FAST, CS-4084

Lecture Notes of Quantum Computing

Dr. Faisal Aslam

Faisal Aslam

August 2023

Contents

1 Dirac's Notation and Tensor Product

Bra-ket notation, also known as Dirac notation, is a mathematical notation used in quantum computing and quantum mechanics to represent vectors and matrices. It was introduced by an amazing physicist Paul Dirac and has become a fundamental tool for expressing quantum concepts concisely and efficiently, thus saving time and space in mathematical descriptions.

1.1 Ket Notation

The ket $|0\rangle$ represents a 2-dimensional vector with a value of 1 in its 0th location and 0 in the other location:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{1.1}$$

Similarly, the ket $|1\rangle$ is a 2-dimensional vector with a value of 1 in its 1st location and 0 in the other location:

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{1.2}$$

Together, $|0\rangle$ and $|1\rangle$ form the standard **basis** for a 2D **vector space**. This means that any 2D vector can be expressed as a linear combination of these basis vectors: $\begin{pmatrix} a \\ b \end{pmatrix} = a\,|0\rangle + b\,|1\rangle$, where a and b are scalar coefficients.

1.1.1 Example

Let's write the vector $\begin{pmatrix} i\sqrt{\frac{2}{3}} \\ -i\frac{1}{\sqrt{3}} \end{pmatrix}$ using the standard basis.

Solution

$$\begin{pmatrix} i\sqrt{\frac{2}{3}} \\ -i\frac{1}{\sqrt{3}} \end{pmatrix} = i\sqrt{\frac{2}{3}}\,|0\rangle - i\frac{1}{\sqrt{3}}\,|1\rangle$$

It's important to note that in the standard basis, each vector has only one nonzero entry while the rest of the entries are zeros. The aforementioned concept extends beyond 2D vectors through the use of the tensor product. Let's quickly learn about tensor product.

1.2 Tensor product

Tensor products are a world in their own. In this context, our emphasis is on utilizing them to construct larger matrices from smaller ones.

Example

Given the following two matrices A and B. Find their tensor produce. That is find $A \otimes B$.

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

Solution

$$A \otimes B = \begin{pmatrix} 0 \times B & -1 \times B \\ 1 \times B & 0 \times B \end{pmatrix} = \begin{pmatrix} 0 & 0 & -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ 0 & 0 & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 & 0 \end{pmatrix}$$

Properties

- Associative: $(A \otimes B) \otimes C = A \otimes (B \otimes C)$
- $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$
- Distributed: $A \otimes (B + C) = (A \otimes B) + (A \otimes C)$
- Scalar floats freely: $(aA) \otimes B = a(A \otimes B) = A \otimes (aB)$

1.3 Extending Ket Notation

By utilizing the tensor product, we can build upon the previous definitions of $|0\rangle$ and $|1\rangle$. Put simply, for any i and j belonging to the set $\{0, 1\}$, the notation $|ij\rangle = |i\rangle \otimes |j\rangle$ represents a vector. This vector has $2^2 = 4$ elements, where the element at the ij-th location has a value of 1, while the rest of the elements are set to zero. For example, $|10\rangle = |1\rangle \otimes |0\rangle$ has a 1 at the 2nd location, with the remaining entries being zeros.

$$\begin{aligned} |10\rangle &= |1\rangle \otimes |0\rangle \\ &= \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} 0\,|0\rangle \\ 1\,|0\rangle \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \end{aligned}$$

Using this extended notation, we can create a standard basis for 4D vectors: $\Big\{ |00\rangle, |01\rangle, |10\rangle, |11\rangle \Big\}$. Thus, any 4D vector can be expressed as a linear combination of these basis vectors:

$$\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle$$

where a, b, c, and d are scalar coefficients.

1.3.1 Example

Represent $\begin{pmatrix} \frac{i}{\sqrt{3}} \\ 0 \\ \frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$ in Bra-Ket notation.

Solution

$$\begin{pmatrix} \frac{i}{\sqrt{3}} \\ 0 \\ \frac{1}{\sqrt{6}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{i}{\sqrt{3}}\,|00\rangle + \frac{1}{\sqrt{6}}\,|10\rangle + \frac{1}{\sqrt{2}}\,|11\rangle$$

Similarly, $|0110\rangle$ has $2^4 = 16$ elements, with its 6th element being 1 while the rest of the elements are zeros.

1.4 Bra Notation

Ket notation is used to represent column vectors, whereas Bra notation represents row vectors. Formally, $\langle\psi| = |\psi\rangle^\dagger$, where the † represents the conjugate transpose (also known as the Hermitian transpose) operation. This operation involves taking the transpose of the vector, making it a row vector, and changing the sign of all iotas.

1.4.1 Example

Convert $|\psi\rangle = \begin{pmatrix} i\sqrt{\frac{2}{3}} \\ -i\frac{1}{\sqrt{3}} \end{pmatrix}$ to Bra notation.

Solution

$$\begin{aligned}\langle\psi| &= |\psi\rangle^\dagger \\ &= \begin{pmatrix} -i\sqrt{\frac{2}{3}} & i\frac{1}{\sqrt{3}} \end{pmatrix} \\ &= -i\sqrt{\frac{2}{3}}\,\langle 0| + i\frac{1}{\sqrt{3}}\,\langle 1|\end{aligned}$$

We can now represent any row vector using a basis in Bra notation. For instance, the basis of $\left\{\langle 00|, \langle 01|, \langle 10|, \langle 11|\right\}$ can be used to represent the vector $\begin{bmatrix} i\sqrt{\frac{2}{3}} & 0 & 0 & -\frac{1}{\sqrt{3}} \end{bmatrix} = i\sqrt{\frac{2}{3}}\,\langle 00| - \frac{1}{\sqrt{3}}\,\langle 11|$.

