Quantum Fourier Transform

based on: learn.qiskit.org/course/ch-algorithms/quantum-fourier-transform

Starting from the beginning, the Fourier transform (FT) is a mathematical operation that converts a function into a form that describes the frequencies present in the original function. Functions that are localized in the time domain have FTs that are spread out across the frequency domain and vice versa. This is known as uncertainty principle and has a critical importance on Quantum Mechanics (QM). In QM we have serveral quantities that are related through a FT (position - momentum, energy-time...) and, if we measure one of the two with high presision, then the accuracy on the other one is very poor. For example, in the extreme case where we measure the position of a particle exactly, we can not obtain any information about its momentum (you will learn more about this in QM courses during the third year).

The classical FT of a function $f(x)$ is

$$\hat{f}(\xi) = \int_{-\infty}^{\infty} f(x)\, e^{-2\pi i \xi x}\, dx$$

and the Fourier inversion integral is given by

$$f(x) = \int_{-\infty}^{\infty} \hat{f}(\xi)\, e^{2\pi i \xi x}\, d\xi$$

x and ξ are conjugated variables. For example, time and frequency. Or, in QM, we can have x the position and $p \equiv \xi$ the momentum.

The FT occurs in many different versions throughout classical computing, in areas ranging from signal processing to data compression to complexity theory. The Quantum FT (QFT) is the quantum implementation of the discrete FT over the amplitudes of a wavefunction. It is part of many quantum algorithms, most notably Shor's factoring algorithm and quantum phase estimation.

The discrete FT acts on a vector $(x_0, \dots, x_{N-1})$ and maps it to the vector $(y_0, \dots, y_{N-1})$ according to

$$y_K = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \, w_N^{jK} \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \, e^{2\pi i \frac{jK}{N}} \; ; \; w_N^{jK} \equiv e^{2\pi i \frac{jK}{N}}$$

Similarly, the QFT acts on a quantum state $|x\rangle = \sum_{j=0}^{N-1} x_j |j\rangle$ and maps it to the quantum state $|y\rangle = \sum_{K=0}^{N-1} y_K |K\rangle$ according to

$$y_K = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \, w_N^{jK} = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \, e^{2\pi i \frac{jK}{N}}$$

Note that only the amplitudes of the state were affected by this transformation.

This can also be expressed as the map:

$$|j\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{K=0}^{N-1} w_N^{jK} |K\rangle$$

Or the unitary matrix:

$$U_{QFT} = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \sum_{K=0}^{N-1} w_N^{jK} |K\rangle\langle j|$$

$|j\rangle$ basis $\rightarrow \langle j|j\rangle = 1$

So, with this we have

$$|y\rangle = U_{QFT}|x\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \sum_{K=0}^{N-1} w_N^{jK} |K\rangle\langle j| \, x_j |j\rangle = \sum_{K=0}^{N-1} \underbrace{\frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j w_N^{jK}}_{= y_K} |K\rangle$$

$$\Rightarrow |y\rangle = U_{QFT}|x\rangle = \sum_{K=0}^{N-1} y_K |K\rangle$$

as expected.

The QFT transforms between two bases, the computational (Z) basis, and the Fourier basis. The Hadamard H-gate is the single-qubit QFT (we will check it later), and it transforms between the Z-basis states $|0\rangle$ and $|1\rangle$ to the X-basis states $|+\rangle$ and $|-\rangle$. In the same way, all multi-qubits states in the computational basis have corresponding states in the Fourier basis. The QFT is simply the function that transforms between these bases.

|State in Computational Basis⟩ $\xrightarrow{QFT}$ |State in Fourier Basis⟩

$QFT|x\rangle = |\tilde{x}\rangle$ (we use tilde ~ to denote states in Fourier Basis)

(See 2.1 in the link given on first page for some Intuition about QFT)

Example: 1-qubit QFT

Consider how the QFT operator 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 $N=2$. Thus:

$$y_0 = \frac{1}{\sqrt{2}} \sum_{j=0}^{1} x_j \, w_2^{j0} = \frac{1}{\sqrt{2}}\left(x_0 w_2^{00} + x_1 w_2^{10}\right) = \frac{1}{\sqrt{2}}\left(\alpha e^{2\pi i \frac{0\cdot 0}{2}} + \beta e^{2\pi i \frac{1\cdot 0}{2}}\right) = \frac{1}{\sqrt{2}}(\alpha+\beta)$$

$$y_1 = \frac{1}{\sqrt{2}} \sum_{j=0}^{1} x_j \, w_2^{j1} = \frac{1}{\sqrt{2}}\left(x_0 w_2^{01} + x_1 w_2^{11}\right) = \frac{1}{\sqrt{2}}\left(\alpha e^{2\pi i \frac{0\cdot 1}{2}} + \beta e^{2\pi i \frac{1\cdot 1}{2}}\right) = \frac{1}{\sqrt{2}}(\alpha-\beta)$$

