QFT, quantum phase estimation, order finding & Shor's algorithm

1. QFT

- Definition

One such transformation is the *discrete Fourier transform*. In the usual mathematical notation, the discrete Fourier transform takes as input a vector of complex numbers, $x_0, \ldots, x_{N-1}$ where the length N of the vector is a fixed parameter. It outputs the transformed data, a vector of complex numbers $y_0, \ldots, y_{N-1}$, defined by

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i jk/N} . \tag{5.1}$$

The *quantum Fourier transform* is exactly the same transformation, although the conventional notation for the quantum Fourier transform is somewhat different. The quantum Fourier transform on an orthonormal basis $|0\rangle, \ldots, |N-1\rangle$ is defined to be a linear operator with the following action on the basis states,

$$|j\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i jk/N} |k\rangle . \tag{5.2}$$

Equivalently, the action on an arbitrary state may be written

$$\sum_{j=0}^{N-1} x_j |j\rangle \longrightarrow \sum_{k=0}^{N-1} y_k |k\rangle , \tag{5.3}$$

where the amplitudes y_k are the discrete Fourier transform of the amplitudes x_j. It is not obvious from the definition, but this transformation is a unitary transformation, and thus can be implemented as the dynamics for a quantum computer. We shall demonstrate the unitarity of the Fourier transform by constructing a manifestly unitary quantum circuit computing the Fourier transform. It is also easy to prove directly that the Fourier transform is unitary:

Exercise 5.1: Give a direct proof that the linear transformation defined by Equation (5.2) is unitary.

- 1-qubit example

Consider how the QFT operator as defined above acts on a single qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. In this case, $x_0 = \alpha$, $x_1 = \beta$, and $N = 2$. Then,

$$y_0 = \frac{1}{\sqrt{2}}\left(\alpha \exp\left(2\pi i \frac{0 \times 0}{2}\right) + \beta \exp\left(2\pi i \frac{1 \times 0}{2}\right)\right) = \frac{1}{\sqrt{2}}(\alpha + \beta)$$

and

$$y_1 = \frac{1}{\sqrt{2}}\left(\alpha \exp\left(2\pi i \frac{0 \times 1}{2}\right) + \beta \exp\left(2\pi i \frac{1 \times 1}{2}\right)\right) = \frac{1}{\sqrt{2}}(\alpha - \beta)$$

such that the final result is the state

$$U_{QFT}|\psi\rangle = \frac{1}{\sqrt{2}}(\alpha + \beta)|0\rangle + \frac{1}{\sqrt{2}}(\alpha - \beta)|1\rangle$$

This operation is exactly the result of applying the Hadamard operator (H) on the qubit:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

If we apply the H operator to the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, we obtain the new state:

$$\frac{1}{\sqrt{2}}(\alpha + \beta)|0\rangle + \frac{1}{\sqrt{2}}(\alpha - \beta)|1\rangle \equiv \tilde{\alpha}|0\rangle + \tilde{\beta}|1\rangle$$

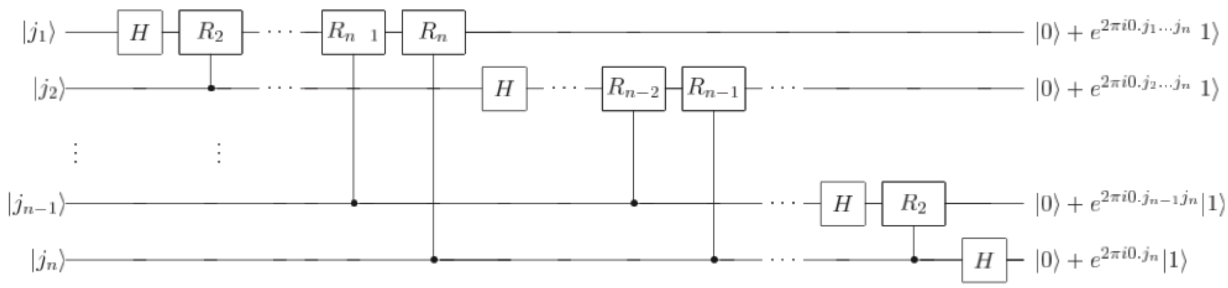
Notice how the Hadamard gate performs the discrete Fourier transform for $N = 2$ on the amplitudes of the state.

