Quantum Computation
Revisiting the quantum Fourier transform

Luís Soares Barbosa & Renato Neves

Universidade do Minho

HASLab HIGH-ASSURANCE SOFTWARE LABORATORY

INL INTERNATIONAL IBERIAN NANOTECHNOLOGY LABORATORY

MSc Physics Engineering

Universidade do Minho, 2023-24

Recap

The previous lecture discussed an algorithm to extract the phase factor $w \in [0, 1[$ from a generic n-qubit quantum state. Writing w as $\frac{x}{2^n}$, for x an integer representable in n qubits, the estimation process was described by

$$\frac{1}{\sqrt{2^n}} \sum_{y \in 2^n} e^{2\pi i (\frac{x}{2^n}) y} |y\rangle \quad \rightsquigarrow \quad |x\rangle$$

Its inverse is QFT, the quantum Fourier transform, a most useful routine in Quantum Computation.

Let us revisit its construction in a systematic way.

The quantum Fourier transform

Essentially, the QFT performs a change-of-basis operation which encodes information of computational basis states in local phases.

For 1 qubit state this is exactly what the Hadamard gate accomplishes:

$$H|0\rangle = \frac{1}{\sqrt{2}}\big(\,|0\rangle + 1\,|1\rangle\,\big) \qquad H|1\rangle = \frac{1}{\sqrt{2}}\big(\,|0\rangle + (-1)\,|1\rangle\,\big)$$

QFT: 1 qubit

Thus, $QFT_1 = H$:

$$QFT_1 |0\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + 1 |1\rangle \big) \qquad QFT_1 |1\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + (-1) |1\rangle \big)$$

Operation H^{-1} allows to extract information encoded in local phases

↓ $= H$

Exercise

Let $\omega_1 = e^{i2\pi\frac{1}{2}}$. Show that $QFT_1 |x\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + \omega_1^{1\cdot x} |1\rangle \Big)$

↓ angle of π radians

QFT: 2 qubits

Let $\omega_2 = e^{i2\pi \frac{1}{4}}$

$$
\begin{aligned}
QFT_2 |00\rangle &= \tfrac{1}{\sqrt{2}}\big(|0\rangle + \omega_2^{2\cdot 0} |1\rangle \big) \otimes \tfrac{1}{\sqrt{2}}\big(|0\rangle + \omega_2^{1\cdot 0} |1\rangle \big) \\
QFT_2 |01\rangle &= \tfrac{1}{\sqrt{2}}\big(|0\rangle + \omega_2^{2\cdot 1} |1\rangle \big) \otimes \tfrac{1}{\sqrt{2}}\big(|0\rangle + \omega_2^{1\cdot 1} |1\rangle \big) \\
QFT_2 |10\rangle &= \tfrac{1}{\sqrt{2}}\big(|0\rangle + \omega_2^{2\cdot 2} |1\rangle \big) \otimes \tfrac{1}{\sqrt{2}}\big(|0\rangle + \omega_2^{1\cdot 2} |1\rangle \big) \\
QFT_2 |11\rangle &= \tfrac{1}{\sqrt{2}}\big(|0\rangle + \omega_2^{2\cdot 3} |1\rangle \big) \otimes \tfrac{1}{\sqrt{2}}\big(|0\rangle + \omega_2^{1\cdot 3} |1\rangle \big)
\end{aligned}
$$

Exercise

Compute the phase coeficients in the expressions above and use Bloch sphere to study $QFT_2 |x\rangle$.

