product between two lines is given by

$$\frac{1}{M} \sum_{y=0}^{M-1} e^{\frac{2\pi i}{M}(x-x')y} = \begin{cases} 1 & \text{if } x = x' \\ 0 & \text{otherwise} \end{cases}$$

so $(QFT)(QFT)^\dagger = (QFT)^\dagger(QFT) = I$.

(b) A state $|x\rangle$ is represented by

$$|x\rangle = |x_0\rangle \otimes |x_1\rangle \otimes \cdots \otimes |x_{m-1}\rangle$$

where $x = x_0 + 2x_1 + \cdots + 2^{m-1}x_{m-1}, x_i \in \{0, 1\}$ is represented in base 2. The Hilbert space is $(\mathbb{C}^2)^{\otimes m}$. The initial state is $|x = 0\rangle = |0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle$.

(c) After the Hadamard gates, the state is

$$\frac{1}{2^{m/2}} \sum_{b_1 \ldots b_M} |b_1\rangle \otimes |b_2\rangle \otimes \cdots \otimes |b_M\rangle = \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle$$

After the V_f gate, the state is

$$\frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} e^{-\frac{2\pi i}{M} f(x)} |x\rangle$$

After the QFT gate, the state is

$$|\Psi\rangle = \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} e^{-\frac{2\pi i}{M} f(x)} \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} e^{\frac{2\pi i}{M} xy} |y\rangle = \frac{1}{\sqrt{M}} \sum_{y=0}^{M-1} \left\{ \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} e^{-\frac{2\pi i}{M} f(x)} e^{\frac{2\pi i}{M} xy} \right\} |y\rangle$$

(d) For $f(x) = Ax + B$, the coefficients of $|\Psi\rangle$ in the computational basis are

$$\frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} e^{-\frac{2\pi i}{M}Ax} e^{-\frac{2\pi i}{M}B} e^{\frac{2\pi i}{M}xy} = e^{-\frac{2\pi i}{M}B} \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} e^{\frac{2\pi i}{M}(y-A)x}.$$

The probability to observe a given state $|y\rangle$ after the measurement is

$$\mathbb{P}(y) = \frac{1}{M}\Big| \sum_{x=0}^{M-1} e^{\frac{2\pi i}{M}(y-A)x} \Big|^2$$

For $y = A$: $\mathbb{P}(y = A) = 1$ et so $\mathbb{P}(y \neq A) = 0$. Therefore, a single measurement suffices to retrieve the value of A. On the other hand, B only appears as a global phase and cannot therefore be determined.

Exercise 2 *Gate U_f for $f(x) = a^x$ mod N*

(a) Observe that $3^1 \bmod 8 = 3$, $3^2 \bmod 8 = 1$, so $3^x \bmod 8 = 1$ or 3 depending whether x is even of odd. This gives rise to the circuit on the figure below on the left (where (x_2, x_1, x_0) is the binary representation of $0 \leq x \leq 7$). You can check that indeed, $(y_2, y_1, y_0) = f(x_2, x_1, x_0) = (0, x_0, 1)$; when x is even (i.e., $x_0 = 0$), then $y = 1 = (0, 0, 1)$ in binary; and when x is odd (i.e., $x_0 = 1$), then $y = 3 = (0, 1, 1)$ in binary,

(b) Observe that $3^1 \bmod 16 = 3$, $3^2 \bmod 16 = 9$, $3^3 \bmod 16 = 11$, $3^4 \bmod 16 = 1$, so similarly, we build the circuit on the figure below on the right, and you can check again that $(y_3, y_2, y_1, y_0) = f(x_3, x_2, x_1, x_0)$.