1.5 Matrices in Bra-Ket Notation

Matrices can be conveniently represented using Bra-Ket notation. Let's take a look at an example, specifically $|0\rangle\langle 0|$:

$$\begin{aligned}|0\rangle\langle 0| &= \begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\end{aligned}$$

Observe that $|0\rangle\langle 0|$ yields a 2×2 matrix. In this matrix, the row and column indexed by 0 contain the value 1, while all other entries are zeros. Similarly, for any i and j the matrix $|i\rangle\langle j|$ will have a 1 at the intersection of the i-th row and j-th column, with all other elements being zeros. Let's see another example, to make it more clear. The matrix $|01\rangle\langle 10|$ will be of dimensions $2^2 \times 2^2$ and will have a 1 at the intersection of $(01)_2 = (1)_{10}$-th row and $(10)_2 = (2)_{10}$-th column. That is:

$$|01\rangle\langle 10| = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & \mathbf{1} & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

We can create basis to represent matrices, just like vector. For instance, basis to represent 2 matrices is $\Big\{ |0\rangle\langle 0|, |0\rangle\langle 1|, |1\rangle\langle 0|, |1\rangle\langle 1| \Big\}$ and basis to represent 4 matrices is $\Big\{ |00\rangle\langle 00|, |00\rangle\langle 01|, |00\rangle\langle 10|, |00\rangle\langle 11|, ...\Big\}$.

1.5.1 Example

Represent the matrix $\begin{pmatrix} 0 & 7 & 0 & 0 \\ 1 & 0 & 0 & 5 \\ 0 & 0 & 9 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ using Bra-Ket notation.

Solution: $7|00\rangle\langle 01| + |01\rangle\langle 00| + 5|01\rangle\langle 11| + 9|10\rangle\langle 10|$

1.6 Inner Product

The inner product of $|\psi\rangle$ and $|\phi\rangle$, also called the BraKet (it's fun to see it coming together), is mathematically represented as $\langle\psi|\phi\rangle = |\psi\rangle^{\dagger} \times |\phi\rangle$.

1.6.1 Example

Find the inner product of $|\psi\rangle = \begin{pmatrix} i\sqrt{\frac{2}{3}} \\ \frac{-i}{\sqrt{3}} \end{pmatrix}$ and $|\phi\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{pmatrix}$.

Solution

$$\begin{aligned} \langle\psi|\phi\rangle &= |\psi\rangle^{\dagger} \times |\phi\rangle \\ &= -i\sqrt{\frac{2}{3}} \times \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{3}} \times \frac{i}{\sqrt{2}} \\ &= \frac{-i}{\sqrt{3}} - \frac{1}{\sqrt{6}} \end{aligned}$$

In the above example, please carefully note how the signs of the iotas are changed when computing the Bra of $|\psi\rangle$, whereas the sign remains the same for $|\phi\rangle$.

1.7 Magnitude (Euclidean Norm)

The Euclidean Norm of a vector $|\psi\rangle$ is defined as $\| \, |\psi\rangle \, \| = \sqrt{\langle\psi|\psi\rangle}$.

1.7.1 Example

Find the norm of $|\psi\rangle = \begin{pmatrix} i\sqrt{\frac{2}{3}} \\ \frac{-i}{\sqrt{3}} \end{pmatrix}$.

Solution

$$\begin{aligned} \| \, |\psi\rangle \, \| &= \sqrt{\langle\psi|\psi\rangle} \\ &= \sqrt{-i\sqrt{\frac{2}{3}} \times i\sqrt{\frac{2}{3}} + \frac{i}{\sqrt{3}} \times \frac{-i}{\sqrt{3}}} \\ &= \sqrt{\frac{2}{3} + \frac{1}{3}} \\ &= 1 \end{aligned}$$

In the above example, please carefully note how the signs of the iotas are handled.

1.8 Unit Vector

A vector $|\psi\rangle$ is called a unit (or normalized) vector if its norm is 1: $\| \, |\psi\rangle \, \| = 1$.

For instance, the vector $|\psi\rangle = \begin{pmatrix} i\sqrt{\frac{2}{3}} \\ \frac{-i}{\sqrt{3}} \end{pmatrix}$ is a unit vector.

1.9 Normalization

An arbitrary vector $|\psi\rangle$ can be convert into a unit vector by dividing it from its norm: $\frac{|\psi\rangle}{\||\psi\rangle\|}$.

1.9.1 Example

Convert vector $|\psi\rangle = \begin{pmatrix} 3i \\ 4 \end{pmatrix}$ to a unit vector.

Solution Let's first calculate its norm: $\| \, |\psi\rangle \, \| = \sqrt{-3i \times 3i + 4 \times 4} = \sqrt{9 + 16} = 5$. Thus, the equivalent unit vector is: $\frac{|\psi\rangle}{\||\psi\rangle\|} = \begin{pmatrix} \frac{3i}{5} \\ \frac{4}{5} \end{pmatrix}$

1.10 Orthogonal Vectors

A set of vectors is called orthogonal to each other if the inner product of every pair in the set is zero. For example, $|\psi\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$ and $|\phi\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$ are orthogonal, as $\langle\psi|\phi\rangle = 0$.

1.11 Orthonormal Vectors

A set of vectors is called orthonormal if two conditions are met: i) the inner product of each pair is zero, and ii) each vector is a unit vector. Mathematically,

$$\langle\psi|\phi\rangle = \begin{cases} 0 & |\psi\rangle \neq |\phi\rangle \\ 1 & |\psi\rangle = |\phi\rangle \end{cases}$$

2 Qubits and their Measurements

2.1 Qubits

In classical computing, the fundamental unit of information is represented by a binary digit, commonly referred to as a **bit**. A bit inherently carries one of two values, either 0 or 1. Conversely, in quantum computers, the elementary unit of information is known as a **qubit**. Unlike a classical bit, a qubit can encode a binary 0 with a probability of p and a binary 1 with a probability of $1-p$, existing in both states simultaneously. Mathematically, a qubit $|\psi\rangle$ is define as:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

where $\alpha, \beta \in \mathbb{C}$ and $\|\,|\psi\rangle\,\| = 1$. The probability of measuring 0 is $|\alpha|^2 = \alpha^*\alpha$ and the probability of measuring 1 is $|\beta|^2 = \beta^*\beta$. Here $*$ represents conjugate, implying the sign of imaginary terms change.

2.1.1 Example

a) Verify that $|\psi\rangle = \frac{i}{\sqrt{3}}\,|0\rangle + \sqrt{\frac{2}{3}}\,|1\rangle$ is a valid qubit. **b)** What is the probability of measuring 0?