QFT: 2 qubits

Hint

$$
\begin{aligned}
\omega_2^{2.0} &= 1 & \qquad \omega_2^{1.0} &= 1 \\
\omega_2^{2.1} &= -1 & \qquad \omega_2^{1.1} &= e^{i\frac{\pi}{2}} \\
\omega_2^{2.2} &= 1 & \qquad \omega_2^{1.2} &= -1 \\
\omega_2^{2.3} &= -1 & \qquad \omega_2^{1.3} &= e^{i\frac{3}{2}\pi}
\end{aligned}
$$

Note that

- information on $|x\rangle$ previously encoded by vectors pointing to the poles becomes encoded by vectors in the xz-plane
- for every ω_2-rotation on the second qubit there are *two* such rotations on the first qubit

QFT: 2 qubits

In order to derive a circuit for QFT_2, compute

$$
\begin{aligned}
QFT_2 |x\rangle &= \frac{1}{\sqrt{2}}\big(|0\rangle + \omega_2^{2\cdot x} |1\rangle \big) \otimes \frac{1}{\sqrt{2}}\big(|0\rangle + \omega_2^{1\cdot x} |1\rangle \big) \\
&= \frac{1}{\sqrt{2}}\big(|0\rangle + \omega_2^{2(2x_1+x_2)} |1\rangle \big) \otimes \frac{1}{\sqrt{2}}\big(|0\rangle + \omega_2^{2x_1+x_2} |1\rangle \big) \\
&= \frac{1}{\sqrt{2}}\big(|0\rangle + \omega_2^{4x_1+2x_2} |1\rangle \big) \otimes \frac{1}{\sqrt{2}}\big(|0\rangle + \omega_2^{2x_1+x_2} |1\rangle \big) \\
&= \frac{1}{\sqrt{2}}\big(|0\rangle + \omega_2^{4x_1}\omega_2^{2x_2} |1\rangle \big) \otimes \frac{1}{\sqrt{2}}\big(|0\rangle + \omega_2^{2x_1}\omega_2^{x_2} |1\rangle \big) \\
&= \frac{1}{\sqrt{2}}\big(|0\rangle + \omega_2^{2x_2} |1\rangle \big) \otimes \frac{1}{\sqrt{2}}\big(|0\rangle + \omega_2^{2x_1}\omega_2^{x_2} |1\rangle \big) \\
&= \underbrace{\frac{1}{\sqrt{2}}\big(|0\rangle + (-1)^{x_2} |1\rangle \big)}_{H|x2\rangle} \otimes \underbrace{\frac{1}{\sqrt{2}}\big(|0\rangle + (-1)^{x_1}\omega_2^{x_2} |1\rangle \big)}_{\text{some controlled rot. on } H|x1\rangle}
\end{aligned}
$$

QFT: 2 qubits

Define

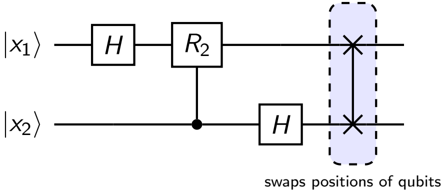
$$R_2 |0\rangle = |0\rangle |; \quad \text{and} \quad R_2 |1\rangle = \omega_2 |1\rangle$$

Intuitively, R_2 rotates a vector in the xz-plane $\frac{\pi}{2}$ radians

It yields a controlled-R_2 operation by $|x\rangle |0\rangle \mapsto |x\rangle |0\rangle$ and $|x\rangle |1\rangle \mapsto R_2 |x\rangle |1\rangle$. or, equivalently,

$$|0\rangle |x_2\rangle \mapsto |0\rangle |x_2\rangle \qquad |1\rangle |x_2\rangle \mapsto \omega_2^{x_2} |1\rangle |x_2\rangle$$

Putting all pieces together to derive the QFT circuit for 2 qubits:



QFT: 3 qubits

$$QFT_3 |x\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + \omega_3^{4\cdot x} |1\rangle \big) \otimes \big(|0\rangle + \omega_3^{2\cdot x} |1\rangle \big) \otimes \big(|0\rangle + \omega_3^{1\cdot x} |1\rangle \big)$$

for $\omega_n = e^{i2\pi \cdot \frac{1}{2^n}}$.

N.B. In the sequel the normalisation factor $\frac{1}{\sqrt{2}}$ will be dropped in each state to make notation easier on the eyes

QFT: 3 qubits

In order to derive a circuit for QFT_3, we observe

$$\omega_n^2 = \omega_{n-1} \text{ and thus } \omega_n^{2^{n-1}} = e^{i\pi} = -1$$

and recall that a binary number $x_1 \dots x_n$ represents the natural number $2^{n-1} \cdot x_1 + \dots + 2^0 \cdot x_n$.

