This Week

Lecture 11

Fourier Transformations, Regular Fourier Transform, Fourier Transform as a matrix, Quantum Fourier Transform, QUI examples, Inverse QFT

Lecture 12

Shor's Quantum Factoring algorithm, Shor's algorithm for factoring and discrete logarithm, HSP Problem

Lab 6

QFT and Shor's algorithm

1

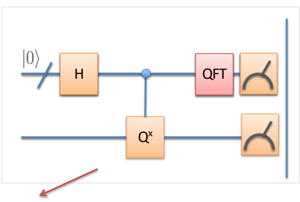
Lecture 11 overview

- Fourier Transformations
  - Phase estimation
  - Regular Fourier Transform
  - Fourier Transform as a matrix
  - Quantum Fourier Transform (QFT)
  - QUI examples
  - Inverse QFT

Reiffel, Chapter 8
Kaye, Chapter 7
Nielsen and Chuang, Chapter 5

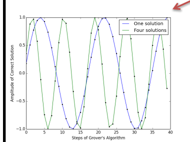
2

Last lecture: Quantum Counting



Dimension: N'

Dimension: N

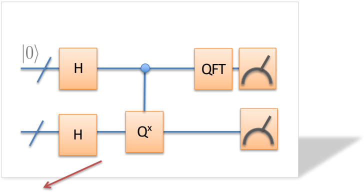


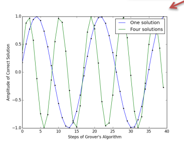
$$|\psi\rangle = \sum_x \sin(2x+1)\theta\,|x\rangle \otimes |\psi_g\rangle$$

After Fourier transforming a periodic function, we get a good approximation to frequency.

3

Last Lecture: Quantum Counting





$$|\psi\rangle = \sum_x \sin(2x+1)\theta\,|x\rangle \otimes |\psi_g\rangle$$

After **Fourier transform** of a periodic function, we get a good approximation to frequency. Example of **quantum phase estimation**.

4

PHYC90045 Introduction to Quantum Computing

Quantum Phase Estimation

5

PHYC90045 Introduction to Quantum Computing

The Problem

Consider an eigenvector $|\psi\rangle$ of a unitary matrix (an operation which you could implement on a quantum computer) U:

$$\boxed{U\,|\psi\rangle = \underbrace{\exp(2\pi i\theta)}_{\text{Eigenvalue}}\,\underbrace{|\psi\rangle}_{\text{Eigenvector}}}$$

The Quantum Phase Estimation algorithm estimates the angle θ. Notice that since U is unitary, all eigenvalues of U will be of this form.

6

The T gate

For example, consider the T gate:

$$T = \begin{bmatrix} 1 & 0 \\ 0 & \exp(i\frac{\pi}{4}) \end{bmatrix}$$

An eigenvector of the T gate is

$$\boxed{T\left|1\right\rangle = \underbrace{\exp\left(i\frac{\pi}{4}\right)}_{\text{Eigenvalue}}\underbrace{\left|1\right\rangle}_{\text{Eigenvector}}}$$

$$\boxed{U\left|\psi\right\rangle = \exp(2\pi i\theta)\left|\psi\right\rangle}$$

So in this case, we want to find:

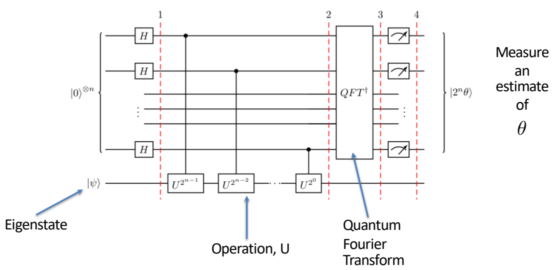
$$\theta = \frac{1}{8}$$

Quantum Phase Estimation gives a way to do this on a quantum computer.

7

PHYC90045 Introduction to Quantum Computing

Quantum Phase Estimation Circuit

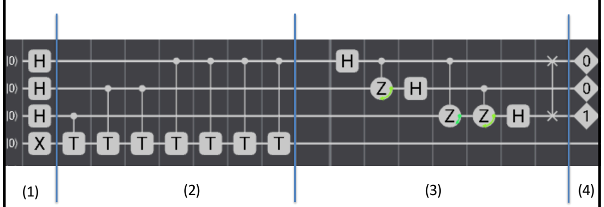


(1) Prepare equal superposition, x in the upper register x and eigenstate $|\psi\rangle$.
(2) Apply U^x to lower register
(3) Apply (inverse) Quantum Fourier Transform to the upper register
(4) Measure to obtain an estimate equal to $2^n\theta$.