Solution: **a)** To verify we have to check if above vector is a unit vector. $\|\,|\psi\rangle\,\| = \frac{-i}{\sqrt{3}} \times \frac{i}{\sqrt{3}} + \sqrt{\frac{2}{3}} \times \sqrt{\frac{2}{3}} = 1$.

b) The probability of measuring 0 is $|\frac{i}{\sqrt{3}}|^2 = \frac{-i}{\sqrt{3}} \times \frac{i}{\sqrt{3}} = \frac{1}{3}$

2.1.2 Superposition vs. Pure State

When the probability of measuring either 0 or 1 is less than 1 (certainty), we classify our qubit as being in a state of **superposition** or quantum state. Conversely, if we have a probability of 1 to measure either 0 or 1, we refer to our qubit as being in a state of **pure state** or classical state.

Multiple qubits The same concept of single qubits can be extended to a register containing more than one qubits. To represent n-qubits you need a vector of 2^n dimensions. That vector contains complex number and it must be a unit vector. For example the following is a valid 2-qubits register: $|\psi\rangle = \frac{i}{\sqrt{3}}\,|00\rangle + \frac{1}{\sqrt{6}}\,|01\rangle + \frac{1}{\sqrt{2}}\,|11\rangle$ as it is a unit vector.

2.2 Physics of qubits

Qubits, leverage the principles of quantum mechanics to represent and manipulate information in a fundamentally different way. In quantum mechanics, qubits can exist in a superposition of states, allowing them to represent both 0 and 1 simultaneously. This property is what gives quantum computers their potential for exponential computational power in certain tasks.

There are several physical systems that can be used to create qubits, and each system has its own unique properties and challenges. Here are a few common implementations of qubits:

Electrons in Superconducting Circuits: Superconducting qubits are among the most widely used qubit implementations. These qubits are created using tiny circuits made of superconducting materials. The two main types of superconducting qubits are the transmon qubit and the flux qubit. They rely on the manipulation of the quantum properties of Cooper pairs of electrons.

Photons: Qubits can also be implemented using single photons, which are particles of light. The polarization or path of these photons can be used to encode quantum information.

Trapped Ions: Trapped ion qubits use individual ions, typically trapped in electromagnetic fields, as qubits. The internal energy levels of these ions serve as the qubit's quantum states, which can be manipulated using lasers and other electromagnetic fields.

Nitrogen-Vacancy Centers in Diamonds: Qubits can also be created using defects in diamond crystals, known as nitrogen-vacancy (NV) centers. These defects can trap an unpaired electron, and the spin states of this electron serve as the qubit's states. NV centers can be manipulated and read out using lasers.

Topological Qubits: These are qubits that are more robust against certain types of errors due to their inherent topological properties. They can be realized in various physical systems, such as certain types of exotic materials.

Creating and maintaining qubits is a significant challenge due to the delicate nature of quantum states. They are susceptible to environmental interference and decoherence, which can cause the quantum information to be lost. Quantum error correction techniques are being developed to address these challenges and enable reliable quantum computation.

2.3 Measuring qubits

The concept of measuring qubits finds its inspiration in the wave-particle duality demonstrated by the famous two-slit experiment. While the intricacies of physics lie beyond the scope of this course, let's satisfy our curiosity by delving into its foundational principles.

In the two-slit experiment, which showcases the strange behavior of quantum particles, we encounter the notion of wave-particle duality. Though the specifics of physics aren't covered here, a basic understanding can still be enlightening.

2.3.1 Physics of Measurements

The two-slit experiment and the wave-particle duality are two fundamental concepts in quantum mechanics that highlight the puzzling and counterintuitive nature of particles at the quantum level.

Two-Slit Experiment The two-slit experiment is a classic demonstration of the wave-like behavior of particles and the interference phenomenon. It involves sending particles, such as electrons or photons (particles of light), through two closely spaced slits in a barrier and observing the pattern that forms on a screen placed behind the slits.

When classical particles like marbles are sent through two slits, they create two separate bands on the screen, each corresponding to a slit. However, when quantum particles are used, something very different happens. Even when particles are sent through the slits one at a time, over time they accumulate on the screen in a pattern that resembles an interference pattern of alternating light and dark bands. This pattern suggests that the particles are behaving like waves, exhibiting interference between the waves that pass through the two slits.

Wave-Particle Duality Wave-particle duality is the concept that particles, such as electrons and photons, can exhibit both wave-like and particle-like properties depending on how they are observed or measured. This duality challenges our classical intuition because we are used to thinking of objects as either waves or particles, not both.

In the context of the two-slit experiment, wave-particle duality becomes evident. When particles are not observed and not measured, they seem to exhibit wave-like behavior, resulting in interference patterns. However, when a measurement is made to determine which slit a particle passes through, the interference pattern disappears, and the particles behave more like localized particles, forming two distinct bands on the screen.

Wave-particle duality suggests that at the quantum level, particles do not have well-defined properties like position or momentum until they are measured. Instead, they exist in a superposition of possible states, where their behavior is described by a wave-function. The wave-function encodes the probability distribution of the different outcomes of measurements. When a measurement is made, the wave-function collapses to one of the possible outcomes, revealing the particle's state.

This duality and the behavior observed in the two-slit experiment are fundamental aspects of quantum mechanics and have been verified through numerous experiments. The phenomenon challenges our classical intuition and requires a shift in how we conceptualize the behavior of particles at the quantum level.

2.4 Full Measurement and State Transition

When a qubit in superposition is measured, the act of measurement collapses it into a pure state. Let's clarify these concepts through a few illustrative examples.

2.4.1 Example: Measurement of a Single Qubit

Consider a qubit in the superposition state $|\psi\rangle = \frac{i}{\sqrt{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle$. If we measure the qubit and obtain the result 0 what will be our resultant state?

Solution The probability of measuring 0 is $\frac{1}{3}$. After the measurement, the qubit transitions to a pure state, becoming $|\psi\rangle = |0\rangle$. Consequently, any subsequent measurements will yield 0 with certainty.

2.4.2 Example: Measurement of Multiple Qubits

Now, let's take two qubits in the superposition state $|\psi\rangle = \frac{i}{\sqrt{3}}|00\rangle + \frac{1}{\sqrt{6}}|01\rangle + \frac{1}{\sqrt{2}}|11\rangle$. If we measure and obtain the result 01 with what probability and what will be the resultant state?

Solution The probability of measuring 01 is $\frac{1}{6}$. After the measurement, the qubit transitions into a pure state, specifically $|\psi\rangle = |01\rangle$. As a consequence, all subsequent measurements will yield 01 with certainty.