$e^{i\pi} = -1$

then, 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: $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

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

$$H|\psi\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\left(\alpha|0\rangle + \beta|1\rangle\right) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\left[\alpha\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right] = \frac{1}{\sqrt{2}}\left[\alpha\begin{pmatrix} 1 \\ 1 \end{pmatrix} + \beta\begin{pmatrix} 1 \\ -1 \end{pmatrix}\right] =$$

$$= \frac{1}{\sqrt{2}}\left[\alpha(|0\rangle + |1\rangle) + \beta(|0\rangle - |1\rangle)\right] = \frac{1}{\sqrt{2}}(\alpha+\beta)|0\rangle + \frac{1}{\sqrt{2}}(\alpha-\beta)|1\rangle \equiv \tilde{\alpha}|0\rangle + \tilde{\beta}|1\rangle$$

as before. Therefore, the Hadamard gate performs the discrete FT for $N=2$ on the amplitudes of the state.

The Quantum Fourier Transform

Let us now derive the QFT of a general state. Consider that we have $N=2^n$, QFT_N acting on the state $|x\rangle = |x_1 \dots x_n\rangle$ where x_1 is the most significant bit: $\quad w_N^{xy} = e^{2\pi i \frac{xy}{N}}$; $N = 2^n$

$$QFT_N|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} w_N^{xy}|y\rangle \overset{\downarrow}{=} \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \exp\left(\frac{2\pi i xy}{2^n}\right)|y\rangle$$

Now we use the fractional binary rotation. If we have a binary string $y = y_1 y_2 \cdots y_n$, where y_k can be 0 or 1, then we can write:

$$y = 2^{n-1}y_1 + 2^{n-2}y_2 + \cdots + 2^0 y_n = 2^n \sum_{K=1}^{n} \frac{y_K}{2^K}$$

For example, 5 in binary is 101, we have $n=3$:

$$2^{3-1}\cdot 1 + 2^{3-2}\cdot 0 + 2^{3-3}\cdot 1 = 4+0+1 = 5$$

With this we can rewrite

$$QFT_N|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \exp\left\{2\pi i\left(\sum_{K=1}^{n} \frac{y_K}{2^K}\right)x\right\}|y_1 \cdots y_n\rangle$$

Now we expand the exponential of a sum to a product of exponentials: $e^{a+b} = e^a \cdot e^b$

$$QFT_N|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \prod_{K=1}^{n} e^{2\pi i x y_K/2^K} |y_1 \cdots y_n\rangle$$

We rearrange the sum and products and expand $\sum_{y=0}^{N-1} = \sum_{y_1=0}^{1} \sum_{y_2=0}^{1} \cdots \sum_{y_n=0}^{1}$

with this every sum has only two terms and the products become tensorial products

$$QFT_N|x\rangle = \frac{1}{\sqrt{N}} \bigotimes_{K=1}^{n} \left(|0\rangle + e^{2\pi i x/2^K}|1\rangle\right)$$

which explicitly is

$$\boxed{QFT_N|x\rangle = \frac{1}{\sqrt{N}} \left(|0\rangle + e^{\frac{2\pi i}{2}x}|1\rangle\right) \otimes \left(|0\rangle + e^{\frac{2\pi i}{4}x}|1\rangle\right) \otimes \cdots \otimes \left(|0\rangle + e^{\frac{2\pi i}{2^n}x}|1\rangle\right)}$$

(see the link for representation of states with 4 qubits)

The circuit that implements the QFT

The implementation of the QFT on a circuit requires two gates. The first one is the single-qubit Hadamard gate, H. The action of H on the single-qubit state $|x_k\rangle$ is

$$H|x_k\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + \exp\left(\frac{2\pi i}{2} x_k\right)|1\rangle\right)$$

[In the previous example we saw that

$$H|\psi\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\left[\alpha|0\rangle + \beta|1\rangle\right] = \frac{1}{\sqrt{2}}\alpha\left(|0\rangle + |1\rangle\right) + \frac{1}{\sqrt{2}}\beta\left(|0\rangle - |1\rangle\right)$$

thus, $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$]

The second one is a two-qubit controlled rotation $CROT_k$ given by

$$CROT_k = \begin{pmatrix} I & 0 \\ 0 & UROT_k \end{pmatrix}$$

with

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad ; \quad UROT_k = \begin{pmatrix} 1 & 0 \\ 0 & \exp\left(\frac{2\pi i}{2^k}\right) \end{pmatrix}$$

