papergrid®

Reflects You

Do not wait to strike till the iron is hot;
but make it hot by striking.

sooraj5s1729@gmail.com +91-9400635788

INDEX

(7)

Name SOORAJ. S. Std Sec

Roll No. Subject School/College

Sl. No.	Date	Title	Page No.	Teacher Sign/ Remarks
		QUANTUM COMPUTATION & QUANTUM INFORMATION - Nielsen & Chuang		

(5.) THE QUANTUM FOURIER TRANSFORM & ITS APPLICATIONS.

- Quantum Algorithms.

Quantum parallelism

Heuristically,

quantum parallelism allows quantum computers to evaluate a function $f(x)$ for many different values of x simultaneously.

Suppose, $f(x) : \{0,1\} \longrightarrow \{0,1\}$ is a function with a one-bit domain and range.

Consider a two qubit quantum computer which starts in the state $|x, y\rangle$.

With an appropriate sequence of logic gates it is possible to transform this state into $|x, y \oplus f(x)\rangle$.

Quantum parallelism

Heuristically,

quantum parallelism allows quantum computers to evaluate a function $f(x)$ for many different values of x simultaneously.

Suppose, $f(x) : \{0,1\} \longrightarrow \{0,1\}$ is a function with a one-bit domain and range.

Consider a two qubit quantum computer which starts in the state $|x, y\rangle$.

With an appropriate sequence of logic gates it is possible to transform this state into $|x, y \oplus f(x)\rangle$.

$$|\psi_{in}\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes |0\rangle = \frac{|0\rangle \otimes |0\rangle + |1\rangle \otimes |0\rangle}{\sqrt{2}}$$

$$|\psi_{out}\rangle = \frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}$$

← The different terms contain information about both $f(0)$ and $f(1)$; it is almost as if we have evaluated $f(x)$ for two values of x simultaneously, a feature known as quantum parallelism.

Unlike classical parallelism, where multiple circuits each built to compute $f(x)$ are executed simultaneously,

here a single $f(x)$ circuit is employed to evaluate the function for multiple values of x simultaneously, By exploiting the ability of a quantum computer to be in superpositions of different states.

Hadamard transform / Walsh-Hadamard transform

- n Hadamard gates acting in parallel on n qubits.

$$H^{\otimes n} = H \otimes H \otimes \cdots \otimes H$$

$H^{\otimes n} |0\rangle^{\otimes n}$ ⇓

$$H^{\otimes n} |00\cdots0\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle$$

where the sum is over all possible values of x.

i.e., the Hadamard transform produces an equal superposition of all computational basis states. Moreover, it does this extremely efficiently, producing a superposition of 2^n states using just n gates.

Eg:-

$$H^{\otimes 2}|00\rangle = \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) = \frac{|00\rangle+|01\rangle+|10\rangle+|11\rangle}{2}$$

∴

Quantum parallel evaluation of a function with an n bit input x and 1 bit output, $f(x)$

Prepare the $n+1$ qubit state $|0\rangle^{\otimes n}|0\rangle$

Apply the Hadamard transform to the first n qubits, followed by the quantum circuit implementing U_f, which produces the state.

$$\frac{1}{\sqrt{2^n}}\sum_x |x\rangle|f(x)\rangle$$

In some sense, quantum parallelism enables all possible values of the function f to be evaluated simultaneously, even though we apparently only evaluated f once.
However, this parallelism is not immediately useful.

Measurement of the state $\sum_x |x, f(x)\rangle$ would give only $f(x)$ for a single qubit value of x.

Quantum computation requires something more than just quantum parallelism to be useful; it requires the ability to extract information about more than one value of $f(x)$ from superposition states like $\sum_x |x, f(x)\rangle$.

Deutsch's algorithm

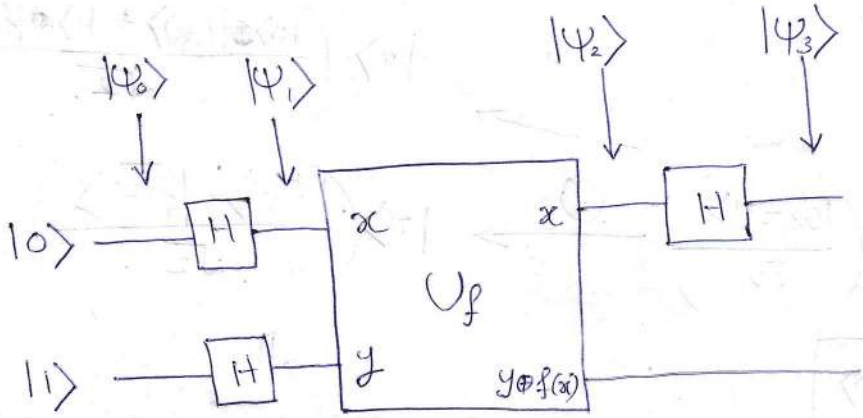


Fig. 1.19 Quantum circuit implementing Deutsch's algorithm.

The i/p state,

$$|\psi_0\rangle = |0\,1\rangle$$

is sent thro' two Hadamard gates to give

$$|\psi_1\rangle = \left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

$$|x\rangle \left(\frac{|0\rangle \oplus |f(x)\rangle - |1\rangle \oplus |f(x)\rangle}{\sqrt{2}}\right)$$

$$|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \xrightarrow{U_f} |x\rangle \left(\frac{|f(x)\rangle - |\overline{f(x)}\rangle}{\sqrt{2}}\right)$$

$$\| $$

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

$|0\rangle \oplus |f(x)\rangle = |f(x)\rangle$
$|1\rangle \oplus |f(x)\rangle = |\overline{f(x)}\rangle$

$\therefore$

$$|\psi_2\rangle = (-1)^{f(0)}\left[\frac{|0\rangle}{\sqrt{2}}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\right] + (-1)^{f(1)}\left[\frac{|1\rangle}{\sqrt{2}}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\right]$$

$$= \begin{cases} \pm \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) & \text{if } f(0) = f(1) \\ \pm \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) & \text{if } f(0) \neq f(1) \end{cases}$$

The final Hadamard gate on the 1st qubit gives us,

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) & \text{if } f(0)=f(1) \\ \pm|1\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) & \text{if } f(0)\neq f(1) \end{cases}$$

$$f(0)\oplus f(1) = \begin{cases} 0 & \text{if } f(0)=f(1) \\ 1 & \text{if } f(0)\neq f(1) \end{cases}$$

$\therefore$

$$|\psi_3\rangle = \pm|f(0)\oplus f(1)\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

$\Rightarrow$ By measuring the 1st qubit we may determine $f(0)\oplus f(1)$.

The quantum circuit has given us the ability to determine a global property of $f(x)$, namely $f(0) \oplus f(1)$, using only one evaluation of $f(x)$!

This is faster than is possible with a classical apparatus, which would require at least two evaluations.

i.e.,

By just measuring the 1st qubit we can distinguish whether the function is balanced $(f(0) \neq f(1))$ or constant $(f(0) = f(1))$.

And we do this by just one function evaluation (along with other transformations but the constraint here was the # of times we apply $f(\cdot)$).

Classical Algorithm

```
if f(0) = 0 :
    if f(1) = 0 :
        print ("Constant")
    else
        print ("Balanced")
else
    if f(1) = 0 :
        print ("Balanced")
    else
        print ("Constant")
```

⟶ We require two function evaluations to figure out the answer.

This example highlights the difference between quantum parallelism and classical randomized algorithms. Naively, one might think that the state $|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle$ corresponds rather closely to a probabilistic classical computer that evaluates $f(0)$ with probability $1/2$ or, $f(1)$ with probability $1/2$.

The difference is that in a classical computer these two alternatives forever exclude one another; in quantum computer it is possible for the 2 alternatives to interfere with one another to yield some global property of the function f, by using something like the Hadamard gate to recombine the different alternatives, as was done in Deutsch's algorithm.

The essence of the design of many quantum algorithms is that a clever choice of function & final transformation allows efficient determination of useful global information about the function — information which can not be attained quickly on a classical computer.

The Deutsch-Jozsa algorithm

Deutsch's problem

- Alice, in Amsterdam, selects a number x from 0 to 2^n-1, and mails it in a letter to Bob, in Boston. Bob calculates some function $f(x)$ and replies with the result, which is either 0 or 1. Now, Bob has promised to use a function f which is one of 2 kinds; either $f(x)$ is constant for all values of x, or else $f(x)$ is balanced, that is, equal to 1 for exactly half of all the possible x, and 0 for the other half. Alice's job is to determine with certainty whether Bob has chosen a constant or a balanced function, corresponding with him as little as possible.

Classical case

Alice may only send Bob one value of x in each letter.

At worst, Alice may receive $\frac{2^n}{2}$ 0's before finally getting a 1, so she will need to query Bob at least $\frac{2^n}{2}+1$ times, to know that Bob's function is balanced. The best deterministic classical algorithm she can use therefore requires $\frac{2^n}{2}+1$ queries.

In each letter, Alice sends Bob n bits of information.

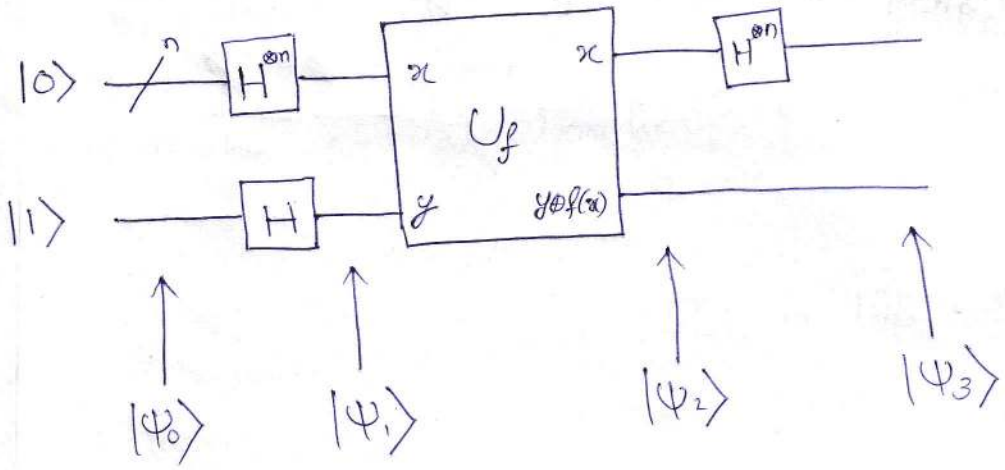
In this example, physical distance is being used to artificially elevate the cost of calculating $f(x)$. But this is not needed in the general problem, where $f(x)$ may be inherently difficult to calculate.

Quantum case

If Bob and Alice were able to exchange qubits, instead of just classical bits, and if Bob agreed to calculate $f(x)$ using a unitary transform U_f, then Alice could achieve her goal in just one correspondence with Bob, using the following algorithm.

Fig 1.20 → Quantum circuit implementing the general Deutsch-Jozsa algorithm

The wire with a '/' thro' it represents a set of n qubits.



The i/p state,

$$|\psi_0\rangle = |0\rangle^{\otimes n} |1\rangle$$

After the Hadamard transform on the query register and the Hadamard gate on the answer register, we have

$$|\psi_1\rangle = \sum_{x \in \{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

→ The query register is now in superposition of all values, and the answer register is in an evenly weighted super position of 0 and 1.

$$\sum_x \frac{|x\rangle}{\sqrt{2^n}} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \xrightarrow{U_f} \sum_x \frac{|x\rangle}{\sqrt{2^n}} \left(\frac{|0\rangle \oplus |f(x)\rangle - |1\rangle \oplus |f(x)\rangle}{\sqrt{2}} \right)$$

$$= \sum_x \frac{|x\rangle}{\sqrt{2^n}} \left(\frac{|f(x)\rangle - |\overline{f(x)}\rangle}{\sqrt{2}} \right)$$

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

The function f is evaluated (by Bob) using $U_f : |x,y\rangle \longrightarrow |x, y \oplus f(x)\rangle$, giving

$$|\psi_2\rangle = \sum_x (-1)^{f(x)} \frac{|x\rangle}{\sqrt{2^n}} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

Alice now has a set of qubits in which the result of Bob's function evaluation is stored in the amplitude of the qubit superposition state.

She now interferes terms in the superposition using a Hadamard transform on the query register.

$$H|0\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \quad \& \quad H|1\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

$\therefore$

For a single qubit, $\boxed{H|x\rangle = \sum_z \frac{(-1)^{xz}|z\rangle}{\sqrt{2}}}$

Thus,

$$H^{\otimes n}|x_1,\cdots,x_n\rangle = \sum_{z_1} \frac{(-1)^{x_1 z_1}|z_1\rangle}{\sqrt{2}} \otimes \sum_{z_2} \frac{(-1)^{x_2 z_2}|z_2\rangle}{\sqrt{2}} \otimes \cdots \otimes \sum_{z_n} \frac{(-1)^{x_n z_n}|z_n\rangle}{\sqrt{2}}$$

$$= \sum_{z_1 z_2 \cdots z_n} \frac{(-1)^{x_1 z_1 + x_2 z_2 + \cdots + x_n z_n}|z_1 z_2 \cdots z_n\rangle}{\sqrt{2^n}}$$

$$= \sum_z \frac{(-1)^{x\cdot z}|z\rangle}{\sqrt{2^n}}$$

$x \cdot z$: bitwise inner product of x & z, modulo 2.