- Factorization

In the following, we take $N = 2^n$, where n is some integer, and the basis $|0\rangle, \ldots, |2^n - 1\rangle$ is the computational basis for an n qubit quantum computer. It is helpful to write the state $|j\rangle$ using the binary representation $j = j_1 j_2 \ldots j_n$. More formally, $j = j_1 2^{n-1} + j_2 2^{n-2} + \cdots + j_n 2^0$. It is also convenient to adopt the notation $0.j_l j_{l+1} \ldots j_m$ to represent the *binary fraction* $j_l/2 + j_{l+1}/4 + \cdots + j_m/2^{m-l+1}$.

$$
\begin{aligned}
|j\rangle \rightarrow & \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi i jk/2^n} |k\rangle \\
&= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \dots \sum_{k_n=0}^{1} e^{2\pi i j \left(\sum_{l=1}^{n} k_l 2^{-l}\right)} |k_1 \dots k_n\rangle \\
&= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \dots \sum_{k_n=0}^{1} \bigotimes_{l=1}^{n} e^{2\pi i j k_l 2^{-l}} |k_l\rangle \\
&= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[\sum_{k_l=0}^{1} e^{2\pi i j k_l 2^{-l}} |k_l\rangle \right] \\
&= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[|0\rangle + e^{2\pi i j 2^{-l}} |1\rangle \right] \\
&= \frac{\left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi i 0.j_1 j_2 \cdots j_n}|1\rangle\right)}{2^{n/2}}
\end{aligned}
$$

- Circuit Realization



$$
R_k \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix} \qquad \boldsymbol{H} : |j_k\rangle \rightarrow \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i 0.j_k}|1\rangle\right)
$$

- Complexity

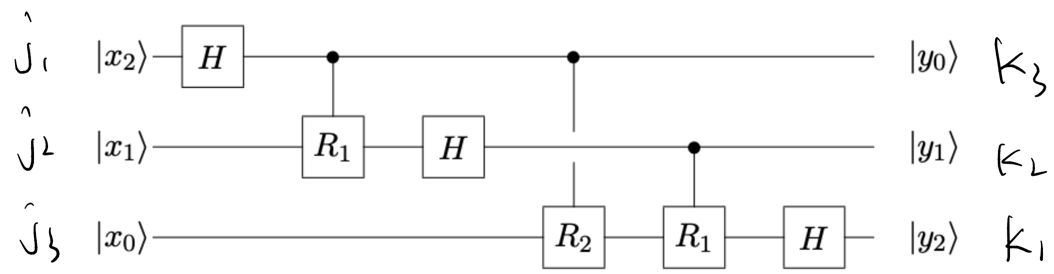
In the case $n = 3$, the QFT is constructed from three $\boldsymbol{H}$ gates and three controlled-$\boldsymbol{R}$ gates. For general n, the obvious generalization of this circuit requires n $\boldsymbol{H}$ gates and $\binom{n}{2} = \frac{1}{2}n(n-1)$ controlled R's. A two qubit gate is applied to each pair of qubits, again with controlled relative phase $\pi/2^d$, where d is the "distance" between the qubits. Thus the circuit family that implements QFT has a size of order $(\log N)^2$.

We can reduce the circuit complexity to linear in $\log N$ if we are willing to settle for an implementation of fixed accuracy, because the two-qubit gates acting on distantly separated qubits contribute only exponentially small phases. If we drop the gates acting on pairs with distance greater than m, than each term in eq. (6.52) is replaced by an approximation to m bits of accuracy; the total error in $xy/2^n$ is certainly no worse than $n2^{-m}$, so we can achieve accuracy ε in $xy/2^n$ with $m \geq \log n/\varepsilon$. If we retain only the gates acting on qubit pairs with distance m or less, then the circuit size is $mn \sim n \log n/\varepsilon$.

