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. In one case, the power of ω will be a multiple of 7. What is the amplitude for this case?
4. The other case is when the previous statement is NOT true. What happens in this case? Pick some y and draw all the values that appear with this y in the complex plane.

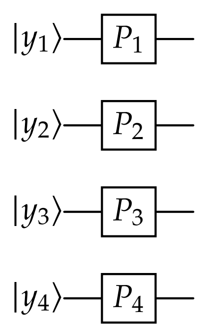
※ Problem 2: QFT Counter

Suppose $x \in \{0, \ldots, 15\}$ is a four bit string. Let $x_1x_2x_3x_4$ be the binary representation of the integer x.

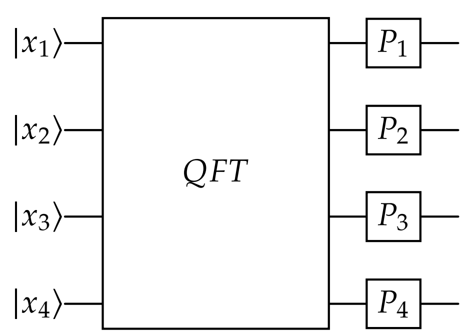
1. Express the state resulting from applying QFT_N to the state $|x\rangle$.

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

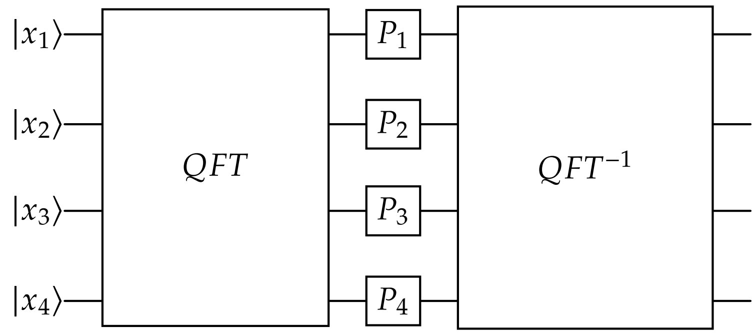
$$P_a = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^a} \end{bmatrix}. \tag{4}$$



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.



4. Finally, express the output of the following circuit. The inverse of the QFT maps from the Fourier amplitudes to the standard basis amplitudes.



|x1⟩
|x2⟩
|x3⟩
|x4⟩
QFT
P1
P2
P3
P4
QFT−1

❊ 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 after 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?