Substituting $H^{\otimes n}|x\rangle = \frac{\sum_z (-1)^{x\cdot z}|z\rangle}{\sqrt{2^n}}$

in $|\psi_2\rangle = \sum_x (-1)^{f(x)} \frac{|x\rangle}{\sqrt{2^n}} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$

$\therefore$

$$|\psi_3\rangle = \sum_x (-1)^{f(x)} \frac{H^{\otimes n}|x\rangle}{\sqrt{2^n}} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

$$= \sum_x (-1)^{f(x)} \frac{\sum_z (-1)^{x\cdot z}|z\rangle}{\sqrt{2^n}} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

$$= \sum_z \left\{ \sum_x \frac{(-1)^{x\cdot z + f(x)}|z\rangle}{2^n} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \right\}$$

Alice now observes the query register.

The amplitude for the state $|0\rangle^{\otimes n}$ is $\sum_x \frac{(-1)^{f(x)}}{2^n}$ since $x \cdot z = 0$.

$|z\rangle = |0\rangle^{\otimes n}$

Two possible cases

- f is constant
  - $f(x_1) = f(x_2) \ldots = f(x_N)$
- f is Balanced
  - $f(x) = 1$ for exactly half of all the possible x, & 0 for the other half.

When f is constant, the amplitude for $|0\rangle^{\otimes n}$ is: $\sum_x \frac{(-1)^{f(x)}}{2^n} = (-1)^{f(x)} \frac{2^n}{2^n} = +1$ or -1 depending on the constant value ~~value~~ $f(x)$ takes.

$\| |\psi_3\rangle \|^2 = 1 \Longrightarrow$ All the other amplitudes must be zero.

Since,

$x = |0\rangle^{\otimes n} \Longrightarrow |\psi_3'\rangle = \pm |0\rangle^{\otimes n} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$

$= \frac{\pm 1}{\sqrt{2}} \cdot |0\rangle^{\otimes n} \left(|0\rangle - |1\rangle \right)$

f is constant

$\Longrightarrow$ an observation will yield 0's for all qubits in the query register.

If f is balanced then the +ve and -ve contributions to the amplitude for $|0\rangle^{\otimes n}$ $\left(\sum_x \frac{(-1)^{f(x)}}{2^n} \right)$ cancel, leaving an amplitude of zero.

f is balanced

$\Longrightarrow$ a measurement must yield a result other than 0 on at least one qubit in the query register.

∴

If Alice measures all 0's then the function is constant; otherwise the function is balanced.

Algorithm : Deutsch - Jozsa

Inputs : A Black Box U_f which performs the transformation $|x\rangle|y\rangle \longrightarrow |x\rangle|y \oplus f(x)\rangle$ for $x \in \{0, \ldots, 2^n - 1\}$ and $f(x) \in \{0, 1\}$.

It is promised that $f(x)$ is either constant for all values of x, or else $f(x)$ is balanced, i.e., equal to 1 for exactly half of all the possible x, and 0 for the other half.

Outputs : 0 iff f is constant

Runtime : One evaluation of U_f. Always succeeds.

Procedure :

① $|0\rangle^{\otimes n} |1\rangle$ initialize state

② $\rightarrow \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$ create superposition using Hadamard gates.

③ $\rightarrow \frac{1}{\sqrt{2^n}} \sum (-1)^{f(x)} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$ calculate function f using U_f

④ $\rightarrow \sum_z \sum_x \frac{(-1)^{x \cdot z + f(x)} |z\rangle}{\sqrt{2^n}} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$ Perform Hadamard transform

⑤ $\rightarrow z$ measure to obtain final output z

* ⟹ A quantum computer can solve Deutsch's problem with one evaluation of the function f compared to the classical requirement for $\frac{2^n}{2} + 1$ evaluations.

Looks impressive!

But,

there are several important caveats.

① Deutsch's problem is not an especially important problem; it has no known applications.

② The comparison b/w classical and quantum algorithms is in some ways an apples and oranges comparison, as the method for evaluating the function is quite different in the 2 cases.

③ If Alice is allowed to use a probabilistic classical computer, then by asking Bob to evaluate $f(x)$ for a few randomly chosen x she can very quickly determine with high probability whether f is constant or balanced. This probabilistic scenario is perhaps more realistic than the deterministic scenario we have been considering.

Ex:1

Probabilistic classical algorithm

Suppose that the problem is not to distinguish b/w the constant & balanced functions with certainty, but rather, with some probability of error $\epsilon < 1/2$.

What is the performance of the best classical algorithm for this problem?

Ans:

Consider that Bob generates a list of arbitrary length from a balanced function. Then, the list will contain equally many zeros and ones, thus if Alice draws a random element in the list it will be a zero or one with a probability $1/2$.

If she draws 2 elements then she can obtain the outcomes 00, 01, 10, and 11, each with an equal probability of $1/4$.

If Alice now has to guess whether the function was constant or balanced, she will guess correctly half of the times.

$$f(t=2) = 2\frac{2^2 \times 2!}{2^2 \times 2^2} = \frac{2}{4} = 1/2$$

If she instead draws a 3rd element the outcome will be a uniform probability distribution over the following possible outcomes

000, 001, 010, 011, 100, 101, 110, 111.

Alice will now guess correctly 6 out of 8 times; the problem is solved with an error probability of $2/8 = 1/4$

Let Alice draws t elements randomly before guessing, the error probability becomes, $\epsilon(t) = \frac{2}{2^t} = \frac{1}{2^{t-1}}$

$2^n/2$ # of 1's and 0's.

$x_1, x_2, \ldots, x_N$

$f(x_1), f(x_2), \ldots, f(x_N)$ } # $= 2^n = N$

half are 1 and other half 0.

$$\epsilon(t) = \frac{2 \times 1}{2}$$

If we tweak this solution so that the same element cannot be drawn twice; Alice stores the addresses to the previously drawn elements, discarding oracle queries to the same address.

The error probability then becomes.

$$\epsilon(t) = 2 \times \frac{2^{n-1} \times (2^{n-1}-1)(2^{n-1}-2) \cdots (2^{n-1}-(t-1))}{2^n (2^n-1)(2^n-2) \cdots (2^n-(t-1))}$$

$$= 2 \prod_{j=1}^{t} \frac{2^{n-1}+1-j}{2^n+1-j}$$

Note: If one draws a # of elements $t > 2^{n-1}+1$ the error probability becomes zero.

With $t=2$ evaluations, the error probability,

$$\epsilon(2) = 2\,\frac{2^{n-1}(2^{n-1}-1)}{2^n(2^n-1)}$$

$$= \frac{2^{n-1}-1}{2^n-1} = \frac{\frac{2^n}{2}-1}{2^n-1}$$

$$= \frac{2^n-2}{2(2^n-1)} = \frac{2^n-1-1}{2(2^n-1)}$$

$$= \frac{1}{2} - \frac{1}{2(2^n-1)} < \frac{1}{2}$$

$\Longrightarrow$ A probabilistic classical computer can solve Deutsch's problem with 2 evaluations with some probability of error $< 1/2$.

Discrete Fourier Transform (DFT)

Fourier transform – limit of Fourier series

A non-periodic function can be viewed as a periodic one, by taking the limit of $L \to \infty$.

Consider the Fourier series for $f(x)$,

$$f(x) = \sum_{n=-\infty}^{+\infty} C_n e^{i\frac{2\pi n}{L}x} = \sum_{n=-\infty}^{+\infty} C_n e^{ik_n x}$$

where, $k_n = \frac{2n\pi}{L}$ and

$$C_n = \frac{1}{L} \int_{-L/2}^{+L/2} f(x)\, e^{-ik_n x}\, dx$$

Fourier series only includes modes with wavenumbers $k_n = \frac{2\pi n}{L}$ with adjacent modes separated by $\delta k = \frac{2\pi}{L}$.

As $L \to \infty$, $\delta k = \frac{2\pi}{L} \to 0$.

— the modes become more & more finely separated in k

In this limit, we are then interested in the variation of C as a function of the continuous variable k.

The factor $\frac{1}{L}$ outside the integral looks problematic in the limit $L \to \infty$, but this can be evaded by defining a new quantity:

$$\tilde{f}(k) = L \times C(k) = \lim_{L\to\infty} \int_{-L/2}^{+L/2} f(x)\, e^{-i n \delta k x}\, dx$$

where; $L \to \infty$, $\delta k = \frac{2\pi}{L} \to 0$, $\lim_{\substack{L\to\infty \\ \delta k \to 0}} n \delta k = k$

$\therefore$

$$\tilde{f}(k) = \int_{-\infty}^{+\infty} f(x)\, e^{-ikx}\, dx$$

which is the Fourier transform of the non-periodic function $f(x)$.

$$f(x) = \lim_{L\to\infty} \sum_{n=-\infty}^{+\infty} C(\delta k)\, e^{in\delta k x}$$

$$= \lim_{L\to\infty} \sum_{n=-\infty}^{+\infty} \frac{L}{2\pi} C(\delta k)\, e^{in\delta k x} \cdot \delta k$$

$$\lim_{\delta k\to 0} \sum g(k)\,\delta k = \int g(k)\, dk$$

$$n: -\infty \to +\infty \Longrightarrow k = n\delta k : -\infty \to +\infty$$

$$f(x) = \frac{1}{2\pi} \int_{-\infty}^{+\infty} \tilde{f}(k)\, e^{ikx}\, dk$$

is the inverse Fourier transform.

DFT

The DFT is the equivalent of the continuous Fourier transform for functions that are sampled discretely at N equally spaced points x_n separated by $\Delta x = L/N$ such that $x_n = n\,\Delta x = n\,L/N$

The Fourier transform of the original signal $f(x)$ could be:

$$\tilde{f}(k) = \int_{-\infty}^{+\infty} f(x)\, e^{-ikx}\, dx$$

Let N samples be,

$$f[x_n] = f[0], f[1], \ldots, f[N-1]$$

$$L = N\delta x \implies \delta x = L/N$$

$$x_n = n\,\delta x = n(L/N)$$

$k_m = m\delta k$ where $k_m = \frac{2m\pi}{L}$ & $\delta k = \frac{2\pi}{L}$

Given the function $f(x)$ is zero outside the region $x \in [0, N]$, we can express its Fourier transform as,

$$\tilde{f}(k) = \int_0^N f(x)\, e^{-ikx}\, dx$$

The integral can be approximated by summing over the N-sampled values:

$$\tilde{f}(k) \approx \sum_{n=0}^{N-1} f[x_n]\, e^{-ik_m x_n}\, \delta x$$

$$= \sum_{n=0}^{N-1} f[x_n]\, e^{-ik_m x_n} \left(\frac{L}{N}\right)$$

$$= \frac{L}{N} \sum_{n=0}^{N-1} f[x_n]\, e^{-i k_m x_n}$$

The discrete Fourier transform (DFT) of the sequence x_n is given by,

$$f[k_m] = \sum_{n=0}^{N-1} f[x_n] e^{-ik_m x_n}$$

* The value of DFT is (upto the constant of proportionality L/N) an approximation of the value of the Fourier transform at the frequency ν_k

$$e^{-ik_m x_n} = e^{-i\frac{2m\pi}{L} \cdot n\delta x} = e^{-i\frac{2m\pi}{L} \times n \times \frac{L}{N}} = e^{-i\frac{2m\pi}{N} n} = e^{-2\pi imn/N}$$

$$f[k_m] = \sum_{n=0}^{N-1} f[x_n] e^{-ik_m x_n}$$

$$= \sum_{n=0}^{N-1} f[x_n] e^{-i\frac{2m\pi}{L} x_n}$$

$$= \sum_{n=0}^{N-1} f[x_n] e^{-2\pi imn/N}$$

The inverse Fourier transform can be expressed as :

$$f(x) = \frac{1}{2\pi} \int_0^{N} \tilde{f}(k)\, e^{ikx}\, dk$$

the integral can be approximated by summing over the N- sampled values

$$f(x_n) \approx \frac{1}{2\pi} \sum_{m=0}^{N-1} f(k_m)\, e^{ik_m x_n}\, \delta k$$

$$= \frac{1}{2\pi} \sum_{m=0}^{N-1} f(k_m)\, e^{ik_m x_n} \times \frac{2\pi}{L}$$

$$= \frac{1}{L} \sum_{m=0}^{N-1} f(k_m)\, e^{ik_m x_n}$$

Substitute $f(k_m) = \frac{L}{N} f[k_m]$

$$f[x_n] = \frac{1}{K} \sum_{m=0}^{N-1} \frac{L}{N} f[k_m] e^{ik_m x_n}$$

$$= \frac{1}{N} \sum_{m=0}^{N-1} f[k_m] e^{ik_m x_n}$$

The inverse DFT is,

$$f[x_n] = \frac{1}{N} \sum_{m=0}^{N-1} f[k_m] e^{ik_m x_n}$$

$$f[x_n] = \frac{1}{N} \sum_{m=0}^{N-1} f[k_m] e^{i\frac{2m\pi}{L} x_n}$$

$$= \frac{1}{N} \sum_{m=0}^{N-1} f[k_m] e^{2\pi i mn/N}$$

□ Change of Basis

DFT of $f[x_n]$:

$$f[k_m] = \sum_{n=0}^{N-1} f[x_n] e^{-2\pi i mn/N}$$

The IDFT is:

$$f[x_n] = \frac{1}{N} \sum_{n=0}^{N-1} f[k_m] e^{2\pi i mn/N}$$

A discrete function of finite duration consisting of N samples can be thought of as a vector in $\mathbb{C}^N$.