In contrast, the best classical algorithms for computing the discrete Fourier transform on 2^n elements are algorithms such as the *Fast Fourier Transform (FFT)*, which compute the discrete Fourier transform using $\Theta(n2^n)$ gates. That is, it requires exponentially more operations to compute the Fourier transform on a classical computer than it does to implement the quantum Fourier transform on a quantum computer.

- Simplification

In fact, if we are going to measure in the computational basis immediately after implementing the QFT (or its inverse), a further simplification is possible – no two-qubit gates are needed at all! We first remark that the controlled – $\boldsymbol{R}_d$ gate acts symmetrically on the two qubits – it acts trivially on $|00\rangle, |01\rangle$, and $|10\rangle$, and modifies the phase of $|11\rangle$ by $e^{i\theta_d}$. Thus, we can interchange the "control" and "target" bits without modifying the gate. With this change, our circuit for the 3-qubit QFT can be redrawn as:



Once we have measured $|y_0\rangle$, we *know* the value of the control bit in the controlled-$\boldsymbol{R}_1$ gate that acted on the first two qubits. Therefore, we will obtain the same probability distribution of measurement outcomes if, instead of applying controlled-$\boldsymbol{R}_1$ and then measuring, we instead measure y_0 first, and then apply $(\boldsymbol{R}_1)^{y_0}$ to the next qubit, conditioned on the outcome of the measurement of the first qubit. Similarly, we can replace the controlled-$\boldsymbol{R}_1$ and controlled-$\boldsymbol{R}_2$ gates acting on the third qubit by the single qubit rotation

$$(\boldsymbol{R}_2)^{y_0}(\boldsymbol{R}_1)^{y_1}, \tag{6.58}$$

(that is, a rotation with relative phase $\pi(.y_1y_0)$) *after* the values of y_1 and y_0 have been measured.

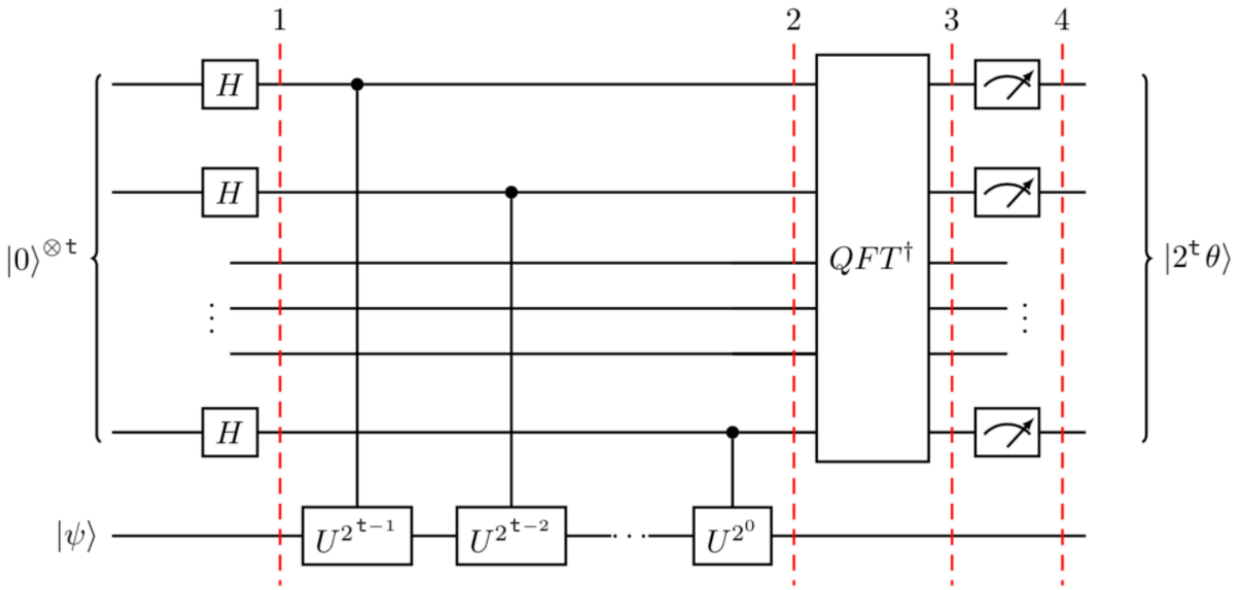
Altogether then, if we are going to measure after performing the QFT, only n Hadamard gates and $n-1$ single-qubit rotations are needed to implement it. The QFT is remarkably simple!