2.5 Partial Measurement and State Evolution

When dealing with a register of multiple qubits, it's possible to selectively measure only a subset of them. This measurement causes the state of the measured qubits to transition from superposition to a pure state, while the remaining qubits maintain their state in superposition. To illuminate this concept, let's explore an illustrative examples.

2.5.1 Illustrative Example

Let's consider the qubit state $|\psi\rangle = \frac{i}{\sqrt{3}}|00\rangle + \frac{1}{\sqrt{6}}|01\rangle + \frac{1}{\sqrt{2}}|11\rangle$. We'll create a table showcasing the probabilities and resultant states when a) the first qubit is measured as 0, and b) the second qubit is measured as 1.

Measurement	**Probability of Measurement**	**Resultant State**
First qubit=0	$\lvert\frac{i}{\sqrt{3}}\rvert^2 + \lvert\frac{1}{\sqrt{6}}\rvert^2 = \frac{1}{2}$	$i\sqrt{\frac{2}{3}}\,\lvert 00\rangle + \frac{1}{\sqrt{3}}\,\lvert 01\rangle$
Second qubit=1	$\lvert\frac{1}{\sqrt{6}}\rvert^2 + \lvert\frac{1}{\sqrt{2}}\rvert^2 = \frac{2}{3}$	$\frac{1}{2}\,\lvert 01\rangle + \frac{\sqrt{3}}{2}\,\lvert 11\rangle$

Pay close attention: when calculating the resultant state, it's crucial to re-normalize our qubit to ensure that the norm of the resulting state remains equal to 1.

2.6 Measuring qubits in non-standard basis

Up until now, our qubits have been measured using the standard basis. However, in quantum computing, our basis may contains any set of orthonormal vectors. To measure qubits in a non-standard orthonormal basis—let's denote it as $\left\{ \lvert\gamma\rangle, \lvert\delta\rangle \right\}$—a two-step process is involved. Firstly, one needs to transform the qubit into this specific basis. After this transformation, the conventional measurement rule we've discussed earlier can be applied.

The formula for transforming qubits $\lvert\psi\rangle$ to the orthonormal basis is expressed as $\langle\gamma|\psi\rangle\,\lvert\gamma\rangle + \langle\delta|\psi\rangle\,\lvert\delta\rangle$. The probability of measuring $\lvert\gamma\rangle$ is $\lvert\,\langle\gamma|\psi\rangle\,\rvert^2$, and the probability of measuring $\lvert\delta\rangle$ is $\lvert\,\langle\delta|\psi\rangle\,\rvert^2$.

To clarify this concept, let's explore an illustrative example.

2.6.1 Illustrative Example

One well-known orthonormal basis is $\left\{ \lvert+\rangle, \lvert-\rangle \right\}$, where $\lvert+\rangle = \frac{1}{\sqrt{2}}\lvert 0\rangle + \frac{1}{\sqrt{2}}\lvert 1\rangle$ and $\lvert-\rangle = \frac{1}{\sqrt{2}}\lvert 0\rangle - \frac{1}{\sqrt{2}}\lvert 1\rangle$. Let's explore how to measure the qubit $\lvert\psi\rangle = \frac{i}{\sqrt{3}}\lvert 0\rangle + \sqrt{\frac{2}{3}}\lvert 1\rangle$ in this basis. Essentially, we want to find the probabilities of measuring $\lvert+\rangle$ and $\lvert-\rangle$, rather than measuring $\lvert 0\rangle$ and $\lvert 1\rangle$.

To achieve this, we first transform our qubit into the $\left\{ \lvert+\rangle, \lvert-\rangle \right\}$ basis using the formula $\lvert\psi\rangle = \langle+|\psi\rangle\,\lvert+\rangle + \langle-|\psi\rangle\,\lvert-\rangle = (\frac{i}{\sqrt{6}} + \frac{1}{\sqrt{3}})\,\lvert+\rangle + (\frac{i}{\sqrt{6}} - \frac{1}{\sqrt{3}})\,\lvert-\rangle$. With this transformation, we can calculate the probability of measuring $\lvert+\rangle$, which is $\lvert\frac{i}{\sqrt{6}} + \frac{1}{\sqrt{3}}\rvert^2 = \frac{1}{2}$. Similarly, the probability of measuring $\lvert-\rangle$ is also $\frac{1}{2}$.

3 Period Finding Algorithm

3.1 Problem definition

Given a function $f : \{0,1\}^n \longrightarrow \{0,1\}^n$, finds its period r such that $f(x) = f(x + kr)$ for every number k.

3.2 Background

Period finding is based on two of the Fourier transform properties. These properties are described in detailed in Section **??**, and repeated briefly below.

1. In case, the period of a function $g : \{0,1\}^n \longrightarrow \{0,1\}^n$ is r then the period of its Fourier transform $F_{2^n} g = \hat{g}$ will be $\frac{N}{r}$, where $N = 2^n$.
2. In case two sets of qubits are same but have different phases shifts then by measuring them their phase difference cannot be determined. However, by applying a Fourier transform we can attained information about their prior phase shift. Example, the two set of qubits $\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$ and $\begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$ are same but has different phase shifts. By measuring them one cannot know what is their phase shift. However, by applying Fourier transform we can differentiate them. That is $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = |0\rangle$ and $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} = |1\rangle$

3.3 Circuit diagram

The circuit of period finding algorithm is shown in Figure 3.1. It is similar to Simon's algorithm circuit diagram Figure **??**. The apparent two differences are that the first n-qubits are applied Fourier transformations twice once before B_f and other after it, instead of $H^{\otimes n}$ transformations. However, as $F_{2^n} = H^{\otimes n}$ when the data is $|0^n\rangle$, thus, actually the circuit differ from Simon's circuit only at a single block when after B_f Fourier transform is used instead of $H^{\otimes n}$.