$$f[x_n] = f[0]e_0 + f[1]e_1 + \cdots\cdots + f[N-1]e_{N-1}$$

$$=$$

$$\begin{bmatrix} f[0] \\ f[1] \\ \vdots \\ f[N-1] \end{bmatrix} = \begin{bmatrix} f[0] \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ f[1] \\ \\ 0 \end{bmatrix} + \cdots\cdots + \begin{bmatrix} 0 \\ 0 \\ \vdots \\ f[N-1] \end{bmatrix}$$

$$f[x_n] = \frac{1}{N}\sum_{m=0}^{N-1} \tilde{f}[k_m] e^{2\pi i m n/N} = \sum_{m=0}^{N-1} \tilde{c}_k e^{2\pi i m n/N}$$

$$\begin{bmatrix} f[0] \\ f[1] \\ \vdots \\ f[N-1] \end{bmatrix} = \tilde{c}_0 \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} + \tilde{c}_1 \begin{bmatrix} 1 \\ e^{i\frac{2\pi}{N}} \\ \vdots \\ e^{i\frac{2\pi(N-1)}{N}} \end{bmatrix} + \tilde{c}_2 \begin{bmatrix} 1 \\ e^{i\frac{2\pi(2)}{N}} \\ \vdots \\ e^{i\frac{2\pi(2)(N-1)}{N}} \end{bmatrix} + \cdots + \tilde{c}_{N-1} \begin{bmatrix} 1 \\ e^{i\frac{2\pi(N-1)}{N}} \\ \vdots \\ e^{i\frac{2\pi(N-1)^2}{N}} \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \cdots & \omega^{(N-1)^2} \end{bmatrix} \begin{bmatrix} \tilde{c}_0 \\ \tilde{c}_1 \\ \tilde{c}_2 \\ \vdots \\ \tilde{c}_{N-1} \end{bmatrix}$$

where, $\omega = e^{i\frac{2\pi}{N}}$ is the N^{th} root of unity

and $\omega^N = \omega^{2N} = \cdots = 1$

$\Rightarrow$ The DFT is used to represent the vector in $\mathbb{C}^N$, corresponds to a discrete function of finite length consisting of N samples; as a linear combination of vectors $v_k \in \mathbb{C}^N$ of the form:

$$v_k = \left(1, e^{i 2\pi k/N}, e^{i 2\pi (2k)/N}, \ldots\ldots, e^{i 2\pi (N-1)k/N}\right)$$

$$k = 0, 1, \ldots, N-1$$

$$\langle v_l, v_k \rangle = \sum_{n=0}^{N-1} e^{i2\pi ln/N} \overline{e^{i2\pi kn/N}}$$

$$= \sum_{n=0}^{N-1} e^{2\pi i (l-k) n/N}$$

$$= 1 + e^{2\pi i(l-k)/N} + e^{2\pi i(l-k)2/N} + e^{2\pi i(l-k)3/N} + \cdots$$

$$\cdots + e^{2\pi i(l-k)(N-1)/N}$$

$$= \begin{cases} 0 & \text{for } l \neq k \\ N & \text{for } l = k. \end{cases}$$

$$\omega^N = 1 \Rightarrow (1-\omega)(1+\omega+\omega^2+\cdots+\omega^{N-1}) = 0$$

$$\Rightarrow 1+\omega+\omega^2+\cdots+\omega^{N-1} = 0 \quad \& \quad \omega^N = 1$$

$$\omega = e^{2\pi i/N}$$

$$\omega^{(l-k)N} = 1 \Rightarrow (1-\omega^{l-k})(1+\omega^{(l-k)}+\omega^{2(l-k)}+\cdots+\omega^{(N-1)(l-k)}) = 0$$

$$l \neq k: \quad 1+\omega^{(l-k)}+\omega^{2(l-k)}+\cdots+\omega^{(N-1)(l-k)} = 0$$

→ The vectors $\{v_k\}_{k=0}^{N-1}$ form an orthogonal basis for $\mathbb{C}^N$, and the DFT can be understood as computing the coefficients for representing a vector in this basis.

The N-point DFT (N-pt DFT) is a linear map from $\mathbb{C}^N$ to $\mathbb{C}^N$.

The Quantum Fourier transform

One of the most useful ways of solving a problem in mathematics or CS is to transform it into some other problem for which a solution is known. A great discovery of quantum computation has been that some such transformations can be computed much faster on a quantum computer than on a classical computer, a discovery which has enabled the construction of fast algorithms for quantum computers.

The quantum Fourier transform is exactly the same transformation as that of DFT, although the conventional notation for the quantum Fourier transform is somewhat different.

The quantum Fourier transform on an orthonormal basis $|0\rangle, \ldots\ldots, |N-1\rangle$ is defined to be a linear operator with the following action on the basis states,

$$|j\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i jk/N} |k\rangle$$

Equivalently, the action on an arbitrary state may be written:

$$\sum_{j=0}^{N-1} x_j |j\rangle \longrightarrow \sum_{k=0}^{N-1} y_k |k\rangle$$

where,

the amplitudes y_k are the discrete Fourier transform of the amplitudes x_j.

$$|\psi_{in}\rangle = \sum_{j=0}^{N-1} x_j |j\rangle$$

After applying the quantum Fourier transform,

$$|\psi_{out}\rangle = \sum_{j=0}^{N-1} \frac{x_j}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i jk/N} |k\rangle$$

$$= \sum_{j=0}^{N-1} \left(\frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} x_j e^{2\pi i jk/N} |k\rangle \right)$$

$$= \sum_{k=0}^{N-1} \left(\frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i jk/N} \right) |k\rangle$$

$$= \sum_{k=0}^{N-1} y_k |k\rangle$$

(OR) $$F|\psi\rangle = F \sum_{j=0}^{N-1} x_j |j\rangle = \sum_{k=0}^{N-1} y_k |k\rangle$$

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

⇒ QFT can be thought of as DFT being applied to the amplitudes of the quantum state.

* The linear transformation defined by the Quantum Fourier transform is unitary

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i jk/N} |k\rangle$$

Proof

$$\langle m|F^{\dagger} F|j\rangle =$$

$$\langle m'|j'\rangle = \frac{1}{N} \sum_{k,n=0}^{N-1} e^{-2\pi i mn/N} e^{2\pi i jk/N} \langle n|k\rangle$$

$$= \frac{1}{N} \sum_{k,n=0}^{N-1} e^{-2\pi i mn/N} e^{2\pi i jk/N} \delta_{n,k}$$

$$= \frac{1}{N} \sum_{k=0}^{N-1} e^{2\pi i (j-m)k/N}$$

$$= \frac{1}{N} \left[1 + e^{2\pi i (j-m)/N} + e^{2\pi i (j-m)2/N} + \cdots + e^{2\pi i (j-m)(N-1)/N} \right]$$

$$= \frac{1}{N} \begin{cases} 0 & \text{for } j \neq m \\ N & \text{for } j = m \end{cases} \qquad \left\{ 1 + \omega + \cdots + \omega^{N-1} = 0, \ \omega^N = 1 \right.$$

$$= \begin{cases} 0 & \text{for } j \neq m \\ 1 & \text{for } j = m \end{cases}$$

$\Longrightarrow$

Ex: 5.9. Explicitly compute the Fourier transform of the n qubit state $|00\ldots0\rangle$.

Ans: For n-qubit state,

$$N = 2^n$$

$$|00\ldots0\rangle \xrightarrow{F} \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i k \cdot 0/2^n} |k\rangle$$

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

We take $N = 2^n$ where n is some integer. and the basis $|0\rangle, \ldots, |2^n - 1\rangle$ is the computational basis for an n qubit quantum computer.

The state $|j\rangle$ can be written using the binary representation $j = j_1 j_2 \ldots j_n$.

More formally

$$j = j_1 j_2 \ldots j_n$$
$$= j_1 2^{n-1} + j_2 2^{n-2} + \ldots + j_n 2^0$$

For the binary fraction we can represent as.

$$0.j_l j_{l+1} \ldots j_m = \frac{j_l}{2} + \frac{j_{l+1}}{4} + \ldots + \frac{j_m}{2^{m-l+1}}$$

Ex:-

Decimal (Base 10)

$13_{10} = 1 \cdot 10^1 + 3 \cdot 10^0$

$0.625_{10} = \frac{6}{10} + \frac{2}{10^2} + \frac{5}{10^3}$

0	0 0 0 0
1	0 0 0 1
2	0 0 1 0
3	0 0 1 1
4	0 1 0 0
5	0 1 0 1
6	0 1 1 0
7	0 1 1 1
8	1 0 0 0
9	1 0 0 1
10	1 0 1 0
11	1 0 1 1
12	1 1 0 0
13	1 1 0 1

Binary (Base 2)

$1101_2 = 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$

$0.101_2 = \frac{1}{2} + \frac{0}{2^2} + \frac{1}{2^3}$

$$|j_1\rangle \xrightarrow{F} \frac{1}{\sqrt{2}} \sum_{k=0}^{1} e^{2\pi i j_1 k/2} |k\rangle = \frac{|0\rangle + e^{2\pi i j_1/2} |1\rangle}{\sqrt{2}}$$

* Quantum Fourier transform in product representation :

$$|j_1, \dots, j_n\rangle \longrightarrow \frac{\left(|0\rangle + e^{2\pi i 0 \cdot j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0 \cdot j_{n-1} j_n}|1\rangle\right) \otimes \cdots \otimes \left(|0\rangle + e^{2\pi i 0 \cdot j_1 j_2 \cdots j_n}|1\rangle\right)}{2^{n/2}}$$

$$= \frac{\left(|0\rangle + e^{2\pi i j/2}|1\rangle\right)\left(|0\rangle + e^{2\pi i j/2^2}|1\rangle\right) \otimes \cdots \otimes \left(|0\rangle + e^{2\pi i j/2^n}|1\rangle\right)}{2^{n/2}}$$

$$= \frac{1}{2^{n/2}} \sum_{k=0}^{2^n - 1} e^{2\pi i j k/2^n}|k\rangle$$

$$|j\rangle = |j_1, \dots, j_n\rangle \longrightarrow \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi i j k/2^n}|k\rangle$$

$$= |j_1\rangle \otimes \cdots \otimes |j_n\rangle$$

Proof

$$k = k_1 k_2 \cdots k_n = k_1 2^{n-1} + k_2 2^{n-2} + \cdots + k_n 2^0 = \sum_{l=1}^{n} k_l 2^{n-l}$$

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} e^{2\pi i j \left(\sum_{l=1}^{n} k_l 2^{n-l}\right)/2^n}|k\rangle$$

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} e^{2\pi i j \left(\sum_{l=1}^{n} k_l 2^{-l}\right)}|k_1 \cdots k_n\rangle$$

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} \left(e^{2\pi i j k_1 2^{-1}}|k_1\rangle \otimes e^{2\pi i j k_2 2^{-2}}|k_2\rangle \otimes \cdots \otimes e^{2\pi i j k_n 2^{-n}}|k_n\rangle\right)$$

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \cdots \sum_{k_n=0}^{1} \left(\bigotimes_{l=1}^{n} e^{2\pi i j k_l 2^{-l}} |k_l\rangle \right)$$

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[\sum_{k_l=0}^{1} e^{2\pi i j k_l 2^{-l}} |k_l\rangle \right]$$

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[|0\rangle + e^{2\pi i j 2^{-l}} |1\rangle \right]$$

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[|0\rangle + e^{2\pi i \left(\sum_{r=1}^{n} j_r 2^{n-r} \right) 2^{-l}} |1\rangle \right]$$

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[|0\rangle + e^{2\pi i \sum_{r=1}^{n} j_r 2^{n-r-l}} |1\rangle \right]$$

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[|0\rangle + e^{2\pi i \left(j_1 2^{n-l-1} + j_2 2^{n-l-2} + \cdots + j_{n-l} 2^{0} + j_{n-l+1} 2^{-1} + \cdots + j_n 2^{-l} \right)} |1\rangle \right]$$

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[|0\rangle + e^{2\pi i \left(j_1 2^{n-l-1} + \cdots + j_{n-l} 2^0 \right)} \times e^{2\pi i \left(j_{n-l+1} 2^{-1} + \cdots + j_n 2^{-l} \right)} |1\rangle \right]$$

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[|0\rangle + e^{2\pi i j_1 j_2 \cdots j_{n-l}} \times e^{2\pi i \left(0 . j_{n-l+1} j_{n-l+2} \cdots j_n \right)} |1\rangle \right]$$

$$e^{2\pi i j_1 j_2 \cdots j_{n-l}} = 1$$

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[|0\rangle + e^{2\pi i \left(0 . j_{n-l+1} j_{n-l+2} \cdots j_n \right)} |1\rangle \right]$$

$$= \frac{\left(|0\rangle + e^{2\pi i 0 . j_n} |1\rangle \right) \otimes \left(|0\rangle + e^{2\pi i 0 . j_{n-1} j_n} |1\rangle \right) \otimes \cdots \otimes \left(|0\rangle + e^{2\pi i 0 . j_1 j_2 \cdots j_n} |1\rangle \right)}{2^{n/2}}$$

QFT - Quantum Circuit

$|j_1\rangle \otimes |j_2\rangle \otimes \cdots \otimes |j_n\rangle$

$$|j_1 \cdots j_n\rangle \rightarrow \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left[|0\rangle + e^{2\pi i (0 \cdot j_{n-l+1} j_{n-l+2} \cdots j_n)} |1\rangle \right]$$

$$= \frac{\left(|0\rangle + e^{2\pi i 0 \cdot j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0 \cdot j_{n-1} j_n}|1\rangle\right) \otimes \cdots \otimes \left(|0\rangle + e^{2\pi i 0 \cdot j_1 j_2 \cdots j_n}|1\rangle\right)}{2^{n/2}}$$

- The last qubit depends on all the input qubits but the dependence decreases as we go further.

