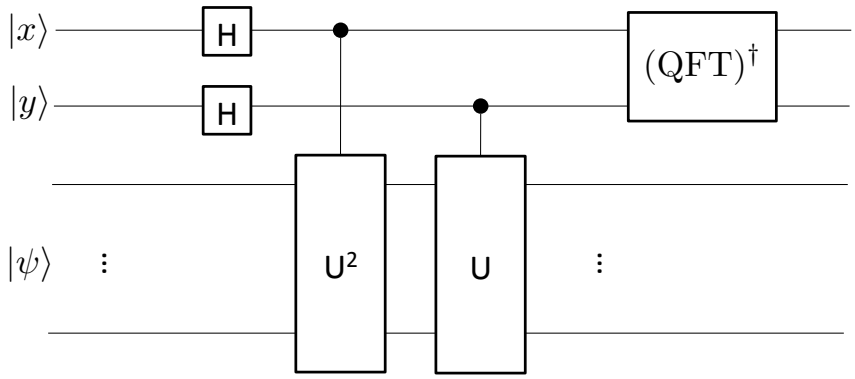
Exercise Set 6: Solution
Quantum Computation

Exercise 1 *Phase estimation based on the Quantum Fourier Transform*

(a) $\dim(S) = \dim(|x\rangle) \times \dim(|y\rangle) \times \dim(|\psi\rangle) = \dim(\mathbb{C}^2) \times \dim(\mathbb{C}^2) \times \dim\big((\mathbb{C}^2)^{\otimes n}\big) = 2^{2+n}$.
The circuit corresponding to S:



(b) The state after the H's: $H|0\rangle \otimes H|0\rangle \otimes |u\rangle = \frac{1}{2}\big(|00u\rangle + |01u\rangle + |10u\rangle + |11u\rangle\big)$
The state after U^{2x} (or R_1): $\frac{1}{2}\big(|00u\rangle + |01u\rangle + e^{4\pi i\varphi}|10u\rangle + e^{4\pi i\varphi}|11u\rangle\big)$
The state after U^{y} (or R_2): $\frac{1}{2}\big(|00u\rangle + e^{2\pi i\varphi}|01u\rangle + e^{4\pi i\varphi}|10u\rangle + e^{6\pi i\varphi}|11u\rangle\big)$

(c) We can write the last expression as

$$\frac{1}{2}\sum_{y_1,y_0\in\{0,1\}} e^{2\pi i\varphi(2y_1+y_0)}|y_1,y_0\rangle \otimes |u\rangle = \frac{1}{2}\sum_{y_1,y_0\in\{0,1\}} e^{\frac{2\pi i}{4}(2\varphi_1+\varphi_0)(2y_1+y_0)}|y_1,y_0\rangle \otimes |u\rangle$$
$$= \mathrm{QFT}\,|\varphi_1,\varphi_0\rangle \otimes |u\rangle$$

QFT is unitary and therefore $(QFT)^\dagger(QFT) = I_n$. Then, the output state of the circuit is $|\varphi_1\rangle \otimes |\varphi_0\rangle \otimes |u\rangle$.

(d) It suffices to measure the two first qubits because they are $|\varphi_1\rangle \otimes |\varphi_0\rangle$.

Exercise 2 *Gates to build U_f for $f(x) = a^x \,(mod\ N)$*

(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

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

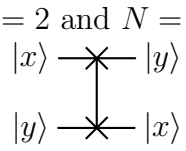
and for $a = 3$ and $N = 4$, we have

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

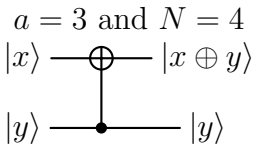
(d) Since $U_a |x, y\rangle = |f_{X=1}(x, y)\rangle |f_{Y=1}(x, y)\rangle$, we have, for $a = 2$ and $N = 3$, $U_a |x, y\rangle = |y\rangle |x\rangle$ and for $a = 3$ and $N = 4$, $U_a |x, y\rangle = |x \oplus y\rangle |y\rangle$.

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 *Approximating QFT*

1. For all $|\psi\rangle$:

$$\begin{aligned}\|(U_1U_2 - V_1V_2)|\psi\rangle\| &= \|(U_1U_2 - V_1U_2 + V_1U_2 - V_1V_2)|\psi\rangle\| \\ &\leq \|(U_1U_2 - V_1U_2)|\psi\rangle\| + \|(V_1U_2 - V_1V_2)|\psi\rangle\| \\ &= \|(U_1 - V_1)U_2|\psi\rangle\| + \|V_1(U_2 - V_2)|\psi\rangle\|.\end{aligned}$$

   Using that V_1 is unitary and does not change the norm, and that U_2 maps normalized states to normalized states, we obtain:

$$D(U_1U_2, V_1V_2) \leq D(U_1, V_1) + D(U_2, V_2).$$

2. We compute:

$$\begin{aligned}D(R_d, I) &= \max_{|\alpha|^2+|\beta|^2=1} \|(R_d - I)(\alpha|0\rangle + \beta|1\rangle)\| \\ &= \max_{|\alpha|^2+|\beta|^2=1} \|\beta(e^{\pi i/2^d} - 1)|1\rangle\| \\ &= |e^{\pi i/2^d} - 1|.\end{aligned}$$

   Using Euler's identity:

$$|e^{i\theta} - 1| = 2\left|\sin\left(\frac{\theta}{2}\right)\right|,$$

   we get:

$$D(R_d, I) = 2\left|\sin\left(\frac{\pi}{2^{d+1}}\right)\right| \approx \frac{\pi}{2^d} = O(2^{-d}).$$

   For the controlled version:

$$D(I_2 \oplus R_d, I_4) = D(R_d, I_2),$$

   since the operator acts non-trivially only on a 2-dimensional subspace, hence:

$$D(I_2 \oplus R_d, I_4) = O(2^{-d}).$$

3. Let the original circuit be written as:

$$U_1U_2U_3 \cdots U_{2M}U_{2M+1},$$

   where the U_{2m} are the gates to be removed.

After removing them:

$$U_1 I U_3 \cdots I U_{2M+1}.$$

Using subadditivity:

$$D(U_1 I U_3 \cdots I U_{2M+1}, U_1 U_2 U_3 \cdots U_{2M} U_{2M+1}) \leq \sum_{m=1}^{M} D(U_{2m}, I).$$

Now, removing all controlled-R_d with $d \geq k$, and noting that for each d there are at most n such gates:

$$\begin{aligned} D(\tilde{Q}_N, Q_N) &\leq \sum_{d=k}^{n-1} n \cdot D(I_2 \oplus R_d, I_4) \\ &= n \sum_{d=k}^{n-1} O(2^{-d}) \\ &= O(n 2^{-k}). \end{aligned}$$

To achieve:

$$D(\tilde{Q}_N, Q_N) = O\left(\frac{1}{n}\right),$$

we choose:

$$k = 2 \log n.$$

Finally, counting gates:

- n Hadamard gates,
- at most n controlled-R_d gates for each $d < k$.

Hence total complexity:

$$O(nk) = O(n \log n).$$