3.4 Working

The working of Phase estimation is also similar to Simon's algorithm as outline below:

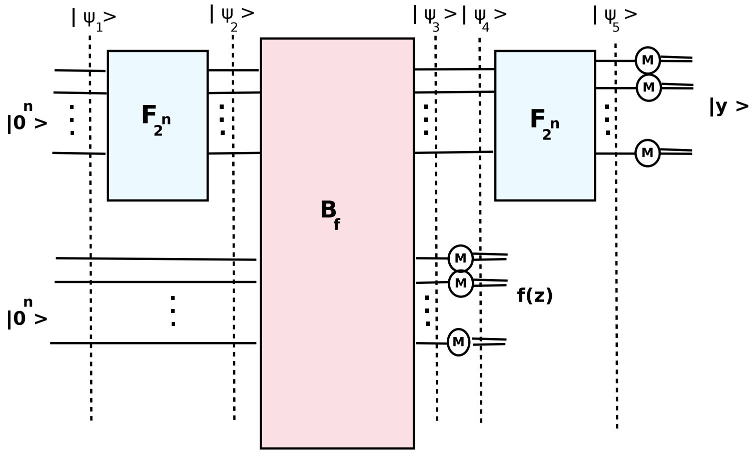

Figure 3.1: The circuit for the Period finding algorithm

$$|\psi_1\rangle = |0^n\rangle\, |0^n\rangle$$

We apply F_{2^n} on the first register. As first register has $|0^n\rangle$ thus in this specific case $F_{2^n} = H^{\otimes n}$.

$$|\psi_2\rangle = F_{2^n}\, |0^n\rangle\, |0^n\rangle = H^{\otimes n}\, |0^n\rangle\, |0^n\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle\, |0^n\rangle$$

Now, we apply B_f on both the register. Recall, the function B_f is defined as follows $B_f\, |x\rangle\, |y\rangle = |x\rangle\, |y \oplus f(x)\rangle$. Also recall, that $|0 \oplus f(x)\rangle = |f(x)\rangle$. Thus,

$$|\psi_3\rangle = B_f\, |\psi_2\rangle$$
$$|\psi_3\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle\, |f(x)\rangle$$

We measure second registers. Suppose our measured value is $f(z)$. Then the first register will have all the possible inputs that may result in $f(z)$. As the function is periodic hence these inputs will be $z, z + r, z + 2r, ..., z + \left(\frac{N}{r} - 1\right) r$. Therefore,

$$|\psi_4\rangle = \sqrt{\frac{r}{N}} \sum_{k=0}^{\frac{N}{r}-1} |z + kr\rangle\, |f(z)\rangle$$

We can now discard last n-qubits as they are not entangled with the first n-qubits.

$$|\psi_4\rangle = \sqrt{\frac{r}{N}} \sum_{k=0}^{\frac{N}{r}-1} |z + kr\rangle$$

We apply Fourier transform on the first n-qubits. This time $F_{2^n} \neq H^{\otimes n}$ because the first n-qubits are not $|0^n\rangle$.

$$|\psi_5\rangle = \sqrt{\frac{r}{N}} \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \alpha_y |y\rangle$$

We measure, $\psi_5 = |y\rangle$, $O(\log N)$ times. Each $|y\rangle$ is a multiple of $\frac{N}{r}$ (as per the second property of Fourier transformation given in Section 3.2). Thus, computing greatest common divisor (GCD) of all of them will get us $\frac{N}{r}$. As we already know, N, thus from $\frac{N}{r}$ we can easily compute r.

3.5 Shorter example

You are given a black-box of function $f : \{0,1\}^3 \rightarrow \{0,1\}^3, f(x) = x \mod 2$. You have to find its period r. Below, in Table 3.1, I show sample outputs of the functions for clarity.

input x	**output** $y = x \mod 2$
0, 2, 4, 6,	0
1, 3, 5, 7	1

Table 3.1: Period function f with period r=2.

Solution

I initialize the two registers.

$$|\psi_1\rangle = |000\rangle |000\rangle$$

Create superposition in the first register.

$$|\psi_2\rangle = \frac{1}{\sqrt{8}} \sum_{x=0}^{7} |x\rangle |000\rangle$$

Now apply B_f on both register. Remember $B_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$. Recall that $|0 \oplus f(x)\rangle = |f(x)\rangle$

$$|\psi_3\rangle = \frac{1}{\sqrt{8}} \sum_{x=0}^{7} |x\rangle \, |x \mod 2\rangle$$

Now we measure the second register. Assume our measurement revealed $f(x) = 1$. Then the first register will have all the possible input corresponding to the output $f(x) = 1$.

$$|\psi_4\rangle = \frac{1}{\sqrt{4}} \Bigg(|1\rangle + |3\rangle + |5\rangle + |7\rangle \Bigg) |1\rangle$$

We ignore the second register now.

$$|\psi_4\rangle = \frac{1}{\sqrt{4}} \Bigg(|1\rangle + |3\rangle + |5\rangle + |7\rangle \Bigg)$$

If we measure now we will get a random value due to phase shift. That is each time we measure, we may be measuring for output $f(x) = 1$ or $f(x) = 0$ (as we have to rerun whole machine, think why?). Thus, getting random values from 0 to 7 each time we measure. However, in case of any output once we apply Fourier transform we will get same result. Hence, to remove phase shift we apply F_8 to it.

$$
\begin{aligned}
|\psi_5\rangle &= F_8 \frac{|1\rangle + |3\rangle + |5\rangle + |7\rangle}{\sqrt{4}} \\
&= \frac{1}{\sqrt{8}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & \omega^8 & \omega^{10} & \omega^{12} & \omega^{14} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \omega^{12} & \omega^{15} & \omega^{18} & \omega^{21} \\ 1 & \omega^4 & \omega^8 & \omega^{12} & \omega^{16} & \omega^{20} & \omega^{24} & \omega^{28} \\ 1 & \omega^5 & \omega^{10} & \omega^{15} & \omega^{20} & \omega^{25} & \omega^{30} & \omega^{35} \\ 1 & \omega^6 & \omega^{12} & \omega^{18} & \omega^{24} & \omega^{30} & \omega^{36} & \omega^{42} \\ 1 & \omega^7 & \omega^{14} & \omega^{21} & \omega^{28} & \omega^{35} & \omega^{42} & \omega^{49} \end{pmatrix} \frac{1}{\sqrt{4}} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} \\
&= \frac{1}{\sqrt{32}} \begin{pmatrix} 1 + 1 + 1 + 1 \\ \omega + \omega^3 + \omega^5 + \omega^7 \\ \omega^2 + \omega^6 + \omega^{10} + \omega^{14} \\ \omega^3 + \omega^9 + \omega^{15} + \omega^{21} \\ \omega^4 + \omega^{12} + \omega^{20} + \omega^{28} \\ \omega^5 + \omega^{15} + \omega^{25} + \omega^{35} \\ \omega^6 + \omega^{18} + \omega^{30} + \omega^{42} \\ \omega^7 + \omega^{21} + \omega^{35} + \omega^{49} \end{pmatrix}
\end{aligned}
$$

That looks messy but we know two things to make our life easy:

- $\omega_8^n = w_8^{n \mod 8}$
- $\omega_8^0 = 1, w_8^1 = w, w_8^2 = -i, w_8^3 = -iw, w_8^4 = -1, w_8^5 = -w, w_8^6 = i, w_8^7 = iw$. This could be easily deduced from Figure **??**.