- $e^{2\pi i (0 \cdot x)} = +1 \text{ or } -1 = e^{2\pi i \frac{\alpha}{2}} = e^{\pi i \alpha}$

$\Longrightarrow$ like a Hadamard transformed qubit

Applying the Hadamard gate to the first qubit of the i/p state $|j\rangle = |j_1 j_2 \cdots j_n\rangle$ produces the state,

$$|j\rangle \xrightarrow{H} \frac{1}{2^{1/2}}\left(|0\rangle + e^{2\pi i\, 0.j_1}|1\rangle\right)|j_2 \cdots j_n\rangle$$

since,

$$e^{2\pi i\, 0.j_1} = e^{2\pi i\left(\frac{j_1}{2}\right)} = \begin{cases} -1 & \text{when } j_1 = 1 \\ 1 & \text{when } j_1 = 0 \end{cases}$$

Define a rotation gate which is a unitary operator defined as,

$$R_k \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}$$

such that

$$|0\rangle \longrightarrow |0\rangle$$

$$|1\rangle \longrightarrow e^{2\pi i/2^k}|1\rangle$$

Applying the controlled-R_2 gate controlled by the second qubit produces the

$$\frac{1}{2^{1/2}}\left(|0\rangle + e^{2\pi i 0.j_1 j_2}|1\rangle\right)|j_2 \cdots j_n\rangle$$

We continue applying the controlled-R_3, R_4 through R_n gates controlled on the appropriate bits, each of which adds an extra bit to the phase of the coefficient of the first $|1\rangle$. At the end of this procedure we have the state,

$$\frac{1}{2^{1/2}}\left(|0\rangle + e^{2\pi i(0.j_1 j_2 \cdots j_n)}|1\rangle\right)|j_2 \cdots j_n\rangle$$

Now, we perform a similar procedure on the second qubit. The Hadamard gate puts us in the state

$$\frac{1}{2^{3/2}}\left(|0\rangle + e^{2\pi i(0.j_1 j_2 \cdots j_n)}|1\rangle\right)\left(|0\rangle + e^{2\pi i\, 0.j_2}|1\rangle\right)|j_3 \cdots j_n\rangle$$

and the controlled-R_2 through R_{n-1} gates yield the state

$$\frac{1}{2^{2/2}}\left(|0\rangle + e^{2\pi i(0.j_1 \cdots j_n)}|1\rangle\right)\left(|0\rangle + e^{2\pi i(0.j_2 \cdots j_n)}|1\rangle\right)|j_3 \cdots j_n\rangle$$

Continuing in this fashion for each qubit, giving a final state

$$\frac{1}{2^{n/2}}\left(|0\rangle + e^{2\pi i(0.j_1 \cdots j_n)}|1\rangle\right)\left(|0\rangle + e^{2\pi i(0.j_2 \cdots j_n)}|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi i\, 0.j_n}|1\rangle\right)$$

Swap operations are then used to reverse the order of the qubits. After the swap operations the state of the qubit is:

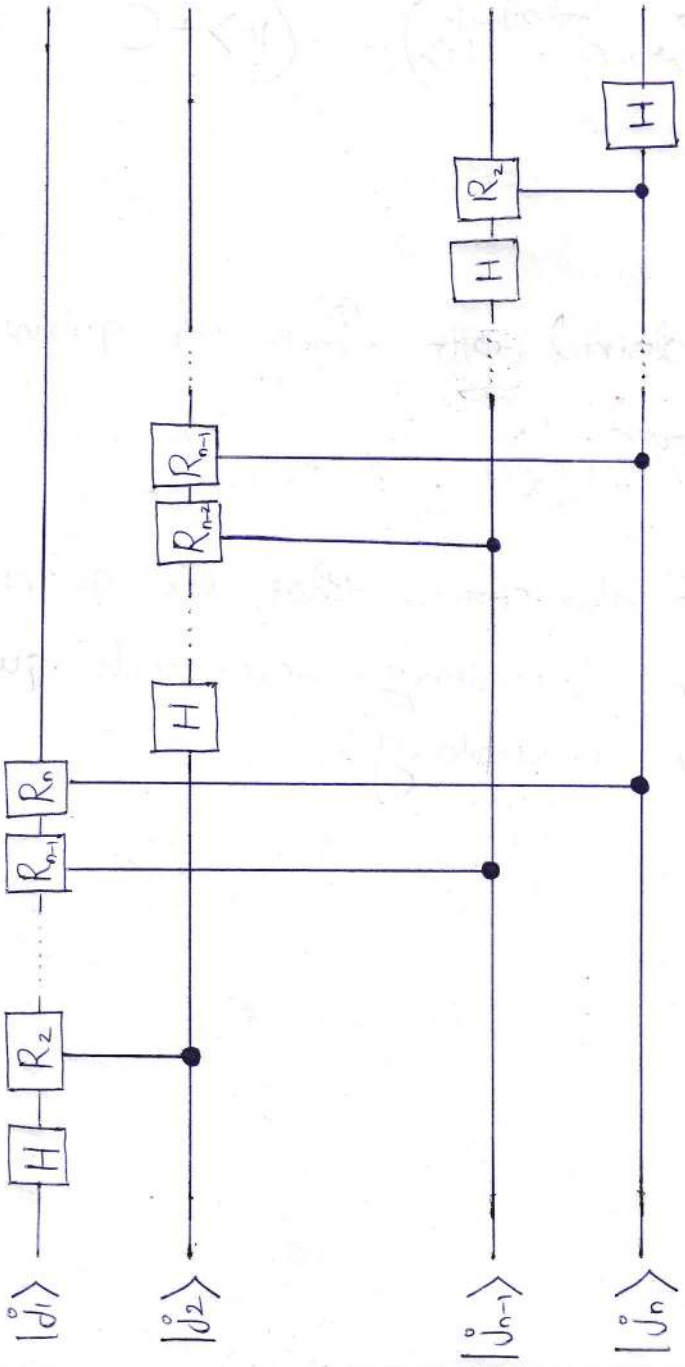
$$\frac{1}{2^{n/2}}\left(|0\rangle + e^{2\pi i\, 0.j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i\, 0.j_{n-1}j_n}|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi i\, 0.j_1 j_2 \cdots j_n}|1\rangle\right)$$

This is the desired o/p from the quantum Fourier transform.

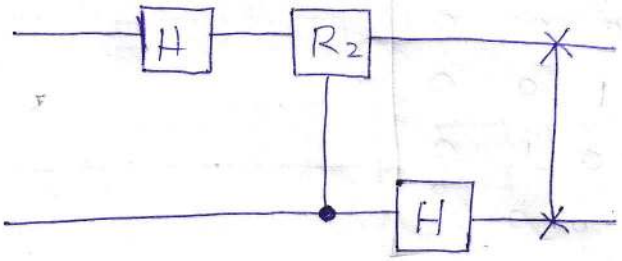
- This construction also proves that the quantum Fourier transform is unitary, since each gate in the circuit is unitary.

Fig 5.1 Efficient circuit for the quantum Fourier transform

Not shown are swap gates at the end of the circuit which reverse the order of the qubits



Two Qubit QFT



$$U_4 = |00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11|$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$U_3 = I \otimes H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}$$

$$U_2 = I \otimes |0\rangle\langle 0| + R_2 \otimes |1\rangle\langle 1|$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \otimes \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & i \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{bmatrix}$$

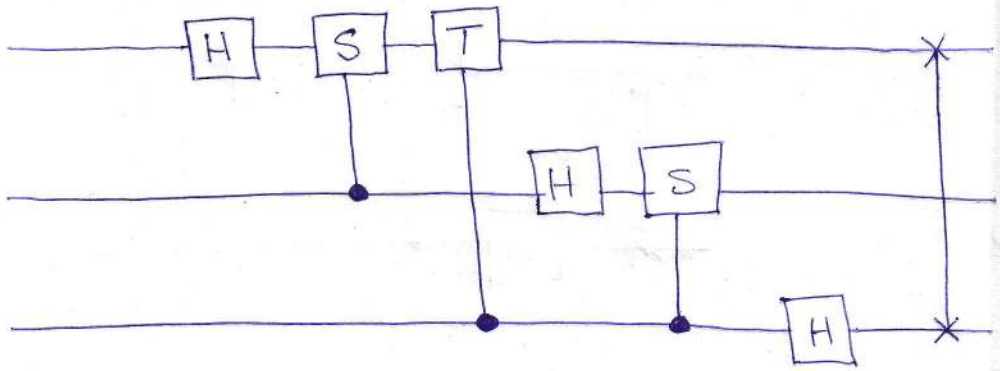
$$U_1 = H \otimes I = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}$$

$$F = U_4 U_3 U_2 U_1$$

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

Three Qubit QFT



Phase gate $S = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/2} \end{bmatrix}$

$\pi/8$ gate $T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

$$F = \frac{1}{\sqrt{8}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^1 & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega^1 & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{bmatrix}$$

Efficiency - QFT

A Hadamard gate & $n-1$ conditional rotations on the 1st qubit — total of n gates.

Followed by,
a Hadamard gate & $n-2$ conditional rotations on the 2nd qubit — total of $n+(n-1)$ gates

$$\Longrightarrow n+(n-1)+\cdots+1 = \frac{n(n+1)}{2} \text{ gates}$$

+

gates involves in the swaps. Was at most $n/2$ swaps are required. & each swap can be accomplished using 3 CNOT gates.

∴ The circuit provides a $O(n^2)$ algorithm for performing the QFT.

In contrast,

the best classical algorithms for computing the DFT on 2^n elements are algorithms such as the FFT, which compute the DFT using $O(n2^n)$ gates.

i.e., it requires exponentially more operations to compute the Fourier transform on a classical computer than it does to implement the Q.FT on a quantum computer.

Ex: 5.4 Give a decomposition of the controlled-R_k gate into single qubit and CNOT gates.

Ans: Any unitary operation can be decomposed as

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$$

3.C (3) M

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}$$

$$\hookrightarrow U = \begin{bmatrix} e^{i(\alpha-\beta/2-\delta/2)}\cos\gamma/2 & -e^{-i(\alpha-\beta/2+\delta/2)}\sin\gamma/2 \\ e^{i(\alpha+\beta/2-\delta/2)}\sin\gamma/2 & e^{i(\alpha+\beta/2+\delta/2)}\cos\gamma/2 \end{bmatrix}$$

$$\Longrightarrow \gamma = 0, \quad \alpha - \left(\frac{\beta}{2}+\frac{\delta}{2}\right) = \pi \quad \left\{ 2\alpha = \pi + \frac{2\pi}{2^k} \right.$$

$$\alpha + \left(\frac{\beta}{2}+\frac{\delta}{2}\right) = \frac{2\pi}{2^k} \quad \left\{ \alpha = \frac{\pi}{2^k} = \frac{2\pi}{2^{k+1}} \right.$$

$$\frac{\beta}{2}+\frac{\delta}{2} = \frac{\pi}{2^k} = \frac{2\pi}{2^{k+1}} \Longrightarrow \beta+\delta = \frac{2\pi}{2^k}$$

Take, $\beta = 0 \;:\; \delta = \frac{2\pi}{2^k}$.

$$\therefore \alpha = \frac{2\pi}{2^{k+1}}, \quad \beta = 0, \quad \gamma = 0, \quad \delta = \frac{2\pi}{2^k}$$

Suppose U is a unitary gate on a single qubit. Then there exists unitary operators A, B, C on a single qubit such that $ABC = I$ & $U = e^{i\alpha} AXBXC$.

where,

$$A = R_z(\beta) R_y(\gamma/2) \; ; \; B = R_y(-\gamma/2) R_z\left(\frac{-(\delta+\beta)}{2}\right)$$