Thus, compute QFT_3 as follows:

QFT: 3 Qubits

$$
\begin{aligned}
&QFT_3 \, |x\rangle \\
&= \big(\, |0\rangle + \omega_3^{4\cdot x} \, |1\rangle \,\big) \otimes \big(\, |0\rangle + \omega_3^{2\cdot x} \, |1\rangle \,\big) \otimes \big(\, |0\rangle + \omega_3^{1\cdot x} \, |1\rangle \,\big) \\
&= \big(\, |0\rangle + (-1)^{x} \, |1\rangle \,\big) \otimes \big(\, |0\rangle + \omega_3^{2\cdot x} \, |1\rangle \,\big) \otimes \big(\, |0\rangle + \omega_3^{1\cdot x} \, |1\rangle \,\big) \\
&= \big(\, |0\rangle + (-1)^{x_3} \, |1\rangle \,\big) \otimes \big(\, |0\rangle + \omega_3^{2\cdot x} \, |1\rangle \,\big) \otimes \big(\, |0\rangle + \omega_3^{1\cdot x} \, |1\rangle \,\big) \\
&= H \, |x_3\rangle \otimes \big(\, |0\rangle + \omega_3^{2\cdot(4x_1+2x_2+x_3)} \, |1\rangle \,\big) \otimes \big(\, |0\rangle + \omega_3^{1\cdot x} \, |1\rangle \,\big) \\
&= H \, |x_3\rangle \otimes \big(\, |0\rangle + \omega_3^{2\cdot(4x_1+2x_2)} \omega_3^{2\cdot x_3} \, |1\rangle \,\big) \otimes \big(\, |0\rangle + \omega_3^{1\cdot x} \, |1\rangle \,\big) \\
&= H \, |x_3\rangle \otimes \big(\, |0\rangle + \omega_2^{2\cdot(2x_1+x_2)} \omega_2^{x_3} \, |1\rangle \,\big) \otimes \big(\, |0\rangle + \omega_3^{4x_1+2x_2+x_3} \, |1\rangle \,\big) \\
&= H \, |x_3\rangle \otimes \big(\, |0\rangle + \omega_2^{2\cdot(2x_1+x_2)} \omega_2^{x_3} \, |1\rangle \,\big) \otimes \big(\, |0\rangle + \omega_3^{4x_1+2x_2} \omega_3^{x_3} \, |1\rangle \,\big) \\
&= H \, |x_3\rangle \otimes \big(\, |0\rangle + \omega_2^{2\cdot(2x_1+x_2)} \omega_2^{x_3} \, |1\rangle \,\big) \otimes \big(\, |0\rangle + \omega_3^{2\cdot(2x_1+x_2)} \omega_3^{x_3} \, |1\rangle \,\big) \\
&= H \, |x_3\rangle \otimes \underbrace{\big(\, |0\rangle + \omega_2^{2\cdot(2x_1+x_2)} \omega_2^{x_3} \, |1\rangle \,\big) \otimes \big(\, |0\rangle + \omega_2^{2x_1+x_2} \omega_3^{x_3} \, |1\rangle \,\big)}_{\text{some controlled-rotations on } QFT_2 |x_1 x_2\rangle}
\end{aligned}
$$

QFT: 3 qubits

Take $R_3 |0\rangle = |0\rangle$ and $R_3 |1\rangle = \omega_3 |1\rangle$. Intuitively, R_3 rotates a vector in the *xz*-plane 'one 2^3-th of the unit circle'.
It yields a controlled-R_3 operation defined by $|x\rangle |0\rangle \mapsto |x\rangle |0\rangle$ and $|x\rangle |1\rangle \mapsto R_3 |x\rangle |1\rangle$. Equivalently

$$|0\rangle |y\rangle \mapsto |0\rangle |y\rangle \text{ and } |1\rangle |y\rangle \mapsto \omega_3^y |1\rangle |y\rangle$$