Thus, after applying above two simplification we get:

$$|\psi_5\rangle = \frac{1}{\sqrt{32}}\begin{pmatrix} 1+1+1+1 \\ w+\omega^3+\omega^5+\omega^7 \\ \omega^2+\omega^6+\omega^{10}+\omega^{14} \\ \omega^3+\omega^9+\omega^{15}+\omega^{21} \\ \omega^4+\omega^{12}+\omega^{20}+\omega^{28} \\ \omega^5+\omega^{15}+\omega^{25}+\omega^{35} \\ \omega^6+\omega^{18}+\omega^{30}+\omega^{42} \\ \omega^7+\omega^{21}+\omega^{35}+\omega^{49} \end{pmatrix} = \frac{1}{\sqrt{32}}\begin{pmatrix} 1+1+1+1 \\ w-iw-w+iw \\ i-i+i-i \\ -iw+w+iw-iw+w+iw-w \\ -w \\ -1-1-1-1 \\ -w+iw+w-iw \\ i-i+i-i \\ iw-w-iw+w \end{pmatrix}$$

$$= \frac{1}{\sqrt{32}}\begin{pmatrix} 4 \\ 0 \\ 0 \\ 0 \\ -4 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \sqrt{\frac{16}{32}}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ -1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \frac{|0\rangle - |4\rangle}{\sqrt{2}}$$

We now measure our output several times and get eventually both 0 and 4. Even when the output is f(0) the measurement of second Fourier transform will be 0 and 4. Try it!

Compute their GCD to 4. Another property of Fourier transform tells that that basically $\frac{N}{r} = 4$. Given that $N = 8$, we get $r = 2$.
Answer

3.6 Longer example

You are given a black-box of function $f : \{0,1\}^4 \longrightarrow \{0,1\}^4, f(x) = 2x \mod 16$. You have to find its period r. Below, in Table 3.2, I show sample outputs of the functions for clarity.

$$|\psi_1\rangle = |0000\rangle\,|0000\rangle$$

input x	**output** $y = 2x \mod 16$
0	$0 \mod 16 = 0$
1	$2 \mod 16 = 2$
2	$4 \mod 16 = 4$
3	$6 \mod 16 = 6$
4	$8 \mod 16 = 8$
5	$10 \mod 16 = 10$
6	$12 \mod 16 = 12$
7	$14 \mod 16 = 14$
8	$16 \mod 16 = 0$
9	$18 \mod 16 = 2$
10	$20 \mod 16 = 4$
...	...

Table 3.2: Period function f with period r=8.

$$|\psi_2\rangle = \frac{1}{\sqrt{16}} \sum_{x=0}^{15} |x\rangle |0000\rangle$$

$$|\psi_3\rangle = B_f |\psi_2\rangle$$

$$|\psi_3\rangle = \frac{1}{\sqrt{16}} \sum_{x=0}^{15} |x\rangle |2x \mod 16\rangle$$

Assume we measure second register and attained output $f(z) = 6$.

$$|\psi_4\rangle = \frac{|3\rangle + |11\rangle}{\sqrt{2}} |4\rangle$$

We drop the second bit like a used tissue-paper.

$$|\psi_4\rangle = \frac{|3\rangle + |11\rangle}{\sqrt{2}}$$

Now we have to apply F_{16} on the above value. Making a 16 × 16 matrix is too much hassle and will take too much space. Hence, I instead use F_{16} butterfly diagrams (a.k.a fast Fourier transform) to solve it. That is not that difficult. Figure 3.2 shows the F_{16} butterfly diagram made using blocks of F_8 butterfly diagram.

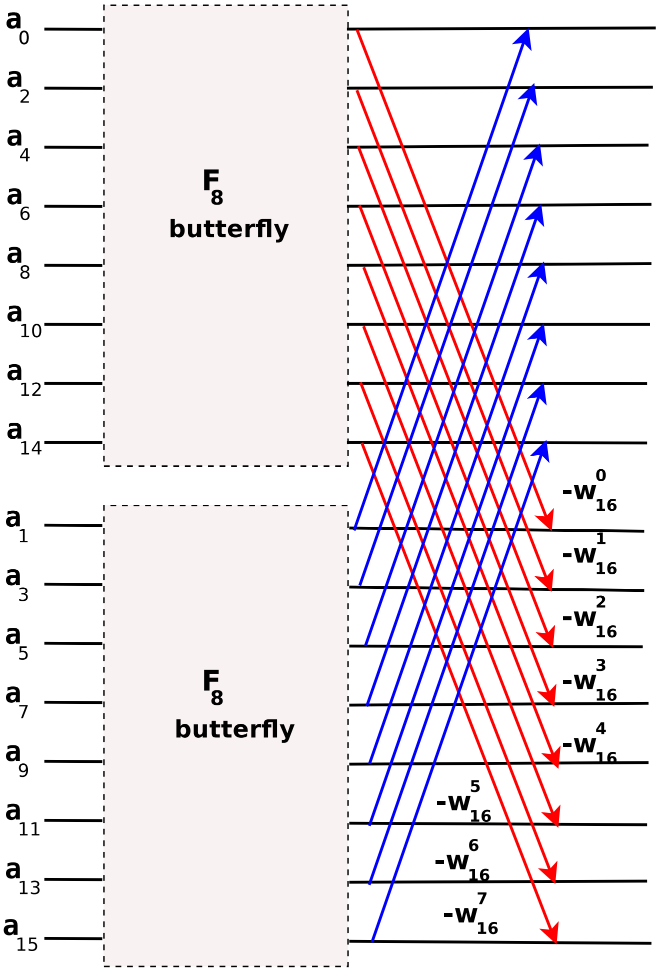

Figure 3.2: F_{16} Butterfly diagram using F_8 butterfly blocks

Using F_{16} butterfly diagram I get the following outcome.

$$|\psi_5\rangle = \frac{1}{\sqrt{32}}\begin{pmatrix} 2 \\ 0 \\ -\sqrt{2} - i\sqrt{2} \\ 0 \\ i2 \\ 0 \\ \sqrt{2} - i\sqrt{2} \\ 0 \\ -2 \\ 0 \\ \sqrt{2} + i\sqrt{2} \\ 0 \\ -i2 \\ 0 \\ -\sqrt{2} + i\sqrt{2} \\ 0 \end{pmatrix}$$

Now we measure $|\psi_5\rangle$ several times. Assume after few tries we obtained outputs 0, 4, and 10. We compute their GCD to obtain 2. Property of Fourier transform tells us that $\frac{N}{r} = 2$, where $N = 16$, solving it we get $r = 8$, which is indeed the desired answer.