8

PHYC90045 Introduction to Quantum Computing

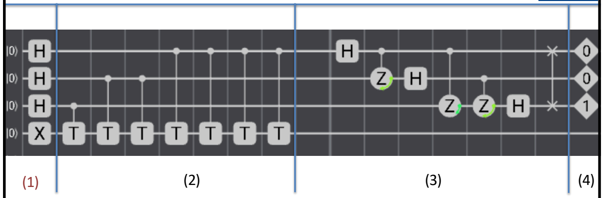
QPE Circuit in the QUI



(1) Prepare equal superposition, x and eigenstate $|\psi\rangle$.
(2) Apply U^x to lower register
(3) Apply (inverse) Quantum Fourier Transform to the x register
(4) Measure to obtain an estimate equal to $2^n\theta$.

9

Step 1: Equal Superposition



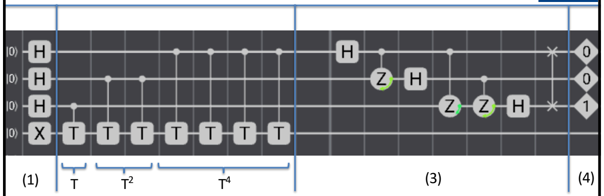
After the first step of the algorithm

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle\,|1\rangle$$

10

PHYC90045 Introduction to Quantum Computing

Step 2: Applying U^x



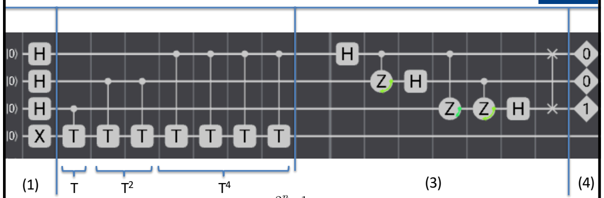
After step 2:

$$\begin{aligned}|\psi\rangle &= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle\, T^x\, |1\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \exp\left(i\frac{\pi}{4}x\right) |1\rangle\end{aligned}$$

11

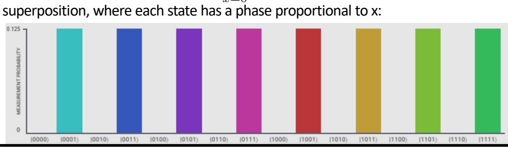
PHYC90045 Introduction to Quantum Computing

Step 2: Applying U^x



$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} \exp\left(i\frac{\pi}{4}x\right) |x\rangle\,|1\rangle$$

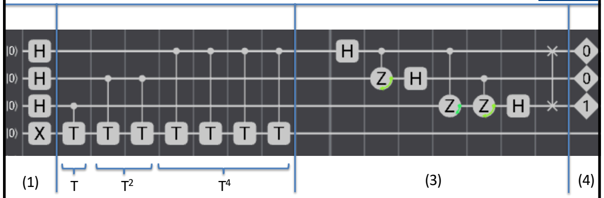
Equal superposition, where each state has a phase proportional to x:



12

PHYC90045 Introduction to Quantum Computing

Step 3: Quantum Fourier Transform



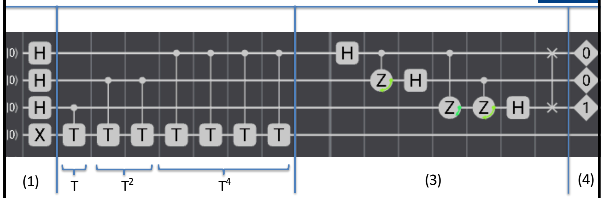
The QFT determines the period of the function, in this case it will exactly find the answer:

$$|\psi\rangle = |001\rangle\,|1\rangle$$

13

PHYC90045 Introduction to Quantum Computing

Step 4: Measure



Finally we measure an obtain the result $001_2=1$, so in this case:

$$2^n\theta = 1$$

$$\theta = \frac{1}{8}$$

As we expected!

$$\boxed{U\,|\psi\rangle = \exp(2\pi i\theta)\,|\psi\rangle}$$

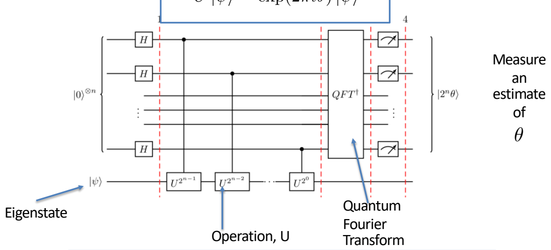
$$\boxed{T\,|1\rangle = \exp\left(i\frac{\pi}{4}\right)|1\rangle}$$

14

PHYC90045 Introduction to Quantum Computing

Quantum Phase Estimation Circuit

$$\boxed{U\,|\psi\rangle = \exp(2\pi i\theta)\,|\psi\rangle}$$



(1) Prepare equal superposition, x and eigenstate $|\psi\rangle$.
(2) Apply U^x to lower register
(3) Apply (inverse) Quantum Fourier Transform to the x register
(4) Measure to obtain an estimate equal to $2^n\theta$.

