CS166 WI24: Homework 6 (Due Friday March 11 11:59pm)

❖ Problem 1: Fourier Transform of Factors

Recall the periodic states defined for fixed N and some r that divides N:

$$|\phi_r\rangle := \sqrt{\frac{r}{N}} \sum_{k=0}^{\frac{N}{r}-1} |kr\rangle. \tag{1}$$

In this problem we will prove that

$$QFT_N |\phi_r\rangle = |\phi_{N/r}\rangle. \tag{2}$$

 Instead of proving it generally, we will look at the case where $N = 21$ and $r = 3$ that we studied in class.

1. Write the state $|\phi_3\rangle$.

2. Apply QFT_{21} to $|\phi_3\rangle$. We know the solution will be $|\phi_7\rangle$, but for this problem, write the state as a sum of states with Fourier amplitudes. Your solution should be in the form

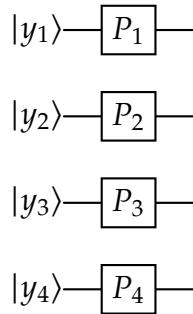 $$\frac{1}{?} \sum_y \sum_k \omega^? |y\rangle. \tag{3}$$

3. There are two cases to analyze. For certain values of y, the amplitude of $|y\rangle$ will be 1. What values of y is this for?

4. The other case is when the previous statement is NOT true. What happens in this case? Pick the smallest value of y that was not chosen in the previous part, and draw all the values that appear with this y in the complex plane. What can you say about the amplitude of $|y\rangle$ in this case?
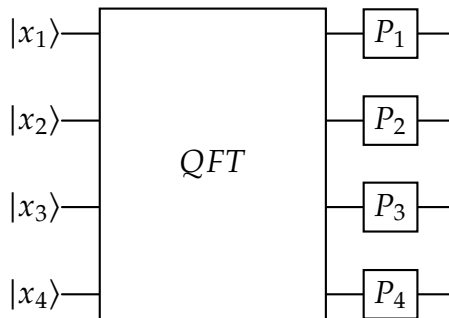
✽ Problem 2: QFT Counter

Suppose $x \in \{0, \ldots, 15\}$ is a four bit string. Let $x_1 x_2 x_3 x_4$ be the binary representation of the integer x.

1. Express the state resulting from applying QFT_N to the state $|x\rangle$.

2. Now suppose that $y \in \{0, \ldots, N-1\}$. Let $y_1 \ldots y_n$ be the binary representation of the integer y. Express the output of the circuit below as a function of y and the N-th root of unity ω. Here, we are using the gate

$$P_a = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^a} \end{bmatrix}. \tag{4}$$

$$|y_1\rangle - \boxed{P_1} -$$

$$|y_2\rangle - \boxed{P_2} -$$

$$|y_3\rangle - \boxed{P_3} -$$

$$|y_4\rangle - \boxed{P_4} -$$

3. Put your answer from the first two parts of this problem to express the output of the the following circuit as a function of x.

$$
\begin{array}{c}
|x_1\rangle - \\
|x_2\rangle - \\
\qquad\qquad QFT \\
|x_3\rangle - \\
|x_4\rangle - \\
\end{array}
\quad
\begin{array}{c}
- \boxed{P_1} - \\
- \boxed{P_2} - \\
- \boxed{P_3} - \\
- \boxed{P_4} - \\
\end{array}
$$

4. Finally, express the output of the following circuit. The inverse of the QFT maps from the Fourier amplitudes to the standard basis amplitudes.
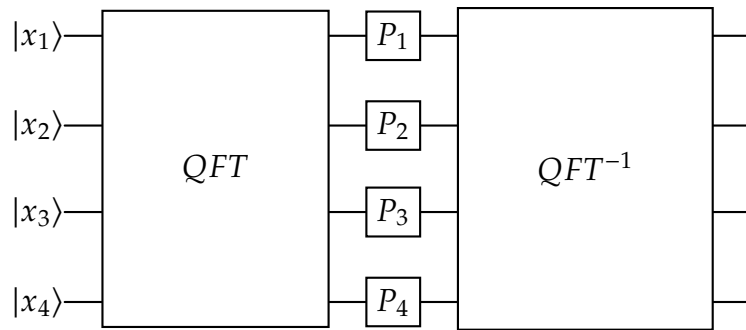
5. (Exploration) In Qiskit, the order of the bits is reversed, so you need to build your QFT circuit in a different order. The circuit we analyzed here is a great way to debug whether or not your QFT circuit is working correctly. When I implemented this in Qiskit though, the effect was the **opposite** of what the analysis here was doing. Does this happen for you too? Why do you think this is happening?