3.7 Points to ponder

Question) I understand that first Fourier transformation (a.k.a $H^{\otimes n}$) is necessary to create superposition for B_f but why we need second Fourier transform? Cannot we just measure output of function B_f repeatedly to find the period?

Answer: Whenever, we measure .....

Question) In the example above, what if the outcome I measure are 0, 4, 8 instead of 0, 4, and 10. In that case, $\frac{N}{r} = 4$ and thus the period also be wrongly 4 instead of 2.

Answer:

3.8 Practice Questions

Question 1: You are given a black-box of function $f : \{0,1\}^3 \rightarrow \{0,1\}^3, f(x) = x \mod 4$. Find its period r using the quantum algorithm.

4 Phase Estimation Algorithm

4.1 Eigenvalues and Eigenvector

Definition 1. *An eigenvector of a matrix A is a non-zero vector $\vec{x}$ such that $A\vec{x} = \lambda\vec{x}$, where λ is a scalar, know as eigenvalue.*

To find eigenvalues of a matrix A, you have to do solve $|A - \lambda I| = 0$ for all possible values of λ.

To find eigenvector, solve each eigenvalue λ, $(A - \lambda I)\vec{x} = \vec{0}$.

4.1.1 Example

Find eigenvalues and eigenvector of matrix $\begin{pmatrix} 3 & 6 & -8 \\ 0 & 0 & 6 \\ 0 & 0 & 2 \end{pmatrix}$

Solution

Step 1: Find all possible eigenvalue by solving $|A - \lambda I| = 0$.

$$A - \lambda I = \begin{pmatrix} 3 & 6 & -8 \\ 0 & 0 & 6 \\ 0 & 0 & 2 \end{pmatrix} - \lambda \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 6 & -8 \\ 0 & 0 & 6 \\ 0 & 0 & 2 \end{pmatrix} + \begin{pmatrix} -\lambda & 0 & 0 \\ 0 & -\lambda & 0 \\ 0 & 0 & -\lambda \end{pmatrix} = \begin{pmatrix} 3-\lambda & 6 & 8 \\ 0 & -\lambda & 6 \\ 0 & 0 & 2-\lambda \end{pmatrix}$$

Now find $|A - \lambda I| = 0$

$$\begin{vmatrix} 3-\lambda & 6 & 8 \\ 0 & -\lambda & 6 \\ 0 & 0 & 2-\lambda \end{vmatrix} = (3-\lambda)(-\lambda)(2-\lambda) = 0$$

Solving it for λ, I get:

$\lambda = 3, 0, 2$ These are the three possible eigenvalues.

Step 2: Find corresponding eigenvectors.

For each eigenvalue (i.e. $\lambda = 3, 0, 2$) we have to find eigenvector separately.

For $\lambda = 2$: Solve $(A - \lambda I)\vec{x} = \vec{0}$.

$$A - \lambda I = \begin{pmatrix} 3 & 6 & -8 \\ 0 & 0 & 6 \\ 0 & 0 & 2 \end{pmatrix} - 2 \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 6 & -8 \\ 0 & -2 & 6 \\ 0 & 0 & 0 \end{pmatrix}$$

Now solve

$$\begin{pmatrix} 1 & 6 & -8 \\ 0 & -2 & 6 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \vec{0}$$

Back substitution

Let $\boldsymbol{x_3 = 1}$

$-2x_2 + 6x_3 = 0$

$-2x_2 = -6$

$\boldsymbol{x_2 = 3}$

$x_1 + 6x_2 - 8x_3 = 0$

$x_1 + 6(3) - 8(1) = 0$

$x_1 = -10$

Thus eigenvector for eigenvalue $\lambda = 2$ is $\begin{pmatrix} -10 \\ 3 \\ 1 \end{pmatrix}$

You can verify the correctness of above result using

$A\vec{x} = \lambda\vec{x}$

Similarly, we have to find eigenvectors for $\lambda = 3, 0$

Do it yourself :).

4.2 Eigenvalues of unitary matrices

As depicted in Figure 4.1, Unitary matrices eigenvalues are on complex plain *unit* circle. Thus, if a unitary matrix eigenvalues are real then they must be 1 or −1. Eigenvalues modulus is always equal to 1 (i.e. $||\lambda|| = \sqrt{\lambda \times \lambda^*} = 1$). Recall, a complex number on unit circle $x + yi$ can also be written as $e^{2\pi i\theta}$, the expression which is usually used for eigenvalues of a unitary matrix. We can always find orthogonal eigenvectors for the eigenvalues of a unitary matrix.

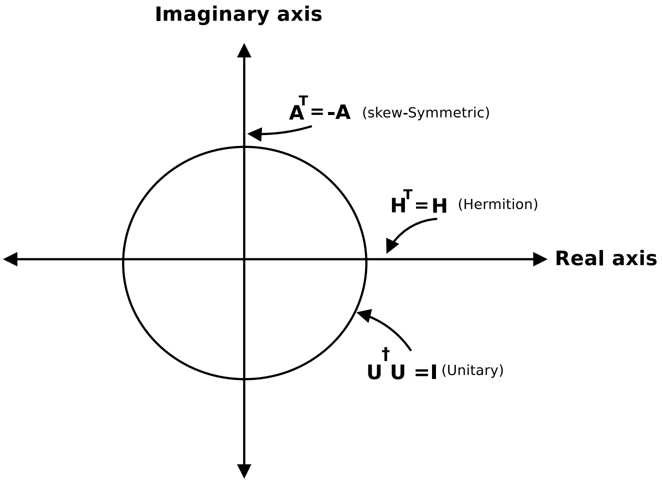

Figure 4.1: Unit complex circle: Eigenvalues of skew-symmetric, U, and H matrices.