15

PHYC90045 Introduction to Quantum Computing

Quantum Fourier Transform

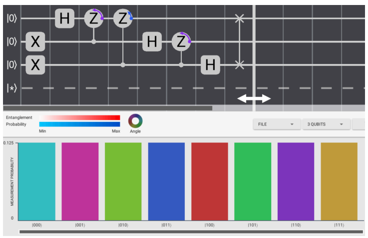
16

PHYC90045 Introduction to Quantum Computing

Fourier Transform in Quantum Computing

In QC the equivalent of the Fourier Transform – quantum Fourier Transform (QFT) – is important in a number of algorithms, most notably Shor's Factoring algorithm…

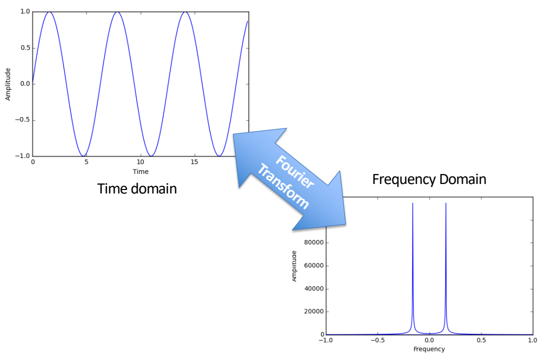
Hence, before we can cover Shor's algorithm we need to understand the QFT and how to implement it in a QC (and on the QUI)…



17

PHYC90045 Introduction to Quantum Computing

Introduction to Fourier Transform



18

Discrete Fourier Transform

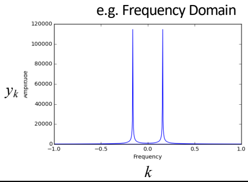
Maps a vector: $(x_0, x_1, ..., x_{N-1}) \in \mathcal{C}^N$ to a vector: $(y_0, y_1, ..., y_{N-1}) \in \mathcal{C}^N$

According to:

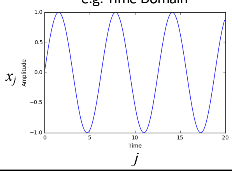
$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i jk/N}$$

NB.
i = sqrt(-1)
j and k are integers

e.g. Frequency Domain



e.g. Time Domain



19

Example: Fourier transform of periodic function

Imagine that we had a periodic function:

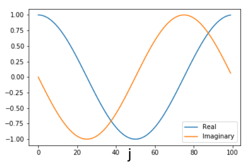
$$x_j = \exp\left(-2\pi i \frac{uj}{N}\right)$$

The frequency, u

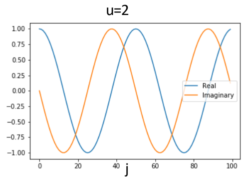
0<=j<N

Complex number, i^2=-1

u=1



u=2



20

Example: Periodic function

$$\begin{aligned} y_k &= \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \exp\left(2\pi i \frac{jk}{N}\right) \\ &= \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \exp\left(-2\pi i \frac{uj}{N}\right) \exp\left(2\pi i \frac{jk}{N}\right) \\ &= \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \exp\left(-2\pi i \frac{j(k-u)}{N}\right) \end{aligned}$$

If k=u then

$$\boxed{y_u = \sqrt{N}}$$

21

Example: Periodic function

For any other value of k,

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \exp\left(-2\pi i \frac{j(k-u)}{N}\right)$$

Recall, for a geometric series,

$$1 + r + r^2 + \ldots + r^{N-1} = \frac{1 - r^N}{1 - r}$$

Where for us,

$$r = \exp\left(-2\pi i \frac{k-u}{N}\right)$$

And therefore

$$r^N = 1$$

Except for k=u,

$$\boxed{y_k = 0}$$

22

Fourier Transform as a Matrix

We define the Fourier transformation matrix as follows:

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

$$y_k = \sum_j F_{kj} x_j \quad \text{where} \quad F_{kj} = \frac{1}{\sqrt{N}} e^{2\pi i jk/N}$$

For example:

N=2: $F = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ N=4: $F = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix}$

We will see that the quantum Fourier transform for one qubit is a Hadamard gate!