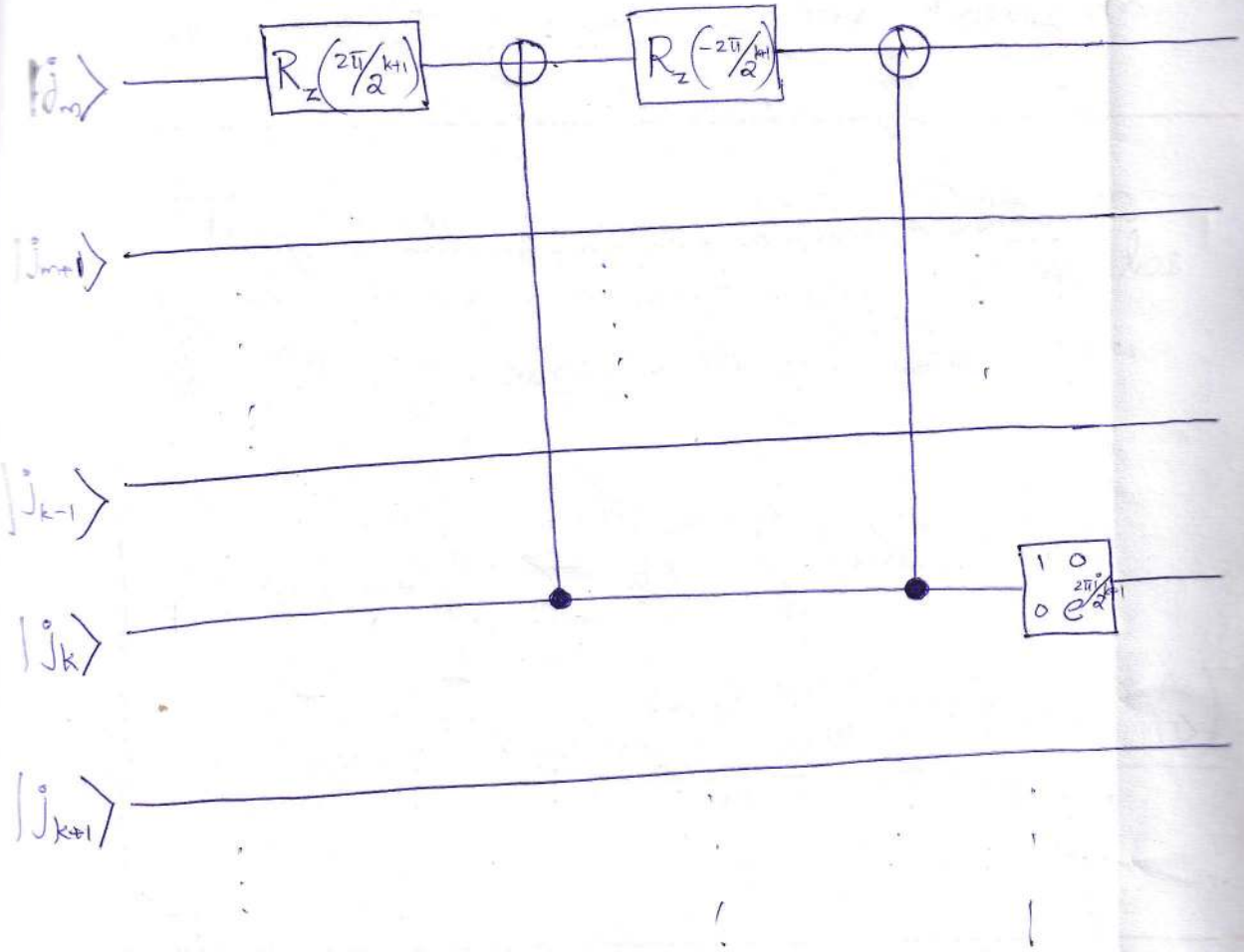
$$C = R_z\left(\frac{\delta - \beta}{2}\right)$$

$$\alpha = \frac{2\pi}{2^{k+1}}, \; \beta = 0, \; \gamma = 0, \; \delta = \frac{2\pi}{2^k}$$

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}$$

$$= e^{2\pi i/2^{k+1}} R_z(0) R_y(0) X R_y(0) R_z\left(\frac{-2\pi}{2^{k+1}}\right) X R_z\left(\frac{2\pi}{2^{k+1}}\right)$$

$$= e^{2\pi i/2^{k+1}} X R_z\left(\frac{-2\pi}{2^{k+1}}\right) X R_z\left(\frac{2\pi}{2^{k+1}}\right)$$


$|j_m\rangle$
$R_z\left(\frac{2\pi}{2^{k+1}}\right)$
$R_z\left(-\frac{2\pi}{2^{k+1}}\right)$
$|j_{m+1}\rangle$
$|j_{k-1}\rangle$
$|j_k\rangle$
$|j_{k+1}\rangle$
1 0
0 $e^{\frac{2\pi i}{2^{k+1}}}$

Ex:5.5. Give a quantum circuit to perform the inverse quantum Fourier transform

Ans:

The inverse quantum Fourier transform is the linear transformation which has the following action on the basis states:

$$|k\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{-2\pi i kj/N} |j\rangle$$

$$= \frac{\left(|0\rangle + e^{-2\pi i 0.k_n}|1\rangle\right) \otimes \left(|0\rangle + e^{-2\pi i 0.k_{n-1}k_n}|1\rangle\right) \otimes \cdots \otimes \left(|0\rangle + e^{-2\pi i 0.k_1 k_2 \cdots k_n}|1\rangle\right)}{2^{n/2}}$$

Applying the Hadamard gate to the 1st qubit of the state $|k\rangle = |k_1 k_2 \cdots k_n\rangle$ produces the state,

$$|k\rangle \longrightarrow \frac{1}{2^{1/2}}\left(|0\rangle + e^{2\pi i 0.k_1}|1\rangle\right)|k_2 \cdots k_n\rangle$$

$$= \frac{1}{2^{1/2}}\left(|0\rangle + e^{-2\pi i 0.k_1}|1\rangle\right)|k_2 \cdots k_n\rangle$$

Applying the controlled-$R_2^\dagger$ gate controlled by the 2nd qubit produces the state

$$\frac{1}{2^{1/2}}\left(|0\rangle + e^{-2\pi i 0.k_1k_2}|1\rangle\right)|k_2 \cdots kn\rangle$$

$$\vdots$$

Replacing the R_i gates in the figure for the circuit of the QFT, with $R_i^\dagger$ gives the quantum circuit to perform the inverse QFT.

Ex: 5.6 Approximate quantum Fourier transform

The quantum circuit construction of the quantum Fourier transform apparently requires gates of exponential precision in the # of qubits used.

However, such precision is never required in any quantum circuit of polynomial size.

Ex:-

Let U be the ideal quantum Fourier transform on n-qubits, and V be the transform which results if the controlled-R_k gates are performed to a precision $\Delta = 1/p(n)$ for some polynomial $p(n)$.

Show that the error $E(U,V) = \max_{|\psi\rangle} \|(U-V)|\psi\rangle\|$ scales as $O\left(n^2/p(n)\right)$, and thus polynomial precision in each gate is sufficient to guarantee polynomial accuracy in the output state.

Ans: $E(U,V) = E\Big(H_1 R_2^1 R_3^1 \cdots R_n^1 \cdots H_{n-1} R_2^{n-1} H_n,$

$H_1 R_2'^1 R_3'^1 \cdots R_n'^1 \cdots H_{n-1} R_2'^{n-1} H_n\Big)$

$\leq E(H_1, H_2) + E(R_2^1, R_2'^1) + E(R_3^1, R_3'^1) + \cdots$

$\cdots + E(R_2^{n-1}, R_2'^{n-1}) + E(H_n, H_n)$

$= 0 + E(R_2^1, R_2'^1) + E(R_3^1, R_3'^1) + \cdots + E(R_2^{n-1}, R_2'^{n-1})$

$= \Delta + \Delta + \cdots + \Delta$

where $R_i'^j$ denotes the controlled-R_i gate with an error $\Delta = 1/p(n)$ which takes the i^{th} gate as a controll bit and j^{th} gate as a target bit.

of R_i^j gates is : $\frac{n(n+1)}{2} - n = \frac{n(n-1)}{2}$

$\Longrightarrow E(U,V)$ scales as $O\left(n^2/p(n)\right)$

Phase Estimation

Suppose, a unitary operator U has an eigen vector $|u\rangle$ with eigenvalue $e^{2\pi i\phi}$, where the value of ϕ is unknown. The goal of the phase estimation algorithm is to estimate ϕ.

To perform the estimation we assume that we have available Black boxes (sometimes known as oracles) capable of preparing the state $|u\rangle$ and performing the controlled-U^{2^j} operation, for suitable non-negative integers j.

* Every eigenvalue of a unitary matrix, U
* A normal matrix is unitary if all its eigenvalues have absolute value one.

The quantum phase estimation procedure uses two registers. The first register contains t qubits initially in the state $|0\rangle$. How we choose t depends on 2 things: the # of digits of accuracy we wish to have in our estimate for ϕ, and with what probability we wish the phase estimation procedure to be useful.

$$U|u\rangle = \lambda|u\rangle$$

U is unitary $\Longrightarrow |\lambda| = 1$

$$\therefore \quad \lambda = e^{2\pi i \phi}$$

where $0 \leq \phi \leq 1$ is called the phase.

Hence the term "phase" in "phase estimation". The term "estimation" comes about not from the fact that quantum computation is probabilistic, but rather in the degree of precision that we are going to compute, or estimate, the phase to.

The phase $\phi \in [0,1]$, so we can write it as a decimal in binary notation as:

$$\phi = 0 \cdot \phi_1 \phi_2 \cdots \phi_t$$

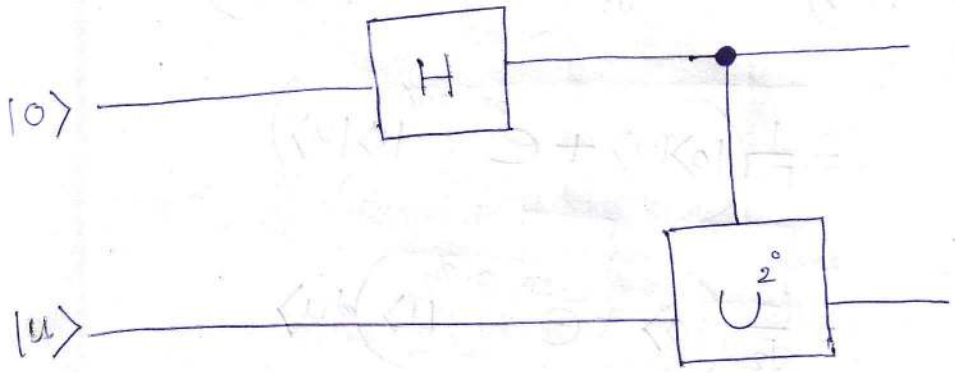
where each ϕ_i is either 0 or 1.

Binary decimal notation

The expression $\phi = 0 \cdot \phi_1 \phi_2 \cdots \phi_t$ is equivalent to:

$$\phi = 0 \cdot \phi_1 \phi_2 \cdots \phi_t \iff \phi = \frac{\phi_1}{2} + \frac{\phi_2}{2^2} + \cdots + \frac{\phi_t}{2^t}$$

$$= \sum_{k=1}^{n} \phi_k 2^{-k}$$



Let U be a unitary operator and $|u\rangle$ an eigenstate with eigenvalue $\lambda = e^{2\pi i \theta \cdot \phi_1}$

1st perform a Hadamard gate on the first qubit to get the state,

$$(H \otimes I)(|0\rangle \otimes |u\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |u\rangle$$

$$= \frac{1}{\sqrt{2}}(|0\rangle|u\rangle + |1\rangle|u\rangle)$$

Performing a controlled U operation, which we have written as U^{2^0}, produces the state,

$$\frac{1}{\sqrt{2}}\left(|0\rangle|u\rangle + |1\rangle|u\rangle\right) \longrightarrow \frac{1}{\sqrt{2}}\left(|0\rangle|u\rangle + |1\rangle U|u\rangle\right)$$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle|u\rangle + e^{2\pi i 0.\phi_1}|1\rangle|u\rangle\right)$$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i 0.\phi_1}|1\rangle\right)\otimes|u\rangle$$

- The 2nd qubit register containing $|u\rangle$ hasn't changed, since $|u\rangle$ is an eigenstate of U. The effect of applying U was that it wrote some information about the eigenvalue into the relative phase of the 1st qubit.

ie.,

$$|0\rangle + |1\rangle \longrightarrow |0\rangle + e^{2\pi i 0.\phi_1}|1\rangle$$

How can we read out this information from the quantum state ?

Applying another Hadamard transformation on the first qubit, which will produce

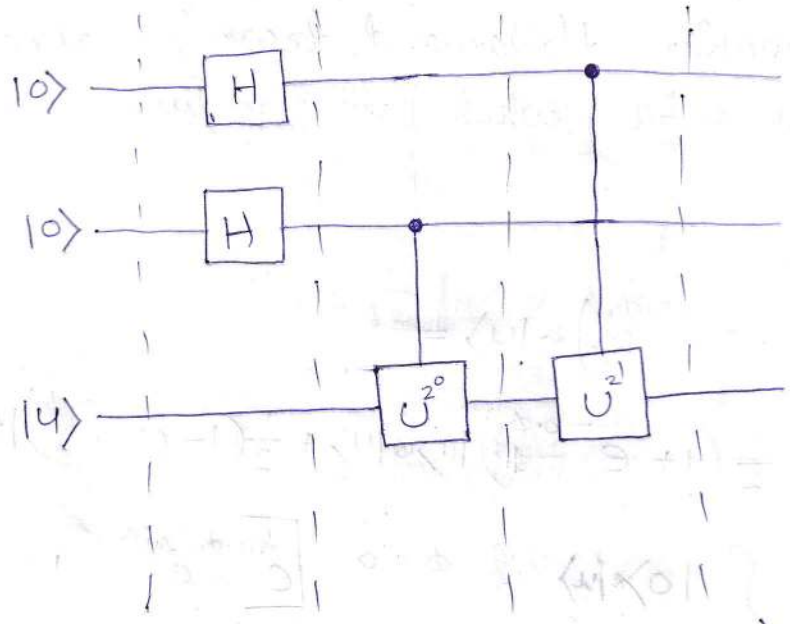
$$(H \otimes I)\ \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i 0.\phi_1}|1\rangle\right) \otimes |u\rangle =$$

$$= \frac{1}{2}\left(1 + e^{2\pi i 0.\phi_1}\right)|0\rangle \otimes |u\rangle + \frac{1}{2}\left(1 - e^{2\pi i 0.\phi_1}\right)|1\rangle \otimes |u\rangle$$

$$= \begin{cases} |0\rangle \otimes |u\rangle \text{ if } \phi_1 = 0 & \left[e^{2\pi i 0.\phi_1} = e^{2\pi i \phi_1/2} = 1\right. \\ |1\rangle \otimes |u\rangle \text{ if } \phi_1 = 1 & \left[e^{2\pi i 0.\phi_1} = e^{2\pi i \phi_1/2} = e^{\pi i} = -1\right. \end{cases}$$

$\Rightarrow$ We measure with certainty (i.e; not probabilistically) a state that tells us what the phase & here the eigenvalue, is.