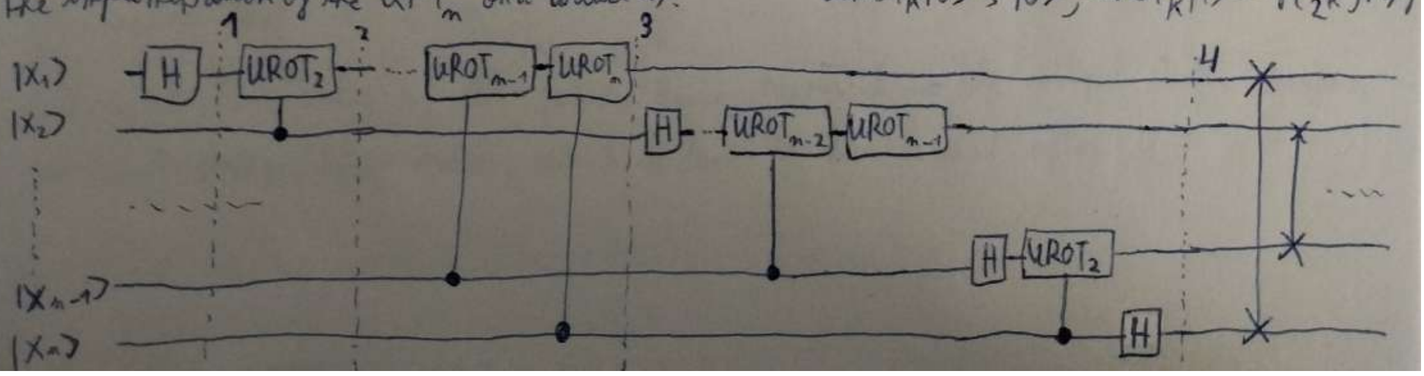
You can see the action of $CROT_k$ on a two-qubit state as applying the identity to the first one and giving a phase to the second one if the first is $|1\rangle$.
For example, given the state $|x_l x_j\rangle$ the action of the $CROT_k$ on it with the first qubit being the control and the second the target is

$$CROT|0x_j\rangle = |0x_j\rangle \quad \text{(control qubit is } |0\rangle\text{, no phase)}$$

$$CROT|1x_j\rangle = \exp\left(\frac{2\pi i}{2^k} x_j\right)|1x_j\rangle$$ (control qubit is $|1\rangle$, we add a phase if the target qubit is also 1.

$UROT_k|0\rangle = |0\rangle$; $UROT_k|1\rangle = \exp\left(\frac{2\pi i}{2^k}\right)|1\rangle$

The implementation of the QFT_n on a circuit is:



Let us check how the circuit operates on a general n-qubit input state $|x_1 x_2 \cdots x_n\rangle$

① Apply H gate to qubit 1

$$H_1 |x_1 x_2 \cdots x_n\rangle = \frac{1}{\sqrt{2}} \left[|0\rangle + \exp\left(\frac{2\pi i}{2} x_1\right) |1\rangle \right] \otimes |x_2 x_3 \cdots x_n\rangle$$

② After applying the $UROT_2$ gate on qubit 1 controlled by qubit 2 the state transforms to

$$\frac{1}{\sqrt{2}} \left[|0\rangle + \exp\left(\frac{2\pi i}{2} x_1 + \frac{2\pi i}{2^2} x_2\right) |1\rangle \right] \otimes |x_2 x_3 \cdots x_n\rangle$$

(we never add a phase to $|0\rangle$ and we add it to $|1\rangle$ if both $|x_1\rangle$ and $|x_2\rangle$ are $|1\rangle$)

③ We can see how this works, every UROT adds a phase to $|1\rangle$, so after applying the $UROT_n$ gate we get

$$\frac{1}{\sqrt{2}} \left[|0\rangle + \exp\left(\frac{2\pi i}{2} x_1 + \frac{2\pi i}{2^2} x_2 + \cdots + \frac{2\pi i}{2^n} x_n\right) |1\rangle \right] \otimes |x_2 x_3 \cdots x_n\rangle$$

now we use again the fractional binary notation

$$x = 2^{n-1} x_1 + 2^{n-2} x_2 + \cdots + 2^0 x_n \to \frac{x}{2^n} = \frac{x_1}{2} + \frac{x_2}{2^2} + \cdots + \frac{x_n}{2^n}$$

then we can rewrite the state as

$$\frac{1}{\sqrt{2}} \left[|0\rangle + \exp\left(\frac{2\pi i}{2^n} x\right) |1\rangle \right] \otimes |x_2 x_3 \cdots x_n\rangle$$