❋ Problem 3: Period Finding

Consider the Period Finding algorithm for the function $f : \{0, \ldots, N-1\} \to \{0, \ldots, M-1\}$, where $f(x) = 3^x \bmod M$. Here, $M = 14$ and $N = 16$.

1. What is the state of the algorithm before measuring the second register of qubits? That is, before applying the QFT to the first register.

2. Given the state you wrote out above, what are the possible measurement outcomes if we measure the second register? Label the measurement outcomes 1 to 6, from smallest to largest integer.

3. Suppose you measure the second register and observe outcome number 4 from above (this is the fourth largest outcome, not the measurement $|3\rangle$). What is the state after measurement?

4. Once the second register is measured, we can ignore it and focus on the first register. If we write the first register in the format

$$\frac{1}{\sqrt{s}} \sum_{j=0}^{s-1} |jr + l\rangle \tag{5}$$

what is r, and l?

✤ Problem 4: Shor's Algorithm (Code)

In this problem, you implement Shor's algorithm to factor 15. I want you to write the code for the quantum portion of the algorithm, and then solve the remaining problems.

In Edstem I will post template code for applying the function 2^s mode 15. When you apply your QFT, do not use a package and hardcode the gates yourself. You can use the gate

```
circ.cp(lambda, a, b)
```

to apply a controlled version of

$$P(\lambda) = e^{i\lambda}. \tag{6}$$

For this gate, the order of the control and target do not matter.

Use 4 classical bits to store your measurement results. The measurement result of the second register does not matter, as the goal is just to create a periodic state. Thus, you should measure the second register first and store this in your classical bits, then overwrite the result when you measure the first register.

1. What are the possible outcomes from measuring first register and which outcomes allow you to recover the period of 2^s mod 15?

2. After determining the period of 2^s mod 15, then how would you use that information to factor 15?

❖ Problem 5: More Bombs

Recall the bombs we talked about in the first module of the course. These bombs would detect photons passing through, and if they work, they would explode. If they were defective, nothing would happen. We used superposition to come up with a strategy to detect working bombs with nonzero probability, but let's see if we can do better using the geometric intuition we got from Grover's algorithm.

As a refresher, we model an experiment using the bombs in the following way:

$$|0\rangle \boxed{R_\theta} \boxed{B} \cdots \boxed{R_\theta} \boxed{B} \boxed{\nearrow}$$
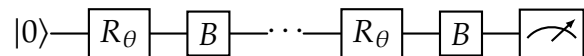
We have a laser initially pointing in the $|0\rangle$ direction, and then we use a beam splitter to create a superposition state of

$$\cos\theta \, |0\rangle + \sin\theta \, |1\rangle. \tag{7}$$

Given this state, the "Bomb gate" does the following:

- If the bomb is **defective**:

  - The gate acts as an **identity gate**.

- If the bomb is **not defective**:

  - The gate acts as a **standard basis measurement**. In other words, with probability $\cos^2\theta$ you observe $|0\rangle$ and with probability $\sin^2\theta$ you observe $|1\rangle$. If we measure $\sin^2\theta$, the bomb explodes.

1. Let's set $\theta = \frac{1}{100}$. Draw the state $R_\theta |0\rangle$ in the $|0\rangle$, $|1\rangle$ plane.

2. Draw the state after applying R_θ and B once each in the case that the bomb is **defective**. If there are multiple outcomes, label each outcome and its probability.

3. Draw the state after applying R_θ and B once each in the case that the bomb is **not defective**. If there are multiple outcomes, label each outcome and its probability.

4. Now suppose we applied the R_θ gate and B gate consecutively for a total of 50 times. Draw the state in the case that the bomb is **defective**. If there are multiple outcomes, label each outcome and its probability. In another picture, draw the state in the case that the bomb is **not defective**. If there are multiple outcomes, label each outcome and its probability.

5. How many applications of the pair of R_θ gate and B gate do we need to apply until we can maximally be certain about which case we are in? Call this number T.

6. (Bonus) Using the Chernoff bound, reason about how likely it is for the bomb to explode using this algorithm, given that it is **not defective**.