2. **Quantum phase estimation**

- Basic algorithm

Quantum phase estimation is one of the most important subroutines in quantum computation. It serves as a central building block for many quantum algorithms. The objective of the algorithm is the following:

Given a unitary operator U, the algorithm estimates θ in $U|\psi\rangle = e^{2\pi i\theta}|\psi\rangle$. Here $|\psi\rangle$ is an eigenvector and $e^{2\pi i\theta}$ is the corresponding eigenvalue. Since U is unitary, all of its eigenvalues have a norm of 1.



t = n

i. Setup: $|\psi\rangle$ is in one set of qubit registers. An additional set of n qubits form the counting register on which we will store the value $2^n\theta$:

$$|\psi_0\rangle = |0\rangle^{\otimes n}|\psi\rangle$$

ii. Superposition: Apply a n-bit Hadamard gate operation $H^{\otimes n}$ on the counting register:

$$|\psi_1\rangle = \frac{1}{2^{\frac{n}{2}}}(|0\rangle + |1\rangle)^{\otimes n}|\psi\rangle$$

iii. Controlled Unitary Operations: We need to introduce the controlled unitary CU that applies the unitary operator U on the target register only if its corresponding control bit is $|1\rangle$. Since U is a unitary operator with eigenvector $|\psi\rangle$ such that $U|\psi\rangle = e^{\boldsymbol{2\pi i\theta}}|\psi\rangle$, this means:

$$U^{2^j}|\psi\rangle = U^{2^j-1}U|\psi\rangle = U^{2^j-1}e^{2\pi i\theta}|\psi\rangle = \cdots = e^{2\pi i 2^j\theta}|\psi\rangle$$

Applying all the n controlled operations CU^{2^j} with $0 \le j \le n-1$, and using the relation $|0\rangle \otimes |\psi\rangle + |1\rangle \otimes e^{2\pi i\theta}|\psi\rangle = \big(|0\rangle + e^{2\pi i\theta}|1\rangle\big) \otimes |\psi\rangle$:

$$|\psi_2\rangle = \frac{1}{2^{\frac{n}{2}}}\Big(|0\rangle + e^{\boldsymbol{2\pi i\theta 2^{n-1}}}|1\rangle\Big) \otimes \cdots \otimes \Big(|0\rangle + e^{\boldsymbol{2\pi i\theta 2^{1}}}|1\rangle\Big) \otimes \Big(|0\rangle + e^{\boldsymbol{2\pi i\theta 2^{0}}}|1\rangle\Big) \otimes |\psi\rangle$$

$$= \frac{1}{2^{\frac{n}{2}}}\sum_{k=0}^{2^n-1} e^{\boldsymbol{2\pi i\theta k}}|k\rangle \otimes |\psi\rangle$$

where k denotes the integer representation of n-bit binary numbers.