④ Finally, in subsequent states we apply similar sequences of gates, applying in every qubit 1 UROT gate less than in the previous state, so we have

$$\frac{1}{\sqrt{2}} \left[|0\rangle + \exp\left(\frac{2\pi i}{2^n} x\right) |1\rangle \right] \otimes \frac{1}{\sqrt{2}} \left[|0\rangle + \exp\left(\frac{2\pi i}{2^{n-1}} x\right) |1\rangle \right] \otimes \cdots \otimes \frac{1}{\sqrt{2}} \left[|0\rangle + \exp\left(\frac{2\pi i}{2^2} x\right) |1\rangle \right] \otimes$$

$$\otimes \frac{1}{\sqrt{2}} \left[|0\rangle + \exp\left(\frac{2\pi i}{2^1} x\right) |1\rangle \right]$$

Which is the same expression of the QFT that we derived before (remember that $N = 2^n \to \frac{1}{\sqrt{N}} = \frac{1}{\sqrt{2^n}}$)

but with the order of the qubits being reversed in the output state. Therefore, we must swap their order, which is done in the circuit after 4

Example: 3-qubit QFT

$N = 2^3 = 8$

We want to compute $|y_3 y_2 y_1\rangle = QFT_8 |x_3 x_2 x_1\rangle$. Following the previous discussion, have to start by applying a H gate to $|x_1\rangle$

$$|x_3\rangle \otimes |x_2\rangle \otimes \frac{1}{\sqrt{2}}\left[|0\rangle + \exp\left(\frac{2\pi i}{2} x_1\right)|1\rangle\right]$$

Next, we apply a $UROT_2$ gate on $|x_1\rangle$ controlled by $|x_2\rangle$

$$|x_3\rangle \otimes |x_2\rangle \otimes \frac{1}{\sqrt{2}}\left[|0\rangle + \exp\left(\frac{2\pi i}{2} x_1 + \frac{2\pi i}{2^2} x_2\right)|1\rangle\right]$$

And we apply a $UROT_3$ gate also to $|1\rangle$ controlled by $|x_3\rangle$

$$|x_3\rangle \otimes |x_2\rangle \otimes \frac{1}{\sqrt{2}}\left[|0\rangle + \exp\left(\frac{2\pi i}{2} x_1 + \frac{2\pi i}{2^2} x_2 + \frac{2\pi i}{2^3} x_3\right)|1\rangle\right]$$

Now we apply a H gate to $|x_2\rangle$

$$|x_3\rangle \otimes \frac{1}{\sqrt{2}}\left[|0\rangle + \exp\left(\frac{2\pi i}{2} x_2\right)|1\rangle\right] \otimes \frac{1}{\sqrt{2}}\left[|0\rangle + \exp\left(\frac{2\pi i}{2^3} x_3 + \frac{2\pi i}{2^2} x_2 + \frac{2\pi i}{2} x_1\right)|1\rangle\right]$$

Then a $UROT_2$ gate to $|x_2\rangle$ controlled by $|x_3\rangle$

$$|x_3\rangle \otimes \frac{1}{\sqrt{2}}\left[|0\rangle + \exp\left(\frac{2\pi i}{2^2} x_3 + \frac{2\pi i}{2} x_2\right)|1\rangle\right] \otimes \frac{1}{\sqrt{2}}\left[|0\rangle + \exp\left(\frac{2\pi i}{2^3} x_3 + \frac{2\pi i}{2^2} x_2 + \frac{2\pi i}{2} x_1\right)|1\rangle\right]$$

Finally, we apply a H gate to $|x_3\rangle$

$$\frac{1}{\sqrt{2}}\left[|0\rangle + \exp\left(\frac{2\pi i}{2} x_3\right)|1\rangle\right] \otimes \frac{1}{\sqrt{2}}\left[|0\rangle + \exp\left(\frac{2\pi i}{2^2} x_3 + \frac{2\pi i}{2} x_2\right)|1\rangle\right] \otimes \frac{1}{\sqrt{2}}\left[|0\rangle + \exp\left(\frac{2\pi i}{2^3} x_3 + \frac{2\pi i}{2^2} x_2 + \frac{2\pi i}{2} x_1\right)|1\rangle\right]$$

Keep in mind the reverse of the output state relative to the desired QFT. Therefore, we must reverse the order of the qubits (in this case swap y_1 and y_3).

This example demonstrates a very useful form of the QFT for $N = 2^n$. Note that only the last qubit depends on the values of all the other input qubits and each further bit depends less and less on the input qubits. This becomes important in physical implementations of the QFT, where nearest-neighbor couplings are easier to achieve than distant couplings between qubits.

Additionally, as the QFT becomes large, an increasing amount of time is spent doing increasingly slight rotations. It turns out that we can ignore rotations below a certain threshold and still get decent results, this is known as the approximate QFT. This is also important in physical implementations as reducing the number of operations can greatly reduce decoherence and potential gate errors. Check 8. on the link for implementation of QFT in Qiskit.