Raul Garcia-Patron
Petros Wallden
Milos Prokop

IQC 2023-24
November 20, 2023

Tutorial 6

Problem 1: Quantum Fourier Transform

As you have seen in the lectures, we can represent any integer z in its binary form as:

$$z = z_1 z_2 \dots z_n$$

where $z_1, z_2, \dots, z_n$ are such so that:

$$z = z_n 2^{n-1} + \dots + z_2 2^1 + z_1$$

a. How many qubits at least would we need to encode the integer states $|14\rangle$ and $|9\rangle$? What is their binary representation when using qubits to encode the integers?

Solution: In order to represent an integer state $|N\rangle$, one would require at least $n = \lceil \log(N+1) \rceil$ qubits. This implies that for both cases we require 4 qubits. The binary representation of these four-qubit integer states is:

$$|14\rangle = |1110\rangle$$
$$|9\rangle = |1001\rangle$$

b. Recall that:

$$0.z_l z_{l+1} \dots z_m \equiv \frac{z_l}{2} + \frac{z_{l+1}}{2^2} + \dots + \frac{z_m}{2^{m-l+1}}$$

Calculate:

1. $2^3 0.z_1 z_2 z_3$, $2^2 0.z_1 z_2 z_3$ and $20.z_1 z_2 z_3$, where $z_i \in \{0, 1\}$.
2. $e^{2\pi i 2^2 0.j_1 j_2 j_3}$ where $j_i \in \{0, 1\}$.

Solution: We start by writing down the expression for $0.z_1 z_2 z_3$:

$$0.z_1 z_2 z_3 = \frac{z_1}{2} + \frac{z_2}{4} + \frac{z_3}{8}$$

Then it is easy to calculate the expressions above. For the first case we have:

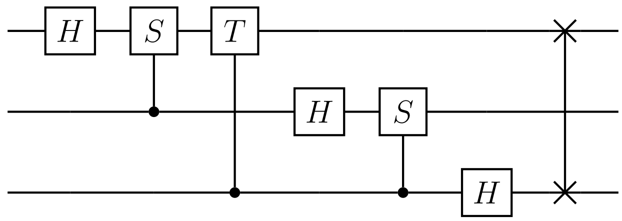
$$2^3 0.z_1 z_2 z_3 = 4z_1 + 2z_2 + z_3$$
$$2^2 0.z_1 z_2 z_3 = 2z_1 + z_2 + \frac{z_3}{2}$$
$$20.z_1 z_2 z_3 = z_1 + \frac{z_2}{2} + \frac{z_3}{4}$$

For the second case:

$$e^{2\pi i 2^2 0.j_1 j_2 j_3} = e^{2\pi i (2j_1 + j_2 + j_3/2)} = e^{2\pi i (2j_1 + j_2)} e^{2\pi i j_3/2} = e^{2\pi i 0.j_3},$$

where in the second equality we used the fact that $2j_1 + j_2$ is an integer and therefore $e^{2\pi i (2j_1 + j_2)} = 1$.

c. Now consider the quantum Fourier circuit for three qubits:

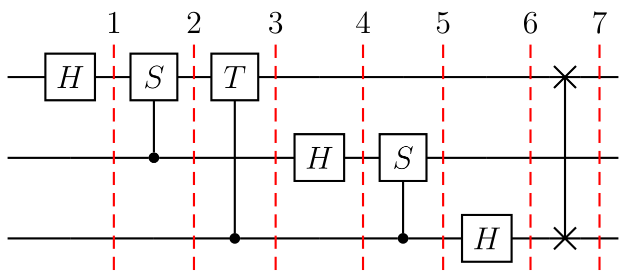


with S and T being the gates:

$$S = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

Suppose that we input the state $|j\rangle = |j_1 j_2 j_3\rangle$. What will be the output state?

Solution: We start as usual by dividing the quantum circuit into subsequent steps:



Initially, the system is in the state:

$$|\psi\rangle_0 = |j_1 j_2 j_3\rangle$$

Then we act with the Hadamard operator on the first qubit and use the fact that $e^{2\pi i 0.j_1}$ is $+1$ if $j_1 = 0$ and -1 if $j_1 = 1$. Thus the state at step 1 is transformed to:

$$|\psi\rangle_1 = \frac{1}{2^{1/2}}(|0\rangle + e^{2\pi i 0.j_1}|1\rangle)|j_2 j_3\rangle$$

Recall that the unitary operator R_k is defined as:

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix}$$

It's easy to see that both S and T are special cases of the operator R_k for two different choices of k. S corresponds to R_2 while T corresponds to R_3.