iv. Inverse Fourier Transform: Notice that the above expression is exactly the result of applying a quantum Fourier transform as we derived in the notebook on Quantum Fourier Transform and its Qiskit Implementation. Recall that QFT maps an n-qubit input state $|x\rangle$ into an output as

$$QFT|x\rangle = \frac{1}{2^{\frac{n}{2}}}\Big(|0\rangle + e^{\frac{2\pi i}{2}x}|1\rangle\Big) \otimes \Big(|0\rangle + e^{\frac{2\pi i}{2^2}x}|1\rangle\Big) \otimes \ldots \otimes \Big(|0\rangle + e^{\frac{2\pi i}{2^{n-1}}x}|1\rangle\Big) \otimes \Big(|0\rangle + e^{\frac{2\pi i}{2^n}x}|1\rangle\Big)$$

Replacing x by $2^n\theta$ in the above expression gives exactly the expression derived in step 2 above. Therefore, to recover the state $|2^n\theta\rangle$, apply an inverse Fourier transform on the auxiliary register. Doing so, we find

$$|\psi_3\rangle = \frac{1}{2^{\frac{n}{2}}}\sum_{k=0}^{2^n-1} e^{\boldsymbol{2\pi i\theta k}}|k\rangle \otimes |\psi\rangle \xrightarrow{\mathcal{QFT}_n^{-1}} \frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{k=0}^{2^n-1} e^{-\frac{2\pi i k}{2^n}(x-2^n\theta)}|x\rangle \otimes |\psi\rangle$$

v. Measurement: The above expression peaks near $x = 2^n\theta$. For the case when $2^n\theta$ is an integer, measuring in the computational basis gives the phase in the auxiliary register with high probability:

$$|\psi_4\rangle = |2^n\theta\rangle \otimes |\psi\rangle$$

For the case when $2^n\theta$ is not an integer, it can be shown that the above expression still peaks near $x = 2^n\theta$ with probability better than $4/\pi^2 \approx 40\%$ [1].

- Performance

suppose $\theta = 0.\theta_1\theta_2\cdots\theta_n\theta_{n+1}\cdots$ $\quad 2^n\theta = \theta_1\theta_2\cdots\theta_n.\theta_{n+1}\cdots$

$$\alpha_x = \frac{1}{2^n}\sum_k e^{-\frac{2\pi i k}{2^n}(x-2^n\theta)}$$

$\tilde{x} = x - \theta_1\theta_2\cdots\theta_n$

$\delta = 0.00\cdots0\theta_{n+1}$

$$\alpha_{\tilde{x}} = \frac{1}{2^n}\sum_k e^{-2\pi i\left(\frac{\tilde{x}}{2^n}-\delta\right)}$$

$$= \frac{1}{2^n}\frac{1-e^{-2\pi i(\tilde{x}-2^n\delta)}}{1-e^{-2\pi i\left(\frac{\tilde{x}}{2^n}-\delta\right)}}$$

$|1-e^{i\theta}| \geq 2|\theta|/\pi \quad \theta\in[-\pi,\pi]$

$|1-e^{i\theta}| \leq |\theta|$

- $\tilde{x}=0$: $\alpha_0 = \frac{1}{2^n}\frac{1-e^{2\pi i\cdot 2^n\cdot\delta}}{1-e^{i2\pi i\delta}} \geq \frac{1}{2^n}\frac{2\cdot 2\pi\cdot 2^n\cdot\delta/\pi}{2\pi\cdot\delta} = \frac{2}{\pi}$ $\quad P_0 \geq \frac{4}{\pi^2}$

- $|\tilde{x}|>L$: $|\alpha_{\tilde{x}}| \leq \frac{1}{2^n}\frac{2}{2\cdot 2\cdot\left|\frac{\tilde{x}}{2^n}-\delta\right|} = \frac{1}{2\left|\tilde{x}-\delta\cdot 2^n\right|} \leq \begin{cases}\frac{1}{2(\tilde{x}-1)} & \tilde{x}>L\\ \frac{1}{2|\tilde{x}|} & \tilde{x}<-L\end{cases}$

