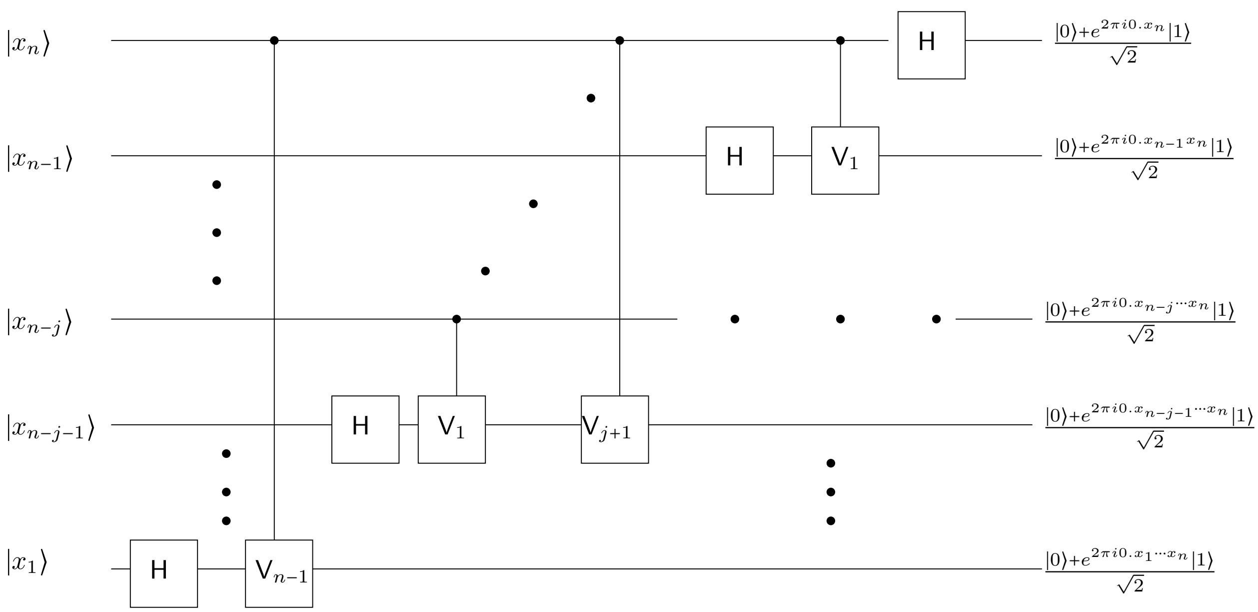
Assignment 5
DUE: Thursday, 4/27/2023, work in pairs.

1. The first problem is about proving the correctness of our construction of a quantum circuit for computing the Quantum Fourier Transform (QFT). From the original QFT, we derived the following form (same thing, written in two ways):

$$\begin{aligned} \mathsf{U}_{FT} &= \frac{1}{2^{n/2}}\Big(|0\rangle + e^{2\pi i 0.x_n}|1\rangle\Big)\otimes\Big(|0\rangle + e^{2\pi i 0.x_{n-1}x_n}|1\rangle\Big)\otimes\cdots\otimes\Big(|0\rangle + e^{2\pi i 0.x_1\cdots x_n}|1\rangle\Big)\\ &= \frac{1}{2^{n/2}}\bigotimes_{j=0}^{n-1}\Big(|0\rangle + e^{2\pi i 0.x_{n-j}x_{n-j+1}x_{n-j+2}\cdots x_n}|1\rangle\Big)\end{aligned}$$

   where, with $x = x_1 2^{n-1} + x_2 2^{n-2} + \cdots + x_{n-1}2 + x_n$, we defined $0.x_{n-j}x_{n-j+1}x_{n-j+2}\cdots x_n = x_{n-j}2^{-1} + x_{n-j+1}2^{-2} + x_{n-j+2}2^{-3} + \cdots + x_n 2^{-j}$. From this we derived the circuit depicted below. Prove, by induction on j, that the output of the j^{th} wire in the circuit is the j^{th} factor in the above tensor product, namely, $|0\rangle + e^{2\pi i 0.x_{n-j}x_{n-j+1}x_{n-j+2}\cdots x_n}|1\rangle$. The base case $j = 0$ was done in class, as was $j = 1$ (although in class the indexing differed by 1, i.e., we had $j = 1$ and 2). Follow through with an inductive proof that if the factor is correct for j it is also correct for $j + 1$.



   HINT: Pay careful attention to what happens as you go from line j (with input state $|x_{n-j}\rangle$) to $j+1$ (with input state $|x_{n-j-1}\rangle$).

---

2. Here we'll turn the crank in the final stage of Shor's algorithm (which is classical, but still very interesting), where we determine r based on continued fractions. The process was discussed in class and is detailed in Appendix K. Following the second example in the text, we give possible values for y. The idea is to find r.

   Take $n = 14$ and suppose we first find $y = 8374$. Using the continued fraction expansion of $y/2^n$, find the first partial sum with denominator $< 2^7 = 128$. This gives you one candidate r. Give the computation and state the value of the candidate r. Now suppose we repeated the entire quantum algorithm (QFT and all) and obtained $y = 8556$. Via the same procedure, you should find another candidate r, which is a multiple of the first one. Which one is the correct r?

---

3. Finally, let's carefully derive a relation which leads to the stated run time of Grover's algorithm. We use the definitions and notations given in the text and in lecture:

$$\begin{aligned}
|\phi\rangle &= \frac{1}{2^n}\sum_{x=0}^{2^n-1}|x\rangle \\
|a_\perp\rangle &= \frac{1}{\sqrt{2^n-1}}\sum_{x=0,x\neq a}^{2^n-1}|x\rangle \\
W &= 2|\phi\rangle\langle\phi| - 1 \\
V &= 1 - 2|a\rangle\langle a| \\
\sin(\theta) &= \frac{1}{2^{n/2}}, \qquad \text{in terms of which we find,} \\
|\phi\rangle &= \sin(\theta)|a\rangle + \cos(\theta)|a_\perp\rangle
\end{aligned}$$

(a) Using some elementary trigonometric identities, prove that

$$\begin{aligned}
WV|a\rangle &= \cos(2\theta)|a\rangle - \sin(2\theta)|a_\perp\rangle \\
WV|a_\perp\rangle &= \sin(2\theta)|a\rangle + \cos(2\theta)|a_\perp\rangle.
\end{aligned}$$

(b) Using part (a), prove the following by induction on k:

$$(WV)^k|\phi\rangle = \sin((2k+1)\theta)|a\rangle + \cos((2k+1)\theta)|a_\perp\rangle. \tag{1}$$

You will almost certainly find the following identities[1] useful:

$$\begin{aligned}
\sin((2k+1)\theta)\cos(2\theta) + \cos((2k+1)\theta)\sin(2\theta) &= \sin((2k+3)\theta) \\
-\sin((2k+1)\theta)\sin(2\theta) + \cos((2k+1)\theta)\cos(2\theta) &= \cos((2k+3)\theta).
\end{aligned}$$

(c) Now remember what we're after in Grover's algorithm: $|a\rangle$! The parameter k is the number of times we apply the Grover iterate WV to $|\phi\rangle$ in order to get as close as possible to $|a\rangle$. Show how Eq. (1) leads to a desired value of k of about $\frac{\pi}{4}2^{n/2} = \frac{\pi}{4}\sqrt{N}$ (where N here is defined as 2^n).

[1] No need to prove these identities, but if you have some free time on your hands, you may find it fun to exploit our old friend $e^{i\theta} = \cos\theta + i\sin\theta$ to derive them.