On the next step, applying the S operator on the first qubit controlled by the second qubits produces the state:

$$|\psi\rangle_2 = \frac{1}{2^{1/2}}(|0\rangle + e^{2\pi i 0.j_1} e^{2\pi i 0.0 j_2}|1\rangle)|j_2 j_3\rangle = \frac{1}{2^{1/2}}(|0\rangle + e^{2\pi i 0.j_1 j_2}|1\rangle)|j_2 j_3\rangle$$

Next, we perform the controlled-T operation and so we get:

$$|\psi\rangle_3 = \frac{1}{2^{1/2}}(|0\rangle + e^{2\pi i 0.j_1 j_2} e^{2\pi i 0.00 j_3} |1\rangle) |j_2 j_3\rangle = \frac{1}{2^{1/2}}(|0\rangle + e^{2\pi i 0.j_1 j_2 j_3} |1\rangle) |j_2 j_3\rangle$$

If we work with the exact same way for the rest of the steps we will get:
Step 4:

$$|\psi\rangle_4 = \frac{1}{2}(|0\rangle + e^{2\pi i 0.j_1 j_2 j_3} |1\rangle)(|0\rangle + e^{2\pi i 0.j_2}) |j_3\rangle$$

Step 5:

$$|\psi\rangle_4 = \frac{1}{2}(|0\rangle + e^{2\pi i 0.j_1 j_2 j_3} |1\rangle)(|0\rangle + e^{2\pi i 0.j_2 j_3}) |j_3\rangle$$

Step 6:

$$|\psi\rangle_4 = \frac{1}{2^{3/2}}(|0\rangle + e^{2\pi i 0.j_1 j_2 j_3} |1\rangle)(|0\rangle + e^{2\pi i 0.j_2 j_3})(|0\rangle + e^{2\pi i 0.j_3} |1\rangle)$$

At the final step, we swap the state of the first and third qubit and recover the *quantum Fourier transformation*:

$$|\psi\rangle_4 = \frac{1}{2^{3/2}}(|0\rangle + e^{2\pi i 0.j_3} |1\rangle)(|0\rangle + e^{2\pi i 0.j_2 j_3})(|0\rangle + e^{2\pi i 0.j_1 j_2 j_3} |1\rangle)$$

Problem 2: Order-Finding

For two positive integers x and N with $x < N$ the *order* of x modulo N is defined to be the *least positive integer* such that:

$$x^r = 1 \mod N$$

a. Show that for $x = 2$ and $N = 5$ we have $r = 4$.

Solution: It's easy to see that for $r = 4$:

$$2^4 = 3 \times 5 + 1,$$

which implies $2^4 = 1 \mod 5$. Similarly, one can show that $2^3 = 3 \mod 5$ and $2^2 = 4 \mod 5$. Therefore, $r = 4$ is the least integer such that $2^4 = 1 \mod 5$.

Note: Remark that modular exponentiation is a periodic function of period r. You can check that for $x = 3$ we also obtain $r = 4$, but for $x = 4$ we have $r = 2$, the latest can be easily derived from the case of $x = 2$.

b. Now consider the transformation U_x which acts on the computational basis states as follows:

$$U_x |y\rangle \equiv |xy \mod N\rangle$$

Prove that:

1. $U_x U_{x'} = U_{xx'}$
2. $U_{x^{-1}} = U_x^{-1} = U_x^\dagger$.
3. $U_x U_x^\dagger = U_x^\dagger U_x = I$, which proves it is an unitary transformation.
4. $U_x^r = I$ where r is the period of x modulo N.

Solution: We start with the first property, which result from the associativity of the multiplication of integer $\mod N$. We have:

$$U_x U_{x'} |y\rangle = U_x |x'y \mod N\rangle = |xx'y \mod N\rangle$$
$$U_{xx'} |y\rangle = |xx'y \mod N\rangle$$

and thus:

$$U_x U_{x'} = U_{xx'} = U_{x'} U_x$$

We continue with the second property:

$$U_{x^{-1}} U_x |y\rangle = U_{x^{-1}} |xy \mod N\rangle = |y\rangle$$

and thus:

$$U_{x^{-1}} = U_x^{-1}$$

Now for the second part of the second property:

$$\langle y| U_x^\dagger U_x |y\rangle = \langle yx \mod N|yx \mod N\rangle = 1$$

and thus $U_x^\dagger U_x = I$ and so the inverse of U_x is $U_x^\dagger$, i.e.:

$$U_{x^{-1}} = U_x^{-1} = U_x^\dagger$$

The third property follows immediately from the previous property as $U_x U_x^\dagger = U_x U_x^{-1} = I = U_x^\dagger U_x$ and thus U_x is a unitary operator.
Then for the final property we have:

$$\underbrace{U_x U_x \dots U_x}_{r} |y\rangle = |x^r y \mod N\rangle = |y\rangle$$

and so we proved that:

$$U_x^r = I$$

c. Show that the states:

$$|u_s\rangle \equiv \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\frac{2\pi i s k}{r}} |x^k \mod N\rangle$$

for integer $0 \leq s \leq r-1$ are eigenstates of U_x. What is their corresponding eigenvalues?