23

Quantum Fourier Transform (QFT)

The Fourier transform, written in this matrix form is unitary. It can make a valid quantum operation:

$$|\psi\rangle = \sum_{j=0}^{N-1} x_j |j\rangle \xrightarrow{\text{QFT}} |\psi'\rangle = \sum_{j=0}^{N-1} y_j |j\rangle \quad \text{with} \quad y_k = \sum_{j=0}^{N-1} F_{kj} x_j, \quad F_{kj} = \frac{1}{\sqrt{N}} e^{2\pi i jk/N}$$

On an individual basis state $|a\rangle$ (i.e. j = a only non-zero x_j) we have:

$$|a\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} y_k |k\rangle, \quad y_k = \sum_{j=0}^{N-1} F_{kj} x_j = F_{ka} = \frac{1}{\sqrt{N}} e^{2\pi i ka/N}$$

i.e. $\mathrm{QFT}\,|a\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2\pi i}{N} ka} |k\rangle$ (more familiar form relating variables a and k by Fourier transform)

Question: How can we systematically make this operation using quantum gates?

24

Product Form of QFT

The Fourier transform can be expressed in a product notation:

$$|j_1,\ldots,j_n\rangle \rightarrow \frac{|0\rangle + e^{2\pi i\, 0.j_n}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2\pi i\, 0.j_{n-1}j_n}|1\rangle}{\sqrt{2}} \otimes \ldots \otimes \frac{|0\rangle + e^{2\pi i\, 0.j_1 j_2 \ldots j_{n-1}j_n}|1\rangle}{\sqrt{2}}$$

(this is not obvious – see appendix at end)

Where the notation $0.j_1 j_2 \ldots j_n = \frac{j_1}{2} + \frac{j_2}{2^2} + \ldots + \frac{j_{n-1}}{2^{n-1}} + \frac{j_n}{2^n}$

is shorthand for writing a fraction in binary notation. That is,

$$0.1 = \frac{1}{2}$$
$$0.11 = \frac{1}{2} + \frac{1}{2^2} = \frac{3}{4}$$
$$0.101 = \frac{1}{2} + \frac{1}{2^3} = \frac{5}{8}$$

etc

25

Product Form: One Qubit

$$|j_1,\ldots,j_n\rangle \rightarrow \frac{|0\rangle + e^{2\pi i\, 0.j_n}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2\pi i\, 0.j_{n-1}j_n}|1\rangle}{\sqrt{2}} \otimes \ldots \otimes \frac{|0\rangle + e^{2\pi i\, 0.j_1 j_2 \ldots j_{n-1}j_n}|1\rangle}{\sqrt{2}}$$

For one qubit (ie. n=1, N=2): $|j_1\rangle \rightarrow \frac{|0\rangle + e^{2\pi i\, 0.j_1}|1\rangle}{\sqrt{2}}$ $\quad j_1 = 0,\ 1$

$$|0\rangle \rightarrow \frac{|0\rangle + e^{2\pi i\ 0.0}|1\rangle}{\sqrt{2}} = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

Beware binary fraction!
0.1 = 1/2 etc

$$|1\rangle \rightarrow \frac{|0\rangle + e^{2\pi i\ \underline{0.1}}|1\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{\pi i}|1\rangle}{\sqrt{2}} = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

(i.e. a Hadamard)

As before, we get:

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

26

Product Form: Two Qubits

$$|j_1,\ldots,j_n\rangle \rightarrow \frac{|0\rangle + e^{2\pi i\, 0.j_n}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2\pi i\, 0.j_{n-1}j_n}|1\rangle}{\sqrt{2}} \otimes \ldots \otimes \frac{|0\rangle + e^{2\pi i\, 0.j_1 j_2 \ldots j_{n-1}j_n}|1\rangle}{\sqrt{2}}$$

$$\boxed{|j_1 j_2\rangle \rightarrow \frac{|0\rangle + e^{2\pi i\, 0.j_2}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2\pi i\, 0.j_1 j_2}|1\rangle}{\sqrt{2}}}$$

$$|00\rangle \rightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}$$

$$|01\rangle \rightarrow \frac{|0\rangle + e^{i2\pi\ 0.1}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{i2\pi\ 0.01}|1\rangle}{\sqrt{2}} = \frac{|00\rangle + i|01\rangle - |10\rangle - i|11\rangle}{2}$$

$$|10\rangle \rightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{i2\pi\ 0.1}|1\rangle}{\sqrt{2}} = \frac{|00\rangle - |01\rangle + |10\rangle - |11\rangle}{2}$$

$$|11\rangle \rightarrow \frac{|0\rangle + e^{i2\pi\ 0.1}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{i2\pi\ 0.11}|1\rangle}{\sqrt{2}} = \frac{|00\rangle - i|01\rangle - |10\rangle + i|11\rangle}{2}$$

