3) End of lecture 11: Circuit and complexity of the QFT.

The QFT is defined by its action on basis vectors
\[ |10\rangle, |11\rangle, \ldots, |1N-1\rangle \] of an \(N\)-dimensional Hilbert space \( \mathcal{H} = \text{Span} \{ |10\rangle, \ldots, |1N-1\rangle \} \):

\[
\text{QFT} |x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \exp \left( \frac{2\pi i x y}{N} \right) |y\rangle.
\]

a) Note that in the special case \(N = 2\), the QFT becomes the usual Hadamard gate:

\[
\text{(QFT)}_{N=2} |x\rangle = \frac{1}{\sqrt{2}} \sum_{y=0}^{1} \exp \left( \frac{2\pi i x y}{2} \right) |y\rangle = \frac{1}{\sqrt{2}} \left( |0\rangle + (-1)^x |1\rangle \right)
\]

Of course the circuit in this case is simply

\[ |x\rangle \xrightarrow{H} |\text{QFT} x\rangle \]

b) Let examine the case \(N = 4\), i.e., \( \mathcal{H} = \text{Span} \{ |10\rangle, |11\rangle, |12\rangle, |13\rangle \} \).

\[
\text{QFT} |x\rangle = \frac{1}{\sqrt{4}} \left( e^{\frac{2\pi i x_0}{4}} |10\rangle + e^{\frac{2\pi i x_1}{4}} |11\rangle + e^{\frac{2\pi i x_2}{4}} |12\rangle + e^{\frac{2\pi i x_3}{4}} |13\rangle \right).
\]

We can represent the \( |12\rangle \) in binary notation:
\[ \begin{align*}
10 & = 100 \quad ; \quad 11 = 101 \quad ; \quad 12 = 110 \quad ; \quad 13 = 111. \\
\text{Then,} \\
\text{QFT}\{x\} &= \frac{1}{\sqrt{4}} \left( 100 + e^{i\frac{\pi}{2}x} \right. \left. 101 + e^{i\pi x} \right. \\
&\quad \left. 110 + e^{i\frac{3\pi}{2} x} \right) \\
&= \frac{1}{\sqrt{2}} (10 + e^{i\pi x}) \otimes (10 + e^{i\pi x}).
\end{align*} \]

Now we can represent \( x \) also in binary notation:

\[ x = 2x_1 + x_0, \] \( x_0, x_1 \in \{0, 1\}. \]

\[ \{0, 1; 2; 3\} \quad \{00, 01, 10, 11\}. \]

\[ \begin{align*}
\frac{i\pi x}{2} & = e^{i\pi x_1} e^{i\pi x_0}, \\
& = e^{i\pi x_0}, \\
& \quad e^{i\pi x_1}, \\
& \quad e^{i\pi x_0}.
\end{align*} \]

Thus,

\[ \text{QFT}\{x\} = \frac{1}{\sqrt{2}} \left( 10 + (-1)^{x_0} 12 \right) \otimes \left( 10 + (-1)^{x_1} e^{i\frac{\pi}{2} x_0} 12 \right). \]

\[ \text{QFT}\{x, x_0\}. \]

A circuit realizing this operation is:

\[ \begin{array}{c}
10 \xrightarrow{\text{SWAP}} 11 \\
10 \xrightarrow{\text{H}} 11 \\
11 \xrightarrow{\text{S}} 11 \\
11 \xrightarrow{\text{S}} 10 \\
10 \xrightarrow{\text{S}} 11 \\
11 \xrightarrow{\text{S}} 10 \\
10 \xrightarrow{\text{S}} 11 \\
\end{array} \]

\[ \text{QFT}\{x, x_0\}. \]
where the SWAP operation is realized as follows:

\[
\begin{array}{cccc}
|1x_1\rangle & |1x_1\rangle & |1x_0\rangle & |1x_0\rangle \\
|1x_0\rangle & |1x_1 + x_o\rangle & |1x_1 + x_o\rangle & |1x_1 + x_o\rangle
\end{array}
\]

Once the SWAP operation is performed on \(|1x_1, x_0\rangle\) we act with \(H\) on the second q-bit:

\[
H \text{ SWAP } |1x_1, x_0\rangle = H |1x_0, x_1\rangle = |1x_0\rangle \cdot \frac{1}{\sqrt{2}} (|0\rangle + (-1)^{x_1} |1\rangle).
\]

Then we act with a controlled \(S = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2} \end{pmatrix}\) gate:

\[
\text{CS } H \text{ SWAP } |1x_0\rangle = \text{CS } |1x_0\rangle \cdot \frac{1}{\sqrt{2}} (|0\rangle + (-1)^{x_1} |1\rangle).
\]

Note that here the CS has two control bits: the first and the second. In fact the matrix for CS (a two bit gate) is

\[
\text{CS} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\pi/2} \end{pmatrix}
\]

so that \(e^{i\pi/4}\) acts only on \(|1\rangle\).