- $$\sum_{|\tilde{x}|>L} P_{\tilde{x}} \leq \sum_{\tilde{x}>L}\frac{1}{4(\tilde{x}-1)^2} + \sum_{\tilde{x}<-L}\frac{1}{4\tilde{x}^2}$$

$$\leq \frac{1}{2}\sum_{\tilde{x}\geq L}\frac{1}{\tilde{x}^2} \leq \frac{1}{2}\int_{L-1}^{2^{n-1}}\frac{1}{\tilde{x}^2}d\tilde{x} \leq \frac{1}{2(L-1)}$$

- $L = 2^{n-m}-1$

$$\delta = \frac{1}{2(2^{n-m}-1)} \Rightarrow n = \log\left(\frac{1}{2\delta}+1\right)+m$$

- General input states

$U = \sum e^{i\theta_i}|u_i\rangle\langle u_i|$

$|\psi\rangle = \sum \alpha_i|u_i\rangle$

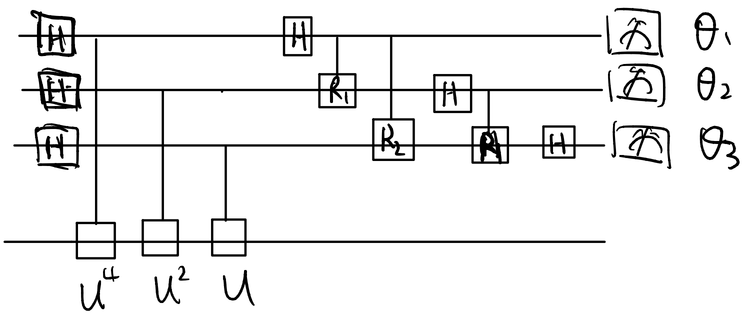
$|0\rangle^{\otimes n}\cdot|\psi\rangle \longrightarrow \sum \alpha_i|\tilde{\theta}_i\rangle|u_i\rangle$

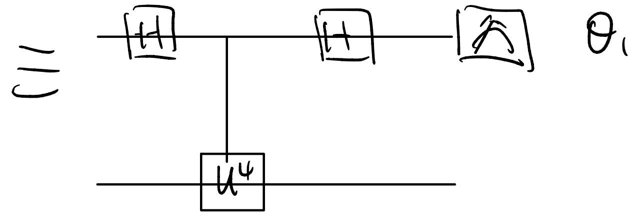
e.g. $U = e^{iM}$ $\quad M = \sum\lambda_i|u_i\rangle\langle u_i|$

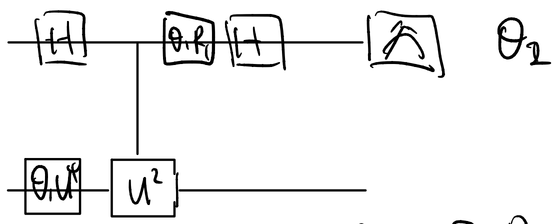
$= \sum e^{i\lambda_i}|u_i\rangle\langle u_i|$

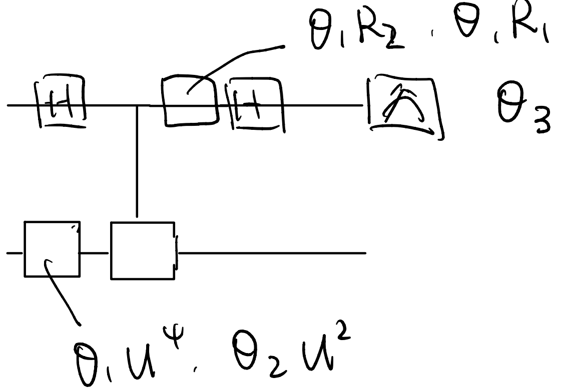
Outputs eigenvalues & eigenvectors of M.

- Kitaev's version (Iterative QPE)









Refs. 1. Nielsen, Chuang book.

2. John preskill's lecture notes