27

Product Notation: Two Qubits

$$|j_1,\ldots,j_n\rangle \rightarrow \frac{|0\rangle + e^{2\pi i\ 0.j_n}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2\pi i\ 0.j_{n-1}j_n}|1\rangle}{\sqrt{2}} \otimes \ldots \otimes \frac{|0\rangle + e^{2\pi i\ 0.j_1 j_2 \cdots j_{n-1}j_n}|1\rangle}{\sqrt{2}}$$

$$|00\rangle \rightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}$$

$$|01\rangle \rightarrow \frac{|0\rangle + e^{i2\pi\ 0.1}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{i2\pi\ 0.01}|1\rangle}{\sqrt{2}} = \frac{|00\rangle + i|01\rangle - |10\rangle - i|11\rangle}{2}$$

$$|10\rangle \rightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{i2\pi\ 0.1}|1\rangle}{\sqrt{2}} = \frac{|00\rangle - |01\rangle + |10\rangle - |11\rangle}{2}$$

$$|11\rangle \rightarrow \frac{|0\rangle + e^{i2\pi\ 0.1}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{i2\pi\ 0.11}|1\rangle}{\sqrt{2}} = \frac{|00\rangle - i|01\rangle - |10\rangle + i|11\rangle}{2}$$

As before: $F = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix}$

28

Pick it apart…

Look a little bit more closely:

$$|j_1,\ldots,j_n\rangle \rightarrow \frac{|0\rangle + e^{2\pi i\ 0.j_n}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2\pi i\ 0.j_{n-1}j_n}|1\rangle}{\sqrt{2}} \otimes \ldots \otimes \frac{|0\rangle + e^{2\pi i\ 0.j_1 j_2 \cdots j_{n-1}j_n}|1\rangle}{\sqrt{2}}$$

Very similar to equal superposition. All qubits have an equal amplitude, just not an equal phase.

Each qubit acquires a phase dependent on (the original state of) all prior qubits.

$$\frac{|0\rangle + e^{2\pi i\, 0.j_1 j_2 \cdots j_n}|1\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{2\pi i\,[\frac{j_1}{2} + \frac{j_2}{2^2} + \ldots + \frac{j_n}{2^n}]}|1\rangle}{\sqrt{2}}$$

$$= \frac{|0\rangle + e^{2\pi i\,\frac{j_1}{2}} e^{2\pi i\,\frac{j_2}{2^2}} \ldots e^{2\pi i\,\frac{j_n}{2^n}}|1\rangle}{\sqrt{2}}$$

Product of phases applied, i.e. of the form $\begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i j_k/2^k} \end{pmatrix}$ e.g. rotation by $\theta = \frac{2\pi}{2^k}$ controlled by j_k

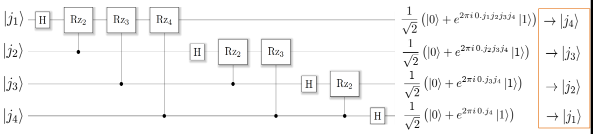
29

Circuit for QFT

Look carefully at the product form:

$$|j_1,\ldots,j_n\rangle \rightarrow \underbrace{\frac{|0\rangle + e^{2\pi i\ 0.j_n}|1\rangle}{\sqrt{2}}}_{|j_1\rangle} \otimes \underbrace{\frac{|0\rangle + e^{2\pi i\ 0.j_{n-1}j_n}|1\rangle}{\sqrt{2}}}_{|j_2\rangle} \otimes \ldots \otimes \underbrace{\frac{|0\rangle + e^{2\pi i\ 0.j_1 j_2 \cdots j_{n-1}j_n}|1\rangle}{\sqrt{2}}}_{|j_n\rangle}$$

Suggests an efficient circuit implementation – e.g. for n=4:



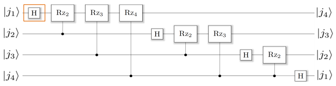
Controlled rotations with: $R_{z_k} = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix}$

Notice how the required QFT form is recovered by re-labelling qubits

30

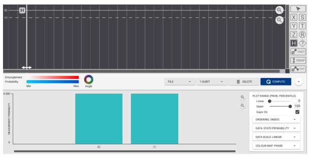
One qubit QFT circuit

Look at the pattern of the circuit:



For one qubit we have just a H-gate:

$$|j_1\rangle \rightarrow \frac{|0\rangle + e^{2\pi i\, 0.j_1}|1\rangle}{\sqrt{2}}$$

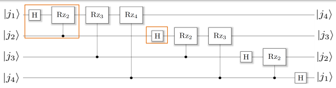


$$|0\rangle \rightarrow \frac{|0\rangle + e^{2\pi i\ 0.0}|1\rangle}{\sqrt{2}} = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

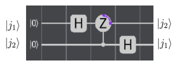
$$|1\rangle \rightarrow \frac{|0\rangle + e^{2\pi i\ 0.1}|1\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{\pi i}|1\rangle}{\sqrt{2}} = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

31

Two Qubit QFT circuit



QUI



$$R_{z_k} = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix} \qquad R_{z_2} = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2} \end{pmatrix}$$

QUI gates:

$$\begin{aligned} R_Z(\theta_R) = e^{i\theta_g}\left[I\cos\frac{\theta_R}{2} - iZ\sin\frac{\theta_R}{2}\right] &= e^{i\theta_g}\left[\begin{pmatrix} \cos\frac{\theta_R}{2} & 0 \\ 0 & \cos\frac{\theta_R}{2} \end{pmatrix} - i\begin{pmatrix} \sin\frac{\theta_R}{2} & 0 \\ 0 & -\sin\frac{\theta_R}{2} \end{pmatrix}\right] \\ &= e^{i\theta_g}\begin{pmatrix} \cos\frac{\theta_R}{2} - i\sin\frac{\theta_R}{2} & 0 \\ 0 & \cos\frac{\theta_R}{2} + i\sin\frac{\theta_R}{2} \end{pmatrix} \\ &= e^{i\theta_g}\begin{pmatrix} e^{-i\theta_R/2} & 0 \\ 0 & e^{+i\theta_R/2} \end{pmatrix} \\ &= e^{i\theta_g}e^{-i\theta_R/2}\begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta_R} \end{pmatrix} \end{aligned}$$

$$R_{z_2} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2} \end{pmatrix} \equiv R_Z\left(\frac{\pi}{2}\right) \qquad \text{with} \quad \theta_g = \frac{\pi}{4}$$

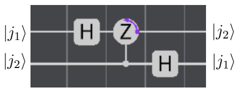
Global phase cancels prefactor

32

Two Qubit QFT circuit - walkthrough

$$|j_1, \ldots, j_n\rangle \rightarrow \frac{|0\rangle + e^{2\pi i\ 0.j_n}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2\pi i\ 0.j_{n-1}j_n}|1\rangle}{\sqrt{2}} \otimes \ldots \otimes \frac{|0\rangle + e^{2\pi i\ 0.j_1 j_2 \ldots j_{n-1} j_n}|1\rangle}{\sqrt{2}}$$

$$R_{z_2} = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2} \end{pmatrix}$$



$|\psi_a\rangle \quad |\psi_b\rangle \quad |\psi_c\rangle$

Check it gives the product form:

$$|\psi_a\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\pi j_1}|1\rangle\right) \otimes |j_2\rangle$$

Hadamard has negative sign on |1> if $j_1 = 1$

$$|\psi_b\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\pi j_1}e^{i(\pi/2)j_2}|1\rangle\right) \otimes |j_2\rangle$$

R_{z2} applied only when $j_2 = 1$

$$|\psi_c\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\pi j_1}e^{i(\pi/2)j_2}|1\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\pi j_2}|1\rangle\right)$$

Hadamard on $|j_2>$

Binary fractions: $e^{i\pi j_1}e^{i(\pi/2)j_2} = e^{2\pi i(j_1/2 + j_2/4)} = e^{2\pi i\, 0.j_1 j_2}$

$$\boxed{|\psi_c\rangle = \underbrace{\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\, 0.j_1 j_2}|1\rangle\right)}_{|j_2\rangle} \otimes \underbrace{\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i\, 0.j_2}|1\rangle\right)}_{|j_1\rangle}}$$

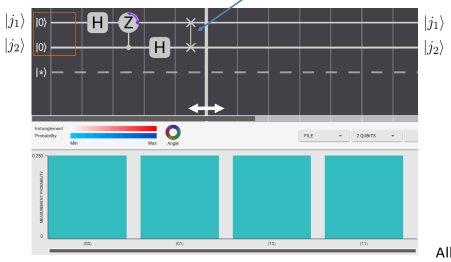
i.e. circuit gives product form with j1 and j2 order reversed