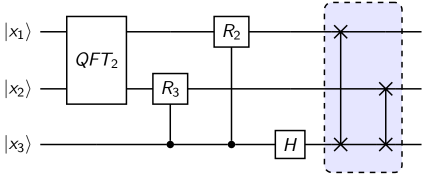
Putting all pieces together we derive the QFT circuit for 3 qubits

QFT: 3 qubits

Take $R_3 |0\rangle = |0\rangle$ and $R_3 |1\rangle = \omega_3 |1\rangle$. Intuitively, R_3 rotates a vector in the xz-plane 'one 2^3-th of the unit circle'.
It yields a controlled-R_3 operation defined by $|x\rangle |0\rangle \mapsto |x\rangle |0\rangle$ and $|x\rangle |1\rangle \mapsto R_3 |x\rangle |1\rangle$. Equivalently

$$|0\rangle |y\rangle \mapsto |0\rangle |y\rangle \text{ and } |1\rangle |y\rangle \mapsto \omega_3^{y} |1\rangle |y\rangle$$

Putting all pieces together we derive the QFT circuit for 3 qubits



swaps positions of qubits by doing $+1$ in base 3

QFT: n qubits

Calculation easily extends to QFT_n (*in lieu* of QFT_3) :

Let $\omega_n = e^{i2\pi \cdot \frac{1}{2^n}}$ (division of the unit circle in 2^n slices)

$$QFT_n |x\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + \omega_n^{2^{n-1} \cdot x} |1\rangle \right) \otimes \cdots \otimes \left(|0\rangle + \omega_n^{2^0 \cdot x} |1\rangle \right)$$

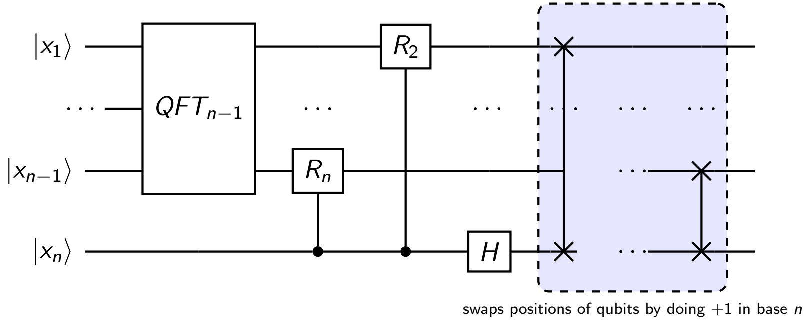
Take $R_n |0\rangle = |0\rangle$ and $R_n |1\rangle = \omega_n |1\rangle$. Intuitively, R_n rotates a vector in the xz-plane 'one 2^n-th of the unit circle'

It yields a controlled-R_n operation defined by $|x\rangle |0\rangle \mapsto |x\rangle |0\rangle$ and $|x\rangle |1\rangle \mapsto R_n |x\rangle |1\rangle$. Equivalently

$$|0\rangle |y\rangle \mapsto |0\rangle |y\rangle \text{ and } |1\rangle |y\rangle \mapsto \omega_n^y |1\rangle |y\rangle$$

QFT: n qubits

This suggests a recursive definition for the general *QFT* circuit:



An equivalent formulation of QFT

Although we have been working with

$$QFT_n |x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \omega_n^{2^{n-1}\cdot x} |1\rangle) \otimes \cdots \otimes \frac{1}{\sqrt{2}}(|0\rangle + \omega_n^{1\cdot x} |1\rangle)$$

we are already familiar with an equivalent, useful definition

$$QFT_n |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \omega_n^{x\cdot k} |k\rangle$$

Examples with $n = 1$ and $n = 2$

$$QFT_1 |x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \omega_1^{x} |1\rangle)$$
$$QFT_2 |x\rangle = \frac{1}{\sqrt{2^2}}(|00\rangle + \omega_2^{x} |01\rangle + \omega_2^{2\cdot x} |10\rangle + \omega_2^{3\cdot x} |11\rangle)$$