Solution: If we act with U_x on the states $|u_s\rangle$ we get:

$$U_x |u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\frac{2\pi i s k}{r}} U_x |x^k \mod N\rangle$$
$$= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{-\frac{2\pi i s k}{r}} |x^{k+1} \mod N\rangle = \frac{1}{\sqrt{r}} \sum_{k'=1}^{r} e^{-\frac{2\pi i s (k'-1)}{r}} |x^{k'} \mod N\rangle$$

where in the last step we switched the variable k with the variable $k' = k+1$. If we continue with the calculation we have:

$$U_x |u_s\rangle = e^{2\pi i s/r} \frac{1}{\sqrt{r}} \sum_{k'=1}^{r} e^{-\frac{2\pi i s k'}{r}} |x^{k'} \mod N\rangle$$

But recall that r is the order of x modulo N and so $x^r = 1 \mod N$. It's easy to see then that the sum in the expression can be replaced to:

$$\sum_{k'=1}^{r} \to \sum_{k=0}^{r-1},$$

as it correspond only to a reordering of the same sum (a shift to the left of a closed cycle). Thus, we can conclude that $|u_s\rangle$ is an eigenstate of the operator U_x with eigenvalue $e^{2\pi i s/r}$:

$$U_x |u_s\rangle = e^{2\pi i s/r} |u_s\rangle$$

d. As you can see preparing the state $|u_s\rangle$ requires that we know r in advance. Fortunately there is clever observation which circumvents the problems of preparing $|u_s\rangle$. Show that:

1.
$$\sum_{s=0}^{r-1} e^{-2\pi i s k/r} = r\delta_{k,0}$$

2.
$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{2\pi i s k/r} |u_s\rangle = |x^k \mod N\rangle$$

which has as special case when $k=0$:

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle,$$

which is a trivial state to generate. This opens the door to applying quantum phase-estimation to sample from $\varphi = s/r$, which later leads to a guess of r as explained in the lecture on Shor's algorithm.

Solution: Consider the first expression and let $k = 0$. It's easy to see that we have a sum of r terms, all equal to the identity and thus:

$$\sum_{s=0}^{r-1} e^{-2\pi i s k/r} = r \text{ if } k = 0$$

Now consider $k \neq 0$. The sum then corresponds to a geometric series which is equal to:

$$\sum_{s=0}^{r-1} e^{-2\pi i s k/r} = \frac{1 - e^{-2\pi i k}}{1 - e^{-2\pi i k/r}} = 0$$

for every $k \in \mathbb{Z}$ with $k \neq 0$. Thus we can conclude that:

$$\sum_{s=0}^{r-1} e^{-2\pi i s k/r} = r\delta_{k,0}$$

For the second expression we have:

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{2\pi i s k/r} |u_s\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \left[e^{2\pi i s k/r} \frac{1}{\sqrt{r}} \sum_{k'=0}^{r-1} e^{-\frac{2\pi i s k'}{r}} |x^{k'} \mod N\rangle \right]$$
$$= \frac{1}{r} \sum_{s=0}^{r-1} \sum_{k'=0}^{r-1} e^{2\pi i s(k-k')/r} |x^k \mod N\rangle = \frac{1}{r} \sum_{k'=0}^{r-1} r\delta_{0,k-k'} |x^{k'} \mod N\rangle$$

where in the last equality we used the result from expression 1. It's trivial to see that $\delta_{0,k-k'} = \delta_{k,k'}$ and the sum over k' contributes only when $k' = k$. Thus:

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{2\pi i s k/r} |u_s\rangle = |x^k \mod N\rangle .$$

The case $k = 1$ is only a corollary of this last result, leading to the input state $|1\rangle$ used in the order finding algorithm.

e. If we wanted to apply a phase estimation procedure we must have efficient procedures to implement a controlled-U^{2^j} operation for any integer j. Given an integer number x, propose a technique to compute x^{2^k} that scales linearly in k.

Solution: if we want to compute x^{2^k} an inefficient approach is to multiply 2^k times x. A more efficient approach is to square iteratively, i.e., we apply the function $y^2 \mod N$ k times to the input x. It is easy to see then that we get the series x^2, x^4, x^{2^3},..., x^{2^k}. Because the multiplication is $\mod N$, the memory register does not need to increase, as it will never be larger than N.

f. Assuming that we are given an unitary S such that implements $S|x\rangle = |x^2 \mod N\rangle$ that needs $O(L^2)$ gates, where $L = \lceil \log N \rceil$, i.e., the size of the register. How many gates we will be needed to implement $|x\rangle \to |x^{2^k} \mod N\rangle$?

Solution: We are given that the unitary S is such that implements $S|x\rangle = |x^2 \mod N\rangle$ using $O(L^2)$ gates. Clearly if we want to implement $|x\rangle \to |x^{2^k} \mod N\rangle$ we need to apply S k times, which lead to an asymptotic scaling $O(kL^2)$ of number of gates. Because in phase estimation we need to implement up to U^{2^k} where $k \in \{0, 2L+1\}$, it is easy to see that need $O(L^3)$ gates.