33

PHYC90045 Introduction to Quantum Computing

Two Qubit QFT circuit - QUI

Note: inserted SWAP gate so ordering is same c/f ket expression



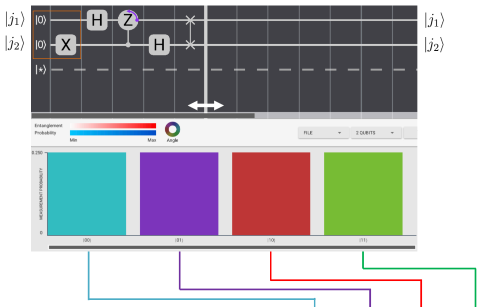
All phases zero

$$\boxed{|00\rangle} \rightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}$$

34

PHYC90045 Introduction to Quantum Computing

Two Qubit QFT circuit - QUI

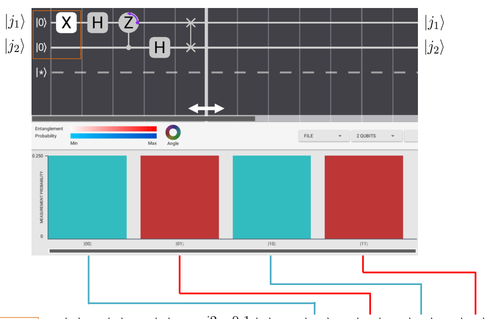


$$\boxed{|01\rangle} \rightarrow \frac{|0\rangle + e^{i2\pi\ 0.1}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{i2\pi\ 0.01}|1\rangle}{\sqrt{2}} = \frac{|00\rangle + i\,|01\rangle - |10\rangle - i\,|11\rangle}{2}$$

35

PHYC90045 Introduction to Quantum Computing

Two Qubit QFT circuit - QUI

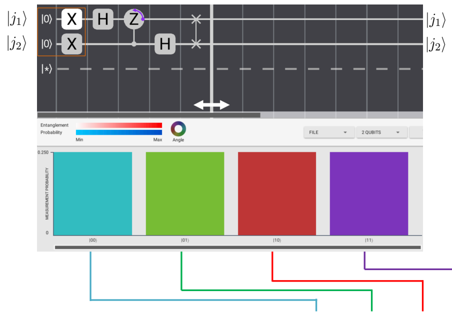


$$\boxed{|10\rangle} \rightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{i2\pi\ 0.1}|1\rangle}{\sqrt{2}} = \frac{|00\rangle - |01\rangle + |10\rangle - |11\rangle}{2}$$

36

PHYC90045 Introduction to Quantum Computing

Two Qubit QFT circuit - QUI

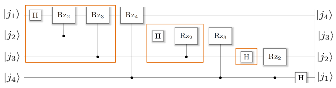


$$|11\rangle \rightarrow \frac{|0\rangle + e^{i2\pi\ 0.1}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{i2\pi\ 0.11}|1\rangle}{\sqrt{2}} = \frac{|00\rangle - i|01\rangle - |10\rangle + i|11\rangle}{2}$$

37

PHYC90045 Introduction to Quantum Computing

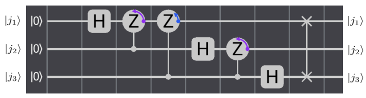
Three Qubit QFT circuit



Rotation gates in the QUI:

$$R_{z_2} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2} \end{pmatrix} \equiv R_Z\left(\frac{\pi}{2}\right) \quad \text{with} \quad \theta_g = \frac{\pi}{4}$$

$$R_{z_3} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} \equiv R_Z\left(\frac{\pi}{4}\right) \quad \text{with} \quad \theta_g = \frac{\pi}{8}$$



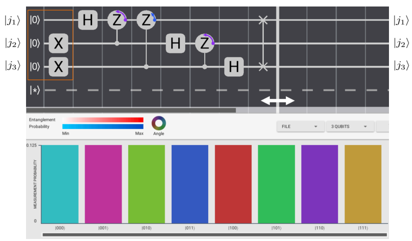
SWAP gate reverses order, so same as input

38

PHYC90045 Introduction to Quantum Computing

Three Qubit QFT - QUI

Example: |011>



NB. same as $\pi/4$ etc

$$|011\rangle \rightarrow \left(\frac{1}{\sqrt{2}}\right)^3 \Big(|000\rangle + e^{3\pi i/4}|001\rangle + e^{3\pi i/2}|010\rangle + e^{9\pi i/4}|011\rangle + e^{i\pi}|100\rangle + e^{7\pi i/4}|101\rangle + e^{5\pi i/2}|110\rangle + e^{13\pi i/4}|111\rangle\Big)$$