* Phase estimation for $t=2$ qubits in the top register.



We have $U|u\rangle = e^{2\pi i \phi}|u\rangle = e^{2\pi i 0.\phi_1\phi_2}|u\rangle$

$$|\psi_1\rangle = |0\rangle \otimes |0\rangle \otimes |u\rangle$$

$$|\psi_2\rangle = \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes |u\rangle$$

If $\phi = 0.\phi_1\phi_2$

$$|\psi_3\rangle = \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes U|u\rangle$$

$$= \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle + e^{2\pi i 0.\phi_1\phi_2}|1\rangle) \otimes |u\rangle$$

The relative phase in the 2nd qubit has two digits because we assumed that $\phi = 0.\phi_1\phi_2$ consists of 2 digits.

$$U^{2^1}|u\rangle = U^2|u\rangle = e^{2\pi i(2\phi)}|u\rangle$$

$$2\phi = 2(0.\phi_1\phi_2) = 2\left(\frac{\phi_1}{2} + \frac{\phi_2}{2^2}\right)$$

$$= \phi_1 2^0 + \phi_2 2^{-1} = \phi_1 . \phi_2$$

$$\Rightarrow e^{2\pi i(2\phi)} = e^{2\pi i(\phi_1 . \phi_2)} = e^{2\pi i(\phi_1 + 0.\phi_2)}$$

$$= e^{2\pi i \phi_1} e^{2\pi i(0.\phi_2)} = e^{2\pi i\, 0.\phi_2}$$

since $\phi_1 \in \mathbb{Z}$

$\phi_1 = 0$ (or) 1

$$U^{2^1}|u\rangle = e^{2\pi i\, 0.\phi_2}|u\rangle$$

$$|\psi_4\rangle = \frac{1}{2}\left(|0\rangle + e^{2\pi i 0.\phi_2}|1\rangle\right) \otimes \left(|0\rangle + e^{2\pi i 0.\phi_1\phi_2}|1\rangle\right) \otimes |4\rangle$$

The quantum Fourier transform is a unitary change of basis with the following effect:

$$QFT\left(|\phi_1\rangle|\phi_2\rangle \cdots |\phi_t\rangle\right) =$$

$$= \frac{\left(|0\rangle + e^{2\pi i 0.\phi_t}|1\rangle\right) \otimes \left(|0\rangle + e^{2\pi i 0.\phi_{t-1}\phi_t}|1\rangle\right) \otimes \cdots \otimes \left(|0\rangle + e^{2\pi i 0.\phi_1\phi_2\cdots\phi_t}|1\rangle\right)}{2^{t/2}}$$

Applying the inverse Quantum Fourier transform to the state,

$$(QFT)^{\dagger}\left(\frac{(|0\rangle + e^{2\pi i 0.\phi_2}|1\rangle)\otimes(|0\rangle + e^{2\pi i 0.\phi_1\phi_2}|1\rangle)}{2}\right)\otimes|u\rangle = |\phi_1\rangle\otimes|\phi_2\rangle\otimes|u\rangle$$

→ A measurement in the computational basis therefore gives us ϕ exactly.

General Phase Estimation Algorithm

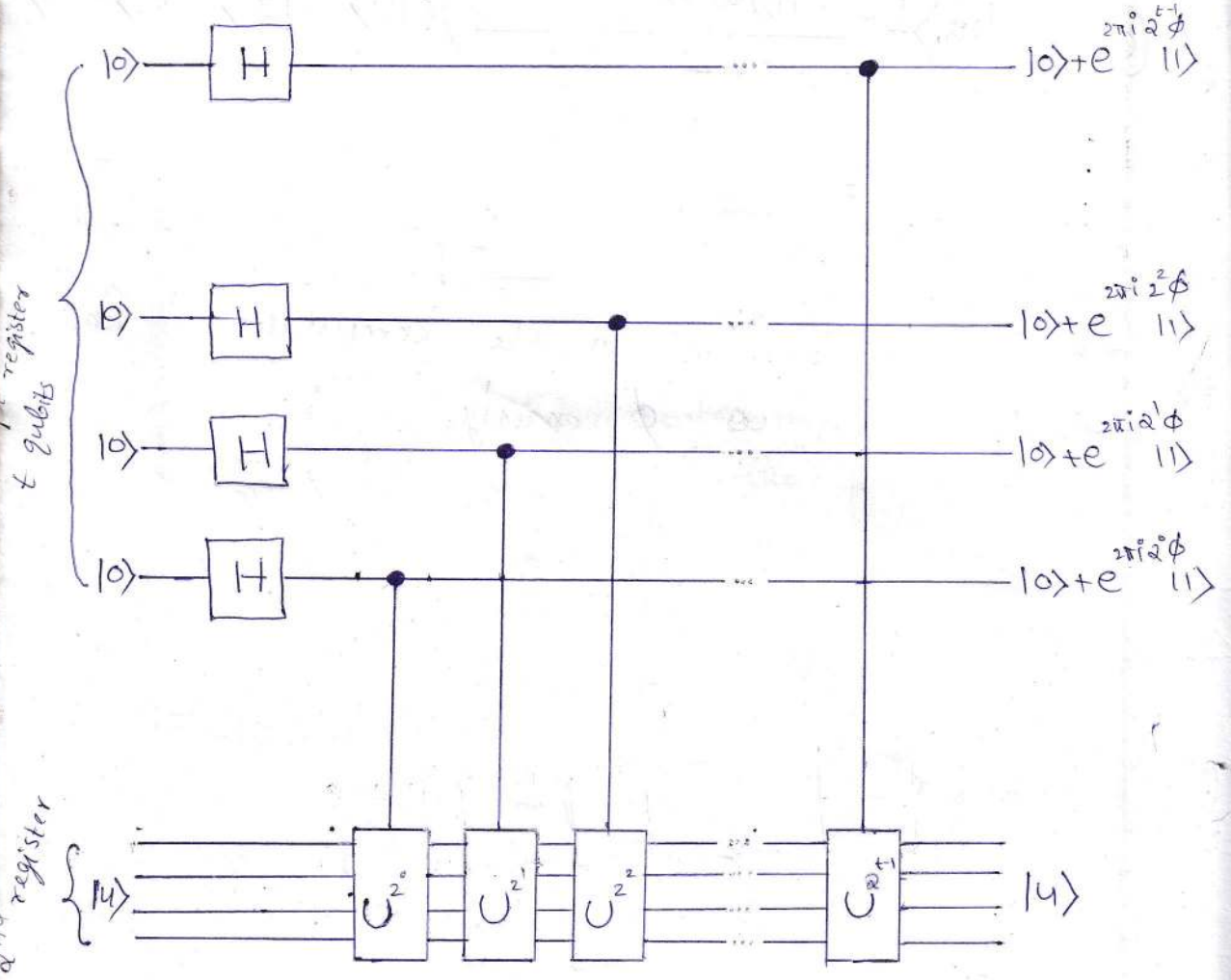


Fig. 5.2 → The 1st stage of the phase estimation procedure. Normalization factors of $1/\sqrt{2}$ have been omitted on the right.

The quantum phase estimation procedure uses two registers. The 1st register contains t qubits initially in the state $|0\rangle$. How we choose t depends on two things: the # of digits of accuracy we wish to have in our estimate for ϕ, and with what probability we wish the phase estimation procedure to be successful.

The 2nd register begins in the state $|u\rangle$ and contains as many qubits as is necessary to store $|u\rangle$.

$U^j|u\rangle = e^{2\pi i \phi}|u\rangle \Longrightarrow U^2|u\rangle = e^{2\pi i (2\phi)}|u\rangle \Longrightarrow U^{2^{t-1}}|u\rangle = e^{2\pi i 2^{t-1}\phi}|u\rangle$

Stage : 1

$$|0\rangle^{\otimes t} \otimes |u\rangle \longrightarrow \frac{1}{2^{t/2}}(|0\rangle+|1\rangle)\otimes(|0\rangle+|1\rangle)\otimes\cdots\cdots\otimes(|0\rangle+|1\rangle)\otimes|u\rangle$$

(after the Hadamards)

$$\longrightarrow \frac{1}{2^{t/2}}(|0\rangle+|1\rangle)\otimes(|0\rangle+|1\rangle)\otimes\cdots\cdots\otimes(|0\rangle+e^{2\pi i 2^0\phi}|1\rangle)\otimes|u\rangle$$

(after the $C(U^{2^0})$)

$$\longrightarrow \frac{1}{2^{t/2}}(|0\rangle+e^{2\pi i 2^{t-1}\phi}|1\rangle)\otimes(|0\rangle+e^{2\pi i 2^{t-2}\phi}|1\rangle)\otimes\cdots\cdots\otimes(|0\rangle+e^{2\pi i 2^0\phi}|1\rangle)\otimes|u\rangle$$

$$= \frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1} e^{2\pi i \phi k}|k\rangle$$

Since,

QFT$|j\rangle$ ↘

Check QFT ↙

$$\frac{1}{2^{t/2}}\sum_{k=0}^{2^t-1} e^{2\pi i j k/2^t}|k\rangle = \frac{(|0\rangle+e^{2\pi i j/2}|1\rangle)(|0\rangle+e^{2\pi i j/2^2}|1\rangle)\cdots\cdots(|0\rangle+e^{2\pi i j/2^t}|1\rangle)}{2^{t/2}}$$

Stage : 2

Stage : 3

Stage : 2

Apply the inverse quantum Fourier transform on the 1st register, which can be done in $O(t^2)$ steps., recovers the state $|2^t\phi\rangle \otimes |u\rangle$

$$2^t\phi = 2^t \left[0.\phi_1\phi_2 \cdots \phi_t\right]$$

$$= 2^t \left[\phi_1 2^{-1} + \phi_2 2^{-2} + \cdots + \phi_t 2^{-t}\right]$$

$$= \phi_1 2^{t-1} + \phi_2 2^{t-2} + \cdots + \phi_{t-1} 2^1 + \phi_t 2^0$$

$$= \phi_1\phi_2 \cdots \phi_t$$

Stage : 3

Read out the state of the 1st register by doing a measurement in the computational basis.

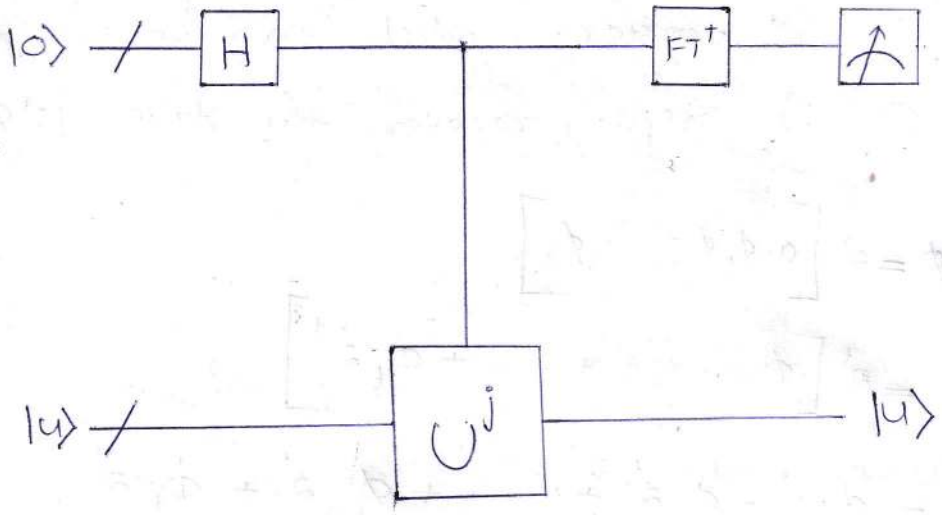


Fig 5-3 Schematic of the overall phase estimation procedure.

The top t qubits (the '/' denotes a bundle of wires) are the 1st register and the bottom qubits are the 2nd register, numbering as many as required to perform U.

$|u\rangle$ is an eigenstate of U with eigenvalue $e^{2\pi i\theta}$.