Another way to express CS is

\[
\text{CS} = |10\rangle \langle 01| \otimes \mathbb{I} + |11\rangle \langle 11| \otimes S
\]

where \(S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\).
The last Hadamard gate acts on the first bit and yields:

$$H \; CS \; H \; SWAP \ket{x_1, x_0} = H \ket{x_0} \frac{1}{\sqrt{2}} \left[ \ket{0} + (-1)^{x_1} e^{i \frac{\pi}{2} x_0} \ket{1} \right]$$

$$= \frac{1}{\sqrt{2}} \left( \ket{0} + (-1)^{x_0} \ket{1} \right) \otimes \frac{1}{\sqrt{2}} \left( \ket{0} + (-1)^{x_1} e^{i \frac{\pi}{2} x_0} \ket{1} \right)$$

So we have the decomposition (for \( N = 4 \))

$$QFT = (H \otimes I) (CS) (I \otimes H) (SWAP)$$

c) This decomposition and the corresponding circuit can easily be generalized to any \( N = 2^m \).

**Lemma:** Let \( x \in \{0, 1, \ldots, N-1\} \) with \( N = 2^m \).

$$QFT \ket{x} = \frac{1}{\sqrt{2^m}} \sum_{l=1}^{2^m} e^{i \frac{\pi}{2^m} x} \ket{l}$$

**Proof:** Use the binary representation for \( \ket{x} = \ket{y_m-1 \ldots y_0} \)

where \( y = 2^{m-1} y_{m-1} + 2^{m-2} y_{m-2} + \ldots + 2^0 y_0 \)

and the \( \text{bits } y_0 \in \{0, 1\} \). Take the definition of \( QFT \ket{x} \)

and split the sum over \( y \in \{0, \ldots, N-1\} \) into a sum over even terms and a sum over odd terms.
\[ q_{FT} |x\rangle = \frac{1}{\sqrt{2^m}} \sum_{y \text{ even}} e^{2\pi i \frac{x y}{2^m}} |y\rangle + \sum_{y \text{ odd}} e^{2\pi i \frac{x y}{2^m}} |y\rangle \]

\[ = \sum_{y' = 0}^{2^m - 1} e^{2\pi i \frac{y'}{2^m}} |y'_{m-1} \ldots y'_1 0\rangle + \sum_{y' = 0}^{2^m - 1} e^{2\pi i \frac{y'_{m-1}}{2^m}} |y'_{m-1} \ldots y'_1 1\rangle \]

where we used the facts that if \( y = 2y' \) and \( y = 2^{m-1} y_{m-1} + \ldots + 2^1 y_1 + 2^0 y_0 \), then
\[
y' = 2^{m-2} y_{m-1} + \ldots + 2^0 y_1 \quad \text{and} \quad y_0 = 0.
\]

if \( y = 2y' + 1 \) and
\[
y = 2^{m-1} y_{m-1} + \ldots + 2^1 y_1 + 2^0 y_0 \quad \text{then}
\]
\[
y' = 2^{m-2} y_{m-1} + \ldots + 2^1 y_2 \quad \text{and} \quad y_0 = 1.
\]

For this decomposition we conclude that
\[
q_{FT} |x\rangle = \left( \sum_{y = 0}^{2^m - 1} e^{2\pi i \frac{y x}{2^m}} |y\rangle \right) \otimes \frac{1}{\sqrt{2}} (10\rangle + e^{2\pi i \frac{x}{2^{m-1}}} 11\rangle)
\]

By repeating the same decomposition again and again on the first parenthesis we obtain the result of the Lemma.
The $l$-th term in the product (Lemma) is:

$$ (|0\rangle + e^{i\frac{\pi}{2^{l-1}}x} |1\rangle). $$

Let us look at the phase factor more closely. The binary expansion of $X$ is:

$$ X = 2^0 \cdot x_0 + \cdots + 2^2 \cdot x_2 + 2^3 \cdot x_1 + 2^4 \cdot x_0. $$

and this implies that

$$ e^{i\frac{\pi}{2^{l-1}}x} = (-1)^k \cdot e^{i\frac{\pi}{2}x_{2^l-1}} \cdot e^{i\frac{\pi}{4}x_{2^{l-2}}} \cdot e^{i\frac{\pi}{8}x_{2^{l-3}}} \cdot \cdots \cdot e^{i\frac{\pi}{2^{l-1}}x_0}. $$

So to obtain the $l$-th term in the product we may use the operations (Hadamard and double control phases).

The output is:

$$ |x_0\rangle \otimes |x_1\rangle \cdots \otimes |x_{2^l-2}\rangle \cdot \frac{1}{\sqrt{2}} (|0\rangle + e^{i\frac{\pi}{2^{l-1}}x} |1\rangle). $$
Remark: If one wants to work to finite accuracy
(which is the case in "practice") one can neglect the
phase factor $\frac{\pi}{2k} \frac{1}{\epsilon} < \epsilon$ (a first accuracy).

Then the nb of steps becomes $O(M) = O(\epsilon M N)$.

[ The coefficient will be $\epsilon$-dependent.]