39

PHYC90045 Introduction to Quantum Computing

Step back for a moment

After all that, let's check on what we were trying to achieve:

On a single basis state $\mathrm{QFT}\,|a\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2\pi i}{N} k a}\,|k\rangle$

e.g. $$|011\rangle \rightarrow \left(\frac{1}{\sqrt{2}}\right)^3 \Big(|000\rangle + e^{3\pi i/4}|001\rangle + e^{3\pi i/2}|010\rangle + e^{9\pi i/4}|011\rangle + e^{i\pi}|100\rangle + e^{7\pi i/4}|101\rangle + e^{5\pi i/2}|110\rangle + e^{13\pi i/4}|111\rangle\Big)$$

i.e. 3=101 $$|3\rangle \rightarrow \left(\frac{1}{\sqrt{2}}\right)^3 \Big(|0\rangle + e^{3\pi i/4}|1\rangle + e^{3\pi i/2}|2\rangle + e^{9\pi i/4}|3\rangle + e^{i\pi}|4\rangle + e^{7\pi i/4}|5\rangle + e^{5\pi i/2}|6\rangle + e^{13\pi i/4}|7\rangle\Big)$$

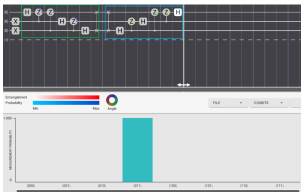
It obeys: $\mathrm{QFT}\,|3\rangle = \frac{1}{\sqrt{8}} \sum_{k=0}^{N-1} e^{\frac{2\pi i}{8} 3k}\,|k\rangle$ (check it!)

40

PHYC90045 Introduction to Quantum Computing

Programing the Inverse QFT

As with any circuit: invert the QFT by inverting every gate and reversing the order:



$$R_{z_2} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2} \end{pmatrix} \equiv R_Z\left(\frac{\pi}{2}\right) \quad \text{with } \theta_g = \frac{\pi}{4}$$

$$R_{z_3} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} \equiv R_Z\left(\frac{\pi}{4}\right) \quad \text{with } \theta_g = \frac{\pi}{8}$$

$$R_Z(\theta_R) = e^{i\theta_g}\left[I\cos\frac{\theta_R}{2} - iZ\sin\frac{\theta_R}{2}\right] = e^{i\theta_g}e^{-i\theta_R/2}\begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta_R} \end{pmatrix}$$

$$R_Z^\dagger(\theta_R) = e^{-i\theta_g}e^{+i\theta_R/2}\begin{pmatrix} 1 & 0 \\ 0 & e^{-i\theta_R} \end{pmatrix}$$

e.g. |011>

i.e. Reverse signs of θ_R and θ_g

$$|011\rangle \boxed{\overset{\mathrm{QFT}}{\rightarrow}} \left(\frac{1}{\sqrt{2}}\right)^3 \Big(|000\rangle + e^{3\pi i/4}|001\rangle + e^{3\pi i/2}|010\rangle + e^{9\pi i/4}|011\rangle + e^{i\pi}|100\rangle + e^{7\pi i/4}|101\rangle + e^{5\pi i/2}|110\rangle + e^{13\pi i/4}|111\rangle\Big) \boxed{\overset{\mathrm{QFT}^\dagger}{\rightarrow}} |011\rangle$$

41

PHYC90045 Introduction to Quantum Computing

Appendix: proof of the product form

In case you want to go through it at your leisure

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i\, jk/N}\,|k\rangle$$
$$= \frac{1}{\sqrt{N}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} e^{2\pi i\, j \sum_l k_l 2^{-l}}\,|k_1 \ldots k_n\rangle$$
$$= \frac{1}{\sqrt{N}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} \otimes_l e^{2\pi i\, j k_l 2^{-l}}\,|k_l\rangle$$
$$= \frac{1}{\sqrt{N}} \otimes_l \left[|0\rangle + e^{2\pi i\, j 2^{-l}}\,|1\rangle\right]$$
$$= \frac{|0\rangle + e^{2\pi i\, 0.j_n}\,|1\rangle}{\sqrt{2}} \otimes \ldots \otimes \frac{|0\rangle + e^{2\pi i\, 0.j_1 j_2 \ldots j_n}\,|1\rangle}{\sqrt{2}}$$

42

This Week

Lecture 11

Fourier Transformations, Regular Fourier Transform, Fourier Transform as a matrix, Quantum Fourier Transform, QUI examples, Inverse QFT

Lecture 12

Shor's Quantum Factoring algorithm, Shor's algorithm for factoring and discrete logarithm, HSP Problem

Lab 6

QFT and Shor's algorithm

43