Suppose,

ϕ may be expressed exactly in t bits, as $\phi = 0.\phi_1\phi_2\cdots\phi_t$. Then

$$e^{2\pi i 2^0\phi} = e^{2\pi i 0.\phi_1\phi_2\cdots\phi_t}$$

$$e^{2\pi i 2^1\phi} = e^{2\pi i \phi_1.\phi_2\cdots\phi_t} = e^{2\pi i 0.\phi_2\cdots\phi_t}$$

$$\vdots$$

$$e^{2\pi i 2^{t-2}\phi} = e^{2\pi i \phi_1\cdots\phi_{t-2}.\phi_{t-1}\phi_t} = e^{2\pi i 0.\phi_{t-1}\phi_t}$$

$$e^{2\pi i 2^{t-1}\phi} = e^{2\pi i \phi_1\cdots\phi_{t-1}.\phi_t} = e^{2\pi i 0.\phi_t}$$

∴ The state resulting from the 1st stage of phase estimation may be rewritten as,

$$\frac{1}{2^{t/2}}\left(|0\rangle + e^{2\pi i 0.\phi_t}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.\phi_{t-1}\phi_t}|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi i 0.\phi_1\cdots\phi_t}|1\rangle\right)\otimes|u\rangle$$

$$\xrightarrow{\text{action } QFT^\dagger} |\phi_1\phi_2\cdots\phi_t\rangle\otimes|u\rangle$$

∴

A measurement in the computational basis therefore gives us ϕ exactly.

⟹ The phase estimation algorithm allows one to estimate the phase ϕ of an eigenvalue of a unitary operator U, given the corresponding eigenvector $|u\rangle$.

An essential feature at the heart of this procedure is the ability of the inverse quantum Fourier transform to perform the transformation,

$$\frac{1}{2^{t/2}} \sum_{j=0}^{2^t-1} e^{2\pi i \phi j} |j\rangle |u\rangle \xrightarrow{(QFT)^\dagger} |\tilde{\phi}\rangle |u\rangle$$

where

$|\tilde{\phi}\rangle$: a state which is a good estimator for ϕ when measured.

Performance & requirements

Let,

b be an integer in the range 0 to $2^t - 1$ such that $\frac{b}{2^t} = 0.b_1 \cdots b_t$ is the best t bit approximation to ϕ which is less than ϕ.

$$b = b_1 b_2 \cdots b_t = b_1 2^{t-1} + b_2 2^{t-2} + \cdots + b_t 2^0$$

$$\frac{b}{2^t} = 0.b_1 b_2 \cdots b_t = b_1 2^{-1} + b_2 2^{-2} + \cdots + b_{t-1} 2^{-t+1} + b_t 2^{-t}$$

$$\phi = 0.\phi_1 \phi_2 \cdots \phi_t \phi_{t+1} \cdots = \phi_1 2^{-1} + \phi_2 2^{-2} + \cdots + \phi_{t-1} 2^{-(t-1)} + \phi_t 2^{-t} + \phi_{t+1} 2^{-(t+1)} + \cdots$$

$$= b_1 2^{-1} + b_2 2^{-2} + \cdots + b_{t-1} 2^{-(t-1)} + \phi_t 2^{-t} + \phi_{t+1} 2^{-(t+1)} + \cdots$$

$$\Longrightarrow \quad 0 \leq \delta = \phi - \frac{b}{2^t} \leq 2^{-t}$$

We need to show that the observation at the end of the phase estimation procedure produces a result which is close to b, and thus enables us to estimate ϕ accurately, with high probability.

Applying the inverse quantum Fourier transform to the final state of the 1st register in the phase estimation procedure, produces the state:

$$\frac{1}{2^t} \sum_{k,l=0}^{2^t-1} e^{-2\pi i k l / 2^t} \; e^{2\pi i \phi k} \; |l\rangle$$

Let α_l be the amplitude of $|(b+l)(\cancel{\text{mod}}\, 2^t)\rangle$,

$$\alpha_l = \frac{1}{2^t} \sum_{k=0}^{2^t-1} \left(e^{2\pi i \left(\phi - \frac{(b+l)}{2^t}\right)} \right)^k$$

$\alpha_l = \alpha_{l+k\times 2^t}$ for any $k \in \mathbb{Z}$

$$(QFT)^\dagger |l\rangle = \frac{1}{2^{t/2}} \sum_{k=0}^{2^t-1} e^{-2\pi i k l / 2^t} |k\rangle$$

$$|\psi\rangle = \frac{1}{2^{t/2}} \sum_{k=0}^{2^t-1} e^{2\pi i \phi k} |k\rangle$$

This is a G.P with $a = 1$ and

$$r = e^{2\pi i(\phi - (b+l)/2^t)}$$

$$S = \frac{a(1-r^n)}{1-r}$$

$$\alpha_l = \frac{1}{2^t}\left(\frac{1 - e^{2\pi i(2^t\phi - (b+l))}}{1 - e^{2\pi i(\phi - (b+l)/2^t)}}\right)$$

$$= \frac{1}{2^t}\left(\frac{1 - e^{2\pi i(2^t\delta - l)}}{1 - e^{2\pi i(\delta - l/2^t)}}\right)$$

$$\delta = \phi - \frac{b}{2^t}$$

Suppose,

the outcome of the final measurement is m.

The probability of obtaining m such that $|m-b| > e$, where e is a positive integer characterizing our desired tolerance to error, is given by, $P(|m-b| > e)$:

Shifting the index l by subtracting $2^{t-1}-1$, i.e.,

$$l \longrightarrow l-(2^{t-1}-1)$$

$$\left[0,\ 2^t-1\right] \longrightarrow \left[-(2^{t-1}-1),\ 2^t-1-(2^{t-1}-1)\right]$$

$$= \left[-2^{t-1}+1,\ 2\cdot 2^{t-1}-1-2^{t-1}+1\right]$$

$$= \left[-2^{t-1}+1,\ 2^{t-1}\right]$$

$$= \left(-2^{t-1},\ 2^{t-1}\right]$$

Q.C Stack 23/11/2021

$$\Longrightarrow \quad -2^{t-1} < l \leq 2^{t-1}$$

$$\therefore P(|m-b|>e) = \sum_{-2^{t-1}<l\leq -(e+1)} |\alpha_l|^2 + \sum_{(e+1)\leq l\leq 2^{t-1}} |\alpha_l|^2$$

where,

α_l is the amplitude of $|(b+l)(\mathrm{mod}\ 2^t)\rangle$,

$$|1 - \exp(i\theta)| = |(1-\cos\theta) - i\sin\theta|$$

$$= |2\sin^2\theta/2 - i\,2\sin\theta/2\cos\theta/2|$$

$$= |2\sin\theta/2\left[\sin\theta/2 - i\cos\theta/2\right]|$$

$$= |2\sin\theta/2(-i)e^{+i\theta/2}| = |2\sin\theta/2|\,|e^{+i\theta/2}|$$

$$= |2\sin\theta/2| \le 2 \quad \text{for any real } \theta.$$

$$\therefore |\alpha_l| = \left|\frac{1}{2^t}\,\frac{1-e^{2\pi i(2^t\delta - l)}}{1-e^{2\pi i(\delta - l/2^t)}}\right| \le \frac{2}{2^t\left|1-e^{2\pi i(\delta - l/2^t)}\right|}$$

$\sin x \geq \frac{2x}{\pi}$ when $0 \leq x \leq \frac{\pi}{2}$

Proof

① $f(x) = \sin x - \frac{2x}{\pi}$ | $0 \leq x \leq \pi/2$

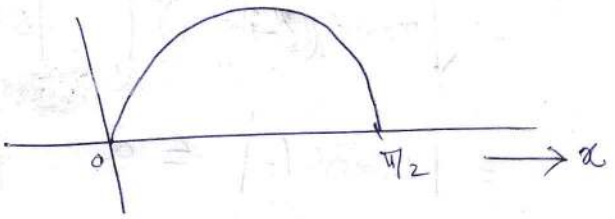
$1 \geq \cos x \geq 0$

$f(0) = 0 - 0 = 0$

$f(\pi/2) = 1 - 1 = 0$

$f'(x) = \cos x - \frac{2}{\pi}$ $\left\{ \begin{array}{l} f'(0) = 1 - \frac{2}{\pi} \geq 0 \\ f'(\pi/2) = -2/\pi < 0 \end{array} \right.$

$f''(x) = -\sin x \leq 0$



$\Rightarrow f(x) = \sin x - \frac{2x}{\pi} \geq 0$ for $0 \leq x \leq \pi/2$

$\therefore \sin x \geq 2x/\pi$

② $f(x) = \frac{\sin x}{x}$, $0 \le x \le \pi/2$

$$f'(x) = \frac{x\cos x - \sin x}{x^2} = \frac{x - \tan x}{x^2 \sec x}$$

$$\tan x = x + \frac{x^3}{3} + \frac{2x^5}{15} + \cdots \Rightarrow \tan x > x$$

$$x - \tan x < 0$$

& $\cos x \ge 0$ &

$\therefore$

$f'(x) < 0$ in $x \in (0, \pi/2)$

$\therefore$ $f(x)$ is strictly decreasing in $(0, \pi/2)$

$f(\pi/2) = \frac{2}{\pi}$ & $\lim_{x\to 0} \frac{\sin x}{x} = \lim_{x\to 0} \cos x = 1$

$\therefore$ $f(x) = \frac{\sin x}{x} \ge \frac{2}{\pi} \Rightarrow \sin x \ge \frac{2x}{\pi}$

$\sin x \ge \frac{x}{\pi/2}$ when $0 \le x \le \pi/2$

$$\sin x \geq \frac{2x}{\pi} \quad \text{when} \quad 0 \leq x \leq \frac{\pi}{2}$$

$$\Rightarrow \sin|x| \geq \frac{2|x|}{\pi} \quad \text{when} \quad -\pi/2 \leq x \leq \pi/2$$

$$\therefore \left|\sin \theta/2\right| \geq \frac{|\theta|}{\pi} \quad \text{when} \quad -\pi/2 \leq \theta/2 \leq \pi/2$$

$$-\pi \leq \theta \leq \pi$$

$$|1 - \exp(i\theta)| = |2\sin\theta/2|\,|e^{-i\theta/2}|$$

$$= 2\left|\sin\theta/2\right| \geq \frac{2|\theta|}{\pi} \quad \text{when} \quad -\pi \leq \theta \leq \pi$$

Now,

when $-2^{t-1}+1 \leq l \leq 2^{t-1}$ & $0 \leq \delta = \phi - \frac{b}{2^t} \leq 2^{-t}$

$$-2^{t-1} \leq -l \leq 2^{t-1} - 1 \quad \& \quad 0 \leq \delta \leq 2^{-t}$$

$$-2^{-1} \leq \frac{-l}{2^t} \leq 2^{-1} - 2^{-t}$$

$$-2^{-1} \leq (\delta - l/2^t) \leq 2^{-1}$$

$$\Rightarrow -\pi \leq 2\pi\left(\delta - l/2^t\right) \leq \pi$$

$$\therefore \left|1 - e^{2\pi i(\delta - l/2^t)}\right| = 2\left|\sin\left[\frac{2\pi(\delta - l/2^t)}{2}\right]\right| \geq 2\,\frac{\left|2\pi(\delta - l/2^t)\right|}{\pi}$$

$$|\alpha_l| \leq \frac{2}{2^t\left|1 - e^{2\pi i(\delta - l/2^t)}\right|} \leq \frac{2}{2^t} \times \frac{\pi}{2\left|2\pi(\delta - l/2^t)\right|}$$

$$\Longrightarrow |\alpha_l| \leq \frac{1}{2^{t+1}\left|\delta - l/2^t\right|} = \frac{1}{2\left|l - 2^t\delta\right|}$$

$$\therefore P(|m-b| > e) \leq \frac{1}{4}\left[\sum_{l=-2^{t-1}+1}^{-(e+1)} \frac{1}{(l-2^t\delta)^2} + \sum_{l=e+1}^{2^{t-1}} \frac{1}{(l-2^t\delta)^2}\right]$$

$$0 \leq \delta = \phi - \frac{b}{2^t} \leq 2^{-t} \longrightarrow 0 \leq 2^t\delta \leq 1$$

When $l < 0$, $(l - 2^t\delta)^2 = (2^t\delta - l)^2 \geq l^2$

$$\Longrightarrow \frac{1}{(l-2^t\delta)^2} \leq \frac{1}{l^2}$$

$0 < l$ &
$-1 \leq -2^t\delta \leq 0$
$\underbrace{\qquad\qquad}$
$-1 < l - 2^t\delta$

When $l > 0$, $l - 2^t\delta \geq l - 1$

$$\Longrightarrow \frac{1}{(l-2^t\delta)^2} \leq \frac{1}{(l-1)^2}$$

$$\therefore P(|m-b|>\epsilon) \le \frac{1}{4}\left[\sum_{l=-2^{t-1}+1}^{-(\epsilon+1)} \frac{1}{l^2} + \sum_{l=\epsilon+1}^{2^{t-1}} \frac{1}{(l-1)^2}\right]$$

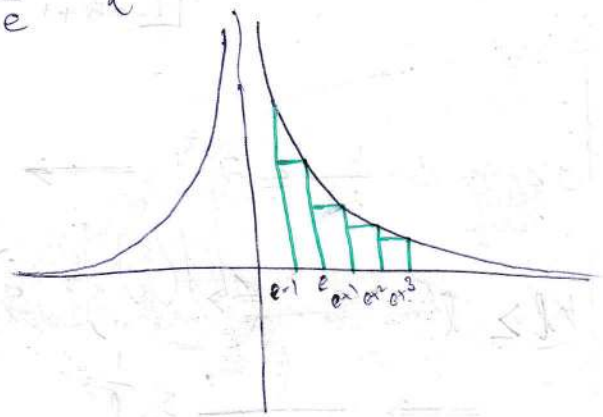
$$\le \frac{1}{4}\left[\sum_{l=-2^{t-1}+1}^{-(\epsilon+1)} \frac{1}{l^2} + \sum_{l=\epsilon}^{2^{t-1}-1} \frac{1}{l^2}\right]$$

$$= \frac{1}{4}\left[\sum_{l=\epsilon+1}^{2^{t-1}-1} \frac{1}{l^2} + \sum_{l=\epsilon}^{2^{t-1}-1} \frac{1}{l^2}\right]$$

$$\le \frac{1}{2}\sum_{l=\epsilon}^{2^{t-1}-1} \frac{1}{l^2}$$

$$= \frac{1}{2}\sum_{l=\epsilon}^{2^{t-1}-1} \frac{\delta l}{l^2} \quad \text{with } \delta l = 1$$

