Exercise Set 8: 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

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

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

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

For $y = A$, $\mathbb{P}(y) = 1$ and for $y \neq A$, $\mathbb{P}(y) = 0$. 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 *Gates to build U_f for $f(x) = a^x \pmod N$*

(a) For $a = 2$ and $N = 3$: $U_2|0\rangle = |0\rangle, U_2|1\rangle = |2\rangle, U_2|2\rangle = |1\rangle, U_2|3\rangle = |3\rangle$. Writing the full states in binary, we obtain $U_2|00\rangle = |00\rangle, U_2|01\rangle = |10\rangle, U_2|10\rangle = |01\rangle$. Thus the matrix is

$$U_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

For $a = 3$ and $N = 4$: $U_3|0\rangle = |0\rangle, U_3|1\rangle = |3\rangle, U_3|2\rangle = |2\rangle, U_3|3\rangle = |1\rangle$. Writing the full states in binary, we obtain $U_3|00\rangle = |00\rangle, U_3|01\rangle = |11\rangle, U_3|10\rangle = |10\rangle, U_3|11\rangle = |01\rangle$. Thus the matrix is

$$U_3 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

We can recognize in both cases permutation matrices. From those matrices, you can perhaps already guess what will be the final ciruit.

(b) For $a = 2$ and $N = 3$: the Boolean functions are

$$\begin{aligned} f_{00}(x,y) &= (1\oplus x)(1\oplus y) \\ f_{01}(x,y) &= x(1\oplus y) \\ f_{10}(x,y) &= (1\oplus x)y \\ f_{11}(x,y) &= xy. \end{aligned}$$

For $a = 3$ and $N = 4$: the Boolean functions are

$$\begin{aligned} f_{00}(x,y) &= (1\oplus x)(1\oplus y) \\ f_{01}(x,y) &= xy \\ f_{10}(x,y) &= x(1\oplus y) \\ f_{11}(x,y) &= (1\oplus x)y. \end{aligned}$$

(c) The function $f_{X=1}(x,y) = f_{10}(x,y) \oplus f_{11}(x,y)$ since both cases are exclusives. In the same way, we have $f_{Y=1}(x,y) = f_{01}(x,y) \oplus f_{11}(x,y)$. Thus for $a=2$ and $N=3$, we have

$$f_{X=1}(x,y) = (1\oplus x)y \oplus xy = y$$
$$f_{Y=1}(x,y) = x(1\oplus y) \oplus xy = x.$$

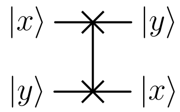
and for $a=3$ and $N=4$, we have

$$f_{X=1}(x,y) = x(1\oplus y) \oplus (1\oplus x)y = x\oplus y$$
$$f_{Y=1}(x,y) = xy \oplus (1\oplus x)y = y.$$

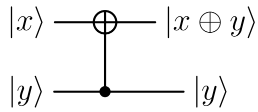
(d) Since $U_a\left|x,y\right\rangle = \left|f_{X=1}(x,y)\right\rangle\left|f_{Y=1}(x,y)\right\rangle$, we have, for $a=2$ and $N=3$, $U_a\left|x,y\right\rangle = \left|y\right\rangle\left|x\right\rangle$ and for $a=3$ and $N=4$, $U_a\left|x,y\right\rangle = \left|x\oplus y\right\rangle\left|y\right\rangle$.

The first circuit is a SWAP gate between the two qubits. In the second case, the circuit is a CNOT gate where the control qubit is the second one. Thus, the circuits are :

$a=2$ and $N=3$



$a=3$ and $N=4$



Exercise 3 *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

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