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

The QFT is defined by its action on basis vectors $\{ |0\rangle, |1\rangle, \dots |N-1\rangle \}$ of an N-dimensional Hilbert space $\mathcal{H} = \text{span}\{ |0\rangle \dots |N-1\rangle \}$:

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

a) <u>Note that in the special case $N = 2$</u> the QFT becomes the usual Hadamard gate:

$$(QFT)_{N=2} |x\rangle = \frac{1}{\sqrt{2}} \sum_{y=0}^{1} \exp(\pi i\, xy)\ |y\rangle = \frac{1}{\sqrt{2}} \sum_{y=0}^{1} (-1)^{xy} |y\rangle$$

$$= \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^x |1\rangle \right)$$

Of course the circuit in this case is simply

$$|x\rangle \rightarrow \boxed{H} \rightarrow \quad H|x\rangle$$

b) <u>Let examine the case $N = 4$</u> i.e. $\mathcal{H} = \text{span}\{ |0\rangle, |1\rangle, |2\rangle, |3\rangle \}$.

$$QFT\, |x\rangle = \frac{1}{\sqrt{4}} \left\{ e^{2\pi i \frac{x \cdot 0}{4}} |0\rangle + e^{2\pi i \frac{x \cdot 1}{4}} |1\rangle + e^{2\pi i \frac{x \cdot 2}{4}} |2\rangle + e^{2\pi i \frac{x \cdot 3}{4}} |3\rangle \right\} .$$

We can represent the $|y\rangle$ in binary notation;

$$|0\rangle = |00\rangle \quad ; \quad |1\rangle = |01\rangle \quad ; \quad |2\rangle = |10\rangle \; ; \; |3\rangle = |11\rangle .$$

Then

$$QFT\,|x\rangle = \frac{1}{\sqrt{4}}\left(|00\rangle + e^{i\frac{\pi}{2}x}|01\rangle + e^{i\pi x}|10\rangle + e^{3i\frac{\pi}{2}x}|11\rangle \right)$$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\pi x}|1\rangle\right) \otimes \left(|0\rangle + e^{i\frac{\pi}{2}x}|1\rangle\right).$$

Now we can represent x also in binary notation:

$$\underset{\{0;1;2;3\}}{\overset{}{x}} \in \quad = \underbrace{2\cdot x_1 + x_0}_{\{00;\ 01;\ 10;\ 11\}} \quad ; \quad x_0, x_1 \in \{0,1\}.$$

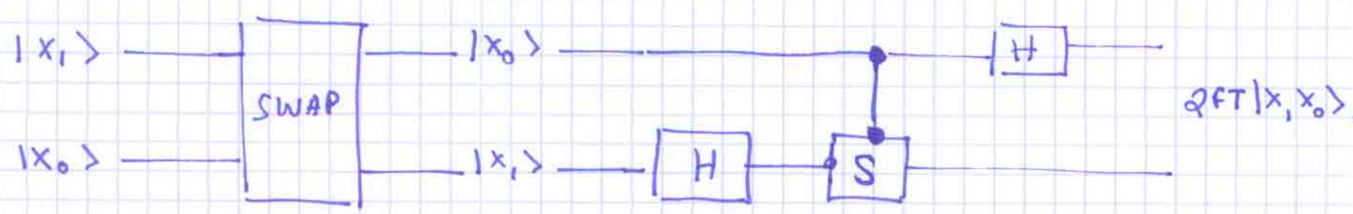
$$\Rightarrow \quad e^{i\pi x} = e^{2\pi i x_1} e^{i\pi x_0} = (-1)^{x_0}$$

$$e^{i\frac{\pi}{2}x} = e^{i\pi x_1} e^{i\frac{\pi}{2}x_0} = (-1)^{x_1} e^{i\frac{\pi}{2}x_0}.$$

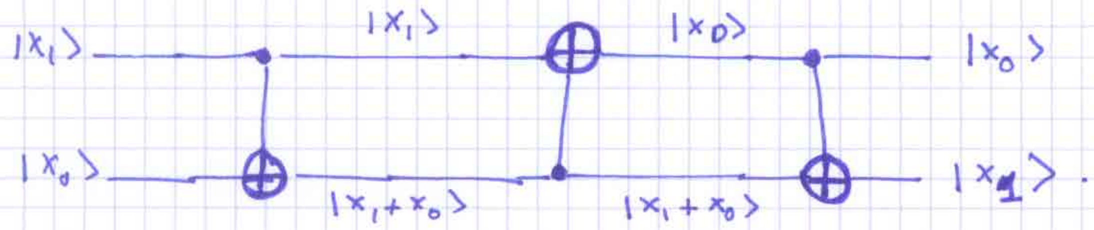
Thus

$$QFT\,\underbrace{|x\rangle}_{QFT\,|x_1 x_0\rangle} = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{x_0}|1\rangle\right) \otimes \left(|0\rangle + (-1)^{x_1} e^{i\frac{\pi}{2}x_0}|1\rangle\right)$$

A circuit realizing this operation is:



where the SWAP operation is realized as follows:



Once the SWAP operation is performed on $|x_1 x_0\rangle$ we act with H on the second qbit:

$$H\ \text{SWAP}\ |x_1 x_0\rangle = H\ |x_0 x_1\rangle = |x_0\rangle \cdot \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{x_1}|1\rangle\right).$$

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

$$\begin{aligned} CS\ H\ \text{SWAP}|x_1 x_0\rangle &= CS\ |x_0\rangle \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{x_1}|1\rangle\right) \\ &= |x_0\rangle \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{x_1} e^{i\frac{\pi}{2}x_0}|1\rangle\right). \end{aligned}$$

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

$$CS = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\frac{\pi}{2}} \end{pmatrix}$$

so that $e^{i\pi/2}$ acts only on $|11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$. Another way to express CS is

$$CS = \underbrace{|0\rangle\langle 0|}_{\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}} \otimes \underbrace{\mathbb{1}}_{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}} + \underbrace{|1\rangle\langle 1|}_{\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}} \otimes \underbrace{S}_{\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2} \end{pmatrix}}.$$

The last Hadamard gate acts on the first bit and yields:

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

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

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

$$QFT = (H \otimes \mathbb{1})\,(CS)\,(\mathbb{1} \otimes H)\,(SWAP)$$

c) <u>This decomposition and the corresponding circuit can easily be generalized to any $N = 2^M$.</u>

Lemma: Let $x \in \{0, 1 \dots N-1\}$ with $N = 2^M$.

$$QFT\,|x\rangle = \prod_{\ell=1}^{M} \left(|0\rangle + e^{\frac{i\pi}{2^{\ell-1}}x}\,|1\rangle\right).$$

Proof: Use the binary representation for $|y\rangle = |y_{M-1} \dots y_0\rangle$

where $y = 2^{M-1} y_{M-1} + 2^{M-2} y_{M-2} + \dots + 2^0 \cdot y_0$

and the bits $y_i \in \{0, 1\}$. Take the definition of $QFT\,|x\rangle$ and split the sum over $y \in \{0 \dots N-1\}$ into a sum over even terms and a sum over odd terms:

$$QFT\,|x\rangle = \frac{1}{2^{m/2}}\sum_{y \text{ even}} e^{2\pi i \frac{xy}{2^m}}|y\rangle + \sum_{y \text{ odd}} e^{2\pi i \frac{xy}{2^m}}|y\rangle$$

$$= \sum_{y'=0}^{2^{m-1}-1} e^{2\pi i \frac{x\, 2y'}{2^m}}|y_{m-1}\cdots y_1\, 0\rangle + \sum_{y'=0}^{2^{m-1}-1} e^{2\pi i x \frac{2y'+1}{2^m}}|y_{m-1}\cdots y_1\, 1\rangle$$

where we used the facts that if $y = 2y'$ and

$$y = 2^{m-1} y_{m-1} + \cdots + 2^1 \cdot y_1 + 2^0 y_0 \quad \text{then}$$

$$y' = 2^{m-2} y_{m-1} + \cdots + 2^0 \cdot y_1 \quad \text{and } y_0 = 0 .$$

if $y = 2y'+1$ and

$$y = 2^{m-1} y_{m-1} + \cdots + 2^1 \cdot y_1 + 2^0 y_0 \quad \text{then}$$

$$y' = 2^{m-2} y_{m-1} + \cdots + 2^0 \cdot y_1 \quad \text{and } y_0 = 1 .$$

For this decomposition we conclude that

$$QFT\,|x\rangle = \left(\frac{1}{2^{(m-1)/2}} \sum_{y=0}^{2^{m-1}-1} e^{\frac{2\pi i\, xy}{2^{m-1}}}|y\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{\frac{\pi i\, x}{2^{m-1}}}|1\rangle\right)$$

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:

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

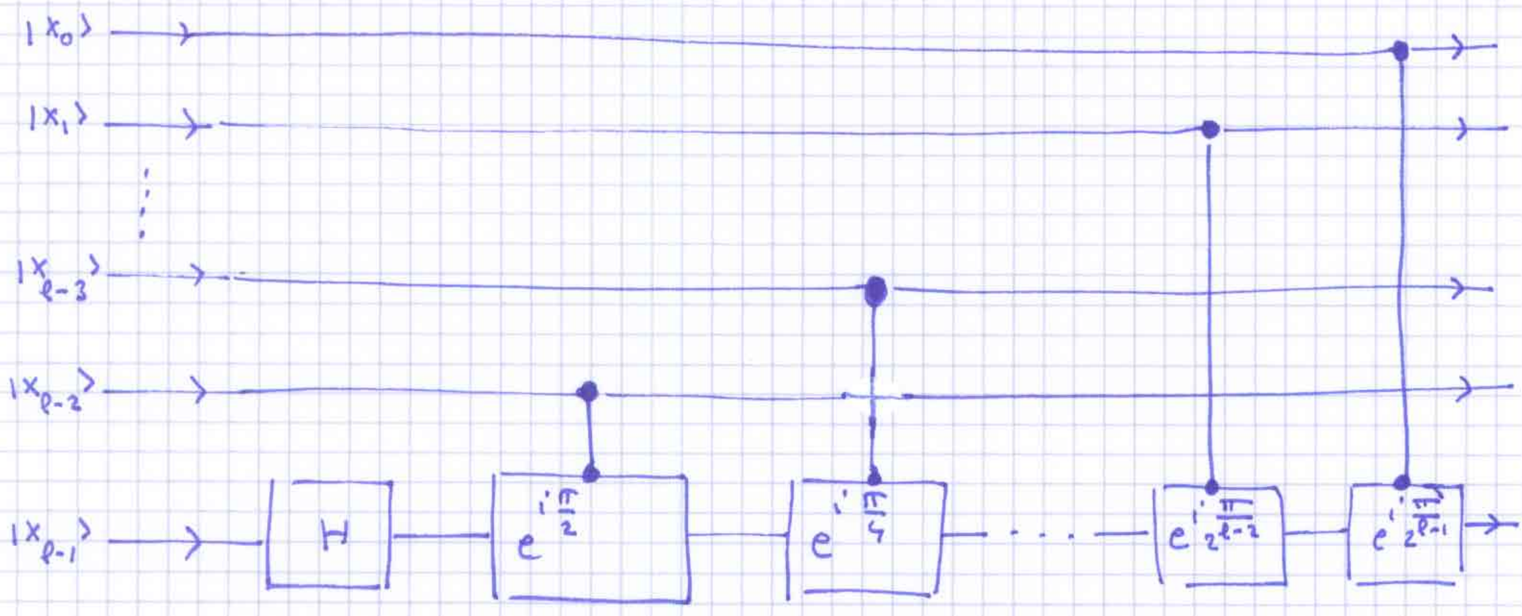
Let us look at the phase factor more closely. The binary expansion of X is:

$$X = 2^{m-1} \cdot x_{m-1} + \ldots + 2^2 \cdot x_2 + 2^1 \cdot x_1 + 2^0 \cdot x_0 .$$

and this implies that

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

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

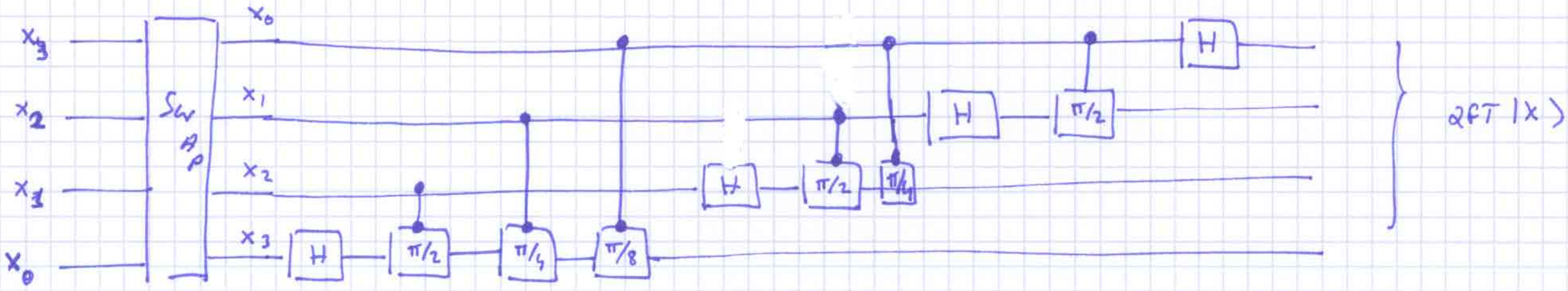


The output is $|x_0\rangle |x_1\rangle \ldots |x_{l-2}\rangle \cdot \frac{1}{\sqrt{2}} \left(|0\rangle + e^{i\frac{\pi}{2^{l-1}}x} |1\rangle \right).$

From these observations we deduce the full circuit for the QFT (Shor 1994)

$$\begin{cases} \text{input} & |x\rangle = |x_{m-1} \dots x_0\rangle \\ \text{output} & QFT\,|x\rangle = \dfrac{1}{2^{m/2}} \displaystyle\sum_{y=0}^{2^m-1} e^{2\pi i \frac{xy}{2^m}} |y\rangle . \end{cases}$$

For $m = 4$ qbits ($N = 2^4 = 16$) the circuit is (a 16×16 matrix):



To perform the SWAP here we can first SWAP x_0 & x_3 and then x_1 & x_2. In any case the SWAP operation requires $O(3m)$ CNOT gates and the rest of the QFT requires:

$$\underbrace{m}_{\text{H \& phase gates}} + \underbrace{(m-1)}_{\text{H \& phase gates}} + \dots \underbrace{1}_{H.} = \frac{m(m-1)}{2} \text{ gates}.$$

$\boxed{\text{So the overall size of the QFT circuit is } O(m^2) = O((\ln N)^2).}$

Remark : If one want to work to finite accuracy (which is the case in "practice") one can neglect the phase gates $\frac{\pi}{2^k}$ for $\frac{1}{2^k} < \varepsilon$ (ε a fixed accuracy).

Then the nb of gates becomes $O(n) = O(\ln N)$.

[the coefficient will be ε-dependent].