Riemann sum $\Rightarrow$



$\frac{1}{l^2}$ is a decreasing function in the true domain

$$\le \frac{1}{2}\int_{\epsilon-1}^{2^{t-1}-1} \frac{1}{l^2}\, dl$$

$$= \frac{1}{2}\left[\frac{-1}{t}\right]_{e-1}^{2^{t-1}}$$

$$= \frac{1}{2}\left[\frac{-1}{2^{t-1}-1} + \frac{1}{e-1}\right]$$

$$\leq \frac{1}{2(e-1)}$$

$$P(|m-b| < e) \geq 1 - \frac{1}{2(e-1)}$$

Suppose we wish to approximate ϕ to an accuracy 2^{-n}.

i.e., $|m-p| = |2^t(\phi' - \phi)|$

$2^{-n} \longrightarrow |m-p| = 2^t \times 2^{-n} = 2^{t-n}$

$2^{t-n} \longrightarrow e = 2^t(2^{-n} - 2^{-t})$

$= 2^{t-n} - 1$

The probability of obtaining an approximation correct to this accuracy is at least

$$1 - \frac{1}{2(e-1)} = 1 - \frac{1}{2\left(2^{t-n}-2\right)}$$

$$\Longrightarrow P\left(|m-b| < 2^{t-n}-1\right) \leq 1 - \frac{1}{2\left(2^{t-n}-2\right)} = 1-\epsilon$$

$$\epsilon = \frac{1}{2\left(2^{t-n}-2\right)} \Longrightarrow 2^{t-n} - 2 = \frac{1}{2\epsilon}$$

$$2^{t-n} = 2 + \frac{1}{2\epsilon} \Longrightarrow t-n = \log_2\left(2+\frac{1}{2\epsilon}\right)$$

$$\Longrightarrow t = n + \log_2\left(2+\frac{1}{2\epsilon}\right)$$

∴ To successfully obtain ϕ accurate to n bits with probability of success atleast $1-\epsilon$ we choose,

$$\boxed{t = n + \log_2\left(2+\frac{1}{2\epsilon}\right)} \quad \text{—— } 5.35$$

By making use of $t = n + p$ qubits in the phase estimation algorithm

The probability of obtaining an approximation correct to this accuracy is at least

$$1 - \frac{1}{2(e-1)} = 1 - \frac{1}{2\left(2^{t-n} - 2\right)}$$

$$\Rightarrow P\left(|m-b| < 2^{t-n} - 1\right) \leq 1 - \frac{1}{2\left(2^{t-n}-2\right)} = 1 - \epsilon$$

$$\epsilon = \frac{1}{2\left(2^{t-n} - 2\right)} \Longrightarrow 2^{t-n} - 2 = \frac{1}{2\epsilon}$$

$$2^{t-n} = 2 + \frac{1}{2\epsilon} \Longrightarrow t - n = \log_2\left(2 + \frac{1}{2\epsilon}\right)$$

$$\Rightarrow t = n + \log_2\left(2 + \frac{1}{2\epsilon}\right)$$

∴ To successfully obtain ϕ accurate to n bits with probability of success atleast $1-\epsilon$ we choose,

$$\boxed{t = n + \log_2\left(2 + \frac{1}{2\epsilon}\right)} \quad \text{—— } 5.35$$

* In order to make use of the phase estimation algorithm, we need to be able to prepare an eigenstate $|u\rangle$ of U.

What if we do not know how to prepare such an eigenstate ?

Suppose we prepare some other state $|\psi\rangle$ in place of $|u\rangle$. Expanding $|\psi\rangle$ in terms of eigenstates $|u\rangle$ of U gives $|\psi\rangle = \sum_u c_u |u\rangle$.

Suppose,

$$U|u\rangle = e^{2\pi i \phi_u}|u\rangle$$

Intuitively, the result of running the phase estimation algorithm will be to give as output a state close to $\sum_u c_u |\tilde{\phi}_u\rangle|u\rangle$ where

$\tilde{\phi}_u$ is a pretty good approximation to the phase ϕ_u.

$\Rightarrow$ Reading out the 1st register will give us a good approximation to ϕ_u, where u is chosen at random with probability $|c_u|^2$.

This procedure allows us to avoid preparing a (possibly unknown) eigenstate, at the cost of introducing some additional randomness into the algorithm.

Ex: 5.8 Suppose the phase estimation algorithm takes the state $|0\rangle|u\rangle$ to the state $|\tilde{\phi}_u\rangle|u\rangle$, so that given the input $|0\rangle\left(\sum_u c_u|u\rangle\right)$, the algorithm outputs $\sum_u c_u|\tilde{\phi}_u\rangle|u\rangle$.

Show that if t is chosen according to Eq. 5.35:

$$t = n + \log_2\left(2 + \frac{1}{2\epsilon}\right)$$

then the probability for measuring ϕ_u accurate to n bits at the conclusion of the phase estimation algorithm is at least $|c_u|^2(1-\epsilon)$.

Ans: The probability of getting the state $|u\rangle$ measured is : $|c_u|^2$

The measurement succeeds with probability $1-\epsilon$.

$\therefore$

The probability for measuring ϕ_u accurate to n bits at the conclusion of the phase estimation algorithm is atleast $|c_u|^2(1-\epsilon)$.

□ Algorithm: Quantum Phase Estimation

Inputs: ① A black box which performs a controlled-U^j operations, for integer j,

② an eigenstate $|u\rangle$ of U with eigenvalue $e^{2\pi i \phi_u}$

③ $t = n + \log_2\left(2 + \frac{1}{2\epsilon}\right)$ qubits initialized to $|0\rangle$.

Outputs: An n-bit approximation $\tilde{\phi}_u$ to ϕ_u.

Runtime: $O(t^2)$ operations and one call to controlled U^j black box. Succeeds with probability at least $1-\epsilon$.

Procedure :

① $|0\rangle|u\rangle$ initial state

② $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle|u\rangle$ create superposition

③ $\rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} |j\rangle U^j|u\rangle$ apply Black box

$= \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} e^{2\pi i j \phi_u} |j\rangle|u\rangle$ result of Black box

④ $\rightarrow |\tilde{\phi}_u\rangle|u\rangle$ apply inverse Fourier transform

⑤ $\rightarrow \phi_u$ measure 1st register.

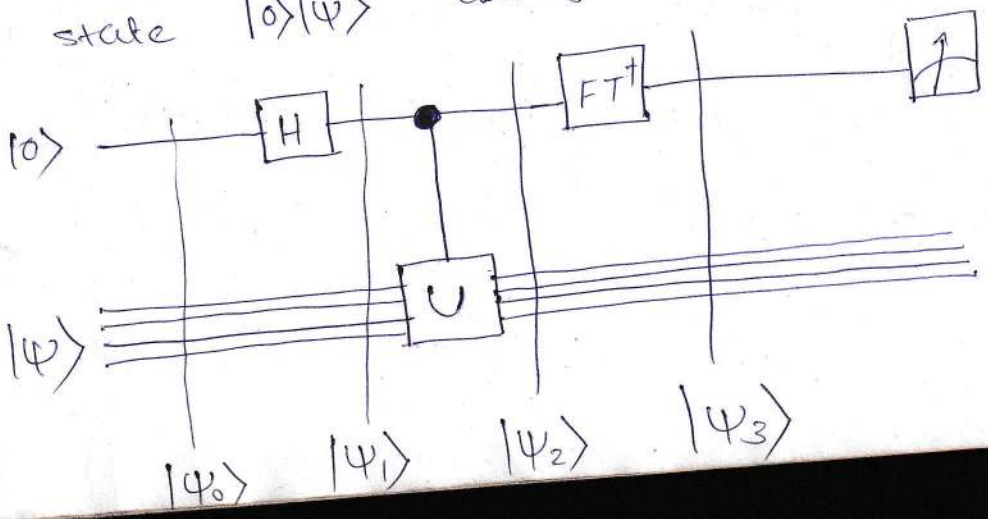
Ex: 5.9 Let U be a unitary transform with eigenvalues ± 1, which acts on a state $|\psi\rangle$. Using the phase estimation procedure, construct a quantum circuit to collapse $|\psi\rangle$ into one or the other of the two eigenspaces of U, giving also a classical indicator as to which space the final state is in.

Compare results with Ex: 4.34.

Ans:

Let $|+1\rangle$ and $|-1\rangle$ be the eigenstates of U with eigenvalues $+1$ and -1, respectively.

Applying the phase estimation procedure to the state $|0\rangle|\psi\rangle$ changes



$$|\psi_0\rangle = |0\rangle|\psi\rangle = \sum_{j=-1,+1} c_j |0\rangle|j\rangle$$

$$|\psi_1\rangle = \sum_{j=-1,+1} c_j \frac{1}{\sqrt{2}} \sum_{k=0,1} |k\rangle|j\rangle$$

$$|\psi_2\rangle = \sum_{j=-1,+1} c_j \frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i \phi} |1\rangle\right)|j\rangle$$

$$\phi_j = \begin{cases} 0 = 0.0 \\ \frac{1}{2} = 0.1 \end{cases}$$

$$\phi = 0.\phi_j$$

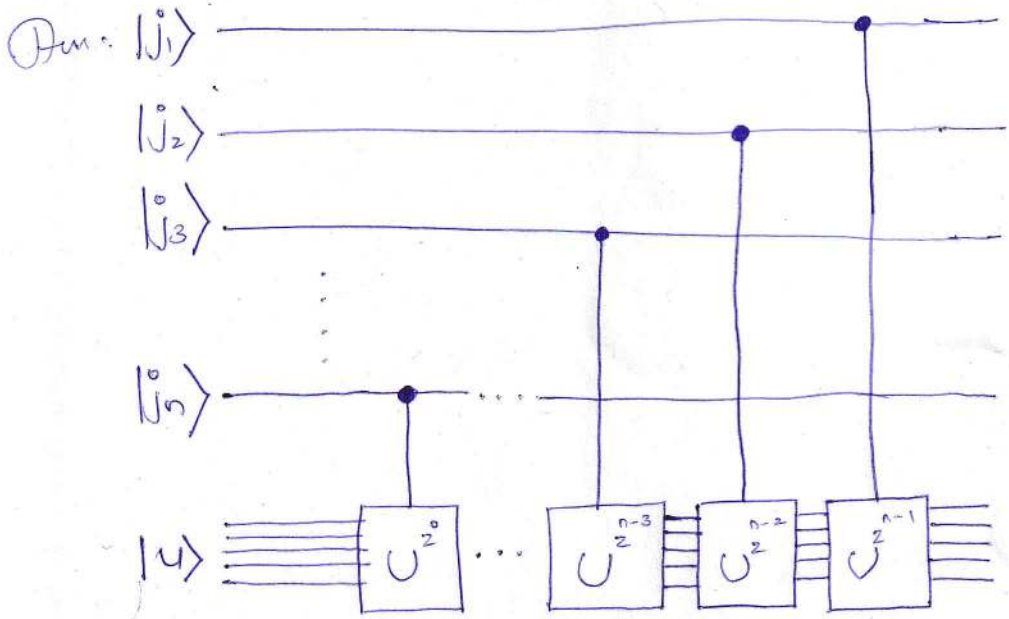
$$|\psi_3\rangle = \sum_{j=-1,+1} c_j |\phi_j\rangle|j\rangle$$

$\Rightarrow$ By measuring the 1st qubit, the 2nd qubit collapses into one of the eigenstates of U which is $|-1\rangle$ or $|+1\rangle$.

When measuring result is 0, the final state of the 2nd qubit is $|+1\rangle$ and vice versa.

Ex: 5.7 Show that the effect of the sequence of controlled-U operations in the phase estimation procedure (apto IQFT) is to take the state $|j\rangle|u\rangle$ to $|j\rangle U^j|u\rangle$. This does not depend on $|u\rangle$ being an eigenstate of U.

Ans.



$$j = j_1 j_2 \cdots j_n$$

$$|j\rangle|u\rangle \longrightarrow |j\rangle U^{j_n 2^0} \cdots U^{j_3 2^{n-3}} U^{j_2 2^{n-2}} U^{j_1 2^{n-1}} |u\rangle$$

$$= |j\rangle U^{j_1 2^{n-1}} U^{j_2 2^{n-2}} U^{j_3 2^{n-3}} \cdots U^{j_n 2^0} |u\rangle$$

$$= |j\rangle U^{j_1 j_2 \cdots j_n} |u\rangle = |j\rangle U^j |u\rangle$$

papergrid®

Reflects You

Do not wait to strike till the iron is hot;
but make it hot by striking.

soorajss1729@gmail.com

INDEX

(7)

Name SOORAJ. S. Std Sec

Roll No. Subject School/College

Sl. No.	Date	Title	Page No.	Teacher Sign/ Remarks
		QUANTUM COMPUTATION & QUANTUM INFORMATION		
		– Nielsen & Chuang		