For unitary matrix $U_{n \times n}$:

- $U \left| v_k \right\rangle = e^{2\pi i \theta_k} \left| v_k \right\rangle$ for k=1 to 2^n.
- Eigenvectors set is orthonormal. That is each pair of eigenvectors $\left| v_p \right\rangle$, and $\left| v_q \right\rangle$, we have $\langle v_p | v_q \rangle = 0$ and $\langle v_p | v_p \rangle = \langle v_q | v_q \rangle = 1$.

4.3 Problem definition

Given a unitary matrix $U_{n \times n}$, and its one eigenvector $\left| v \right\rangle$, the phase estimation problem ask you to find m-bits approximation of $\theta \in [0, 1)$ say $\hat{\theta}$ where

$$U \left| v \right\rangle = e^{2\pi i \theta} \left| v \right\rangle$$

4.4 Description

The following description is adaption of Prof. John Watrous notes [1]. Please check them out for more details.

The quantum circuit of phase estimation is given in Figure 4.2. We now describe it step-by-step.

$$\left| \psi_1 \right\rangle = \left| 0^m \right\rangle \left| v \right\rangle$$

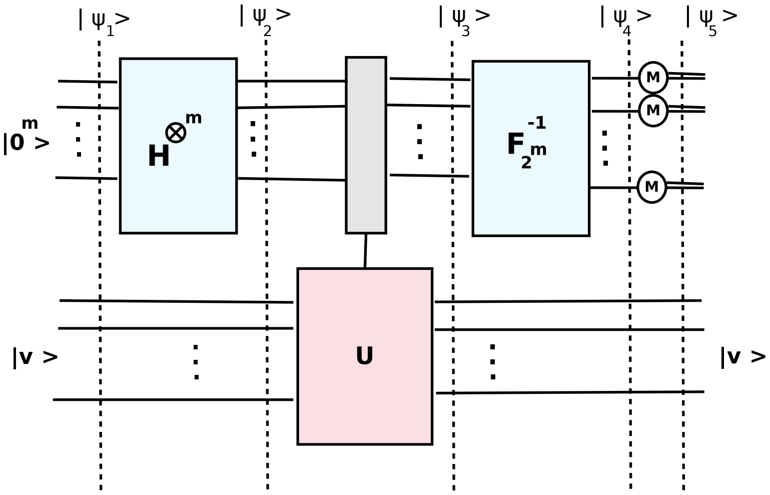

Figure 4.2: Quantum circuit for phase estimation

The value of m tells us the precision with which we wish to compute phase θ as well as the probability of successfully computing it.

Whereas, the dimension of Unitary matrix and corresponding eigenvector $|v\rangle$ are of n-bits. Let say $M = 2^m$, then:

$$|\psi_2\rangle = \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle |v\rangle$$

The next step is crucial and different than what we have done so far. Note carefully that here we apply unitary transformation U multiple times based on the values of $|x\rangle$.

$$|\psi_3\rangle = \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle U^x |v\rangle$$

As we know that $U|v\rangle = e^{2\pi i\theta} |v\rangle$, therefore, $U^x |v\rangle = (e^{2\pi i\theta})^x |v\rangle = e^{2\pi ix\theta} |v\rangle$. Thus,

$$|\psi_3\rangle = \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} e^{2\pi ix\theta} |x\rangle |v\rangle$$

The two registers are not entangled thus we can simply ignore the second register now.

$$|\psi_3\rangle = \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} e^{2\pi i x\theta} |x\rangle$$

Case 1: $\theta = \frac{j}{M}$, for $j \in \{0, 1, ..., M-1\}$

Then given that $\omega = e^{\frac{2\pi i}{M}}$. We have

$$|\psi_3\rangle = \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} e^{2\pi i x \frac{j}{M}} |x\rangle = \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} \omega^{xj} |x\rangle$$

Here if we find j then we will find θ as $\theta = \frac{j}{M}$. Note that $|\psi_3\rangle$ represents j^{th} column of Fourier transform matrix. That is:

$$|\psi_3\rangle = \begin{pmatrix} \omega^{0\times j} \\ \omega^{1\times j} \\ \omega^{2\times j} \\ \dots \\ \omega^{(M-1)\times j} \end{pmatrix}$$

Also note that, given quantum Fourier transform matrix $F_M |j\rangle$ simply provide us j^{th} column of Fourier transform matrix. That is,

$$F_M |j\rangle = \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} \omega^{xj} |x\rangle$$

Therefore, applying inverse Fourier transform matrix on the j^{th} column should provide us the value of j (our aim was to find j as $\theta = \frac{j}{M}$). Thus,

$$|\psi_4\rangle = F_M^{-1} |\psi_3\rangle = |j\rangle$$

We measure $|\psi_4\rangle$ From here we find our θ by diving what we have measure with M.

Case 2: θ has any value

In the second case we once again start with ψ_3 and now θ could be anything.

$$|\psi_3\rangle = \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} e^{2\pi i x\theta} |x\rangle$$

Recall, apply quantum Fourier transform matrix $F_M |j\rangle$ simply provide us j^{th} column of Fourier transform matrix. That is,

$$F_M |j\rangle = \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} \omega^{xj} |x\rangle$$

However, when we apply F_M^{-1} then the sign flips. That is:

$$F_M^{-1} |j\rangle = \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} \omega^{-xj} |x\rangle$$

Thus, applying inverse Fourier transform on $|\psi_3\rangle$ will give us:

$$\begin{aligned} |\psi_4\rangle = F_M^{-1}\psi_3 = F_M^{-1}&\left(\frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} e^{2\pi i x\theta} |x\rangle\right) \\ &= \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} e^{2\pi i x\theta} F_M^{-1} |x\rangle \\ &= \frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} e^{2\pi i x\theta} \left(\frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} e^{-\frac{2\pi i x j}{M}} |j\rangle\right) \\ &= \frac{1}{M} \sum_{x=0}^{M-1} \sum_{j=0}^{M-1} e^{2\pi i x\left(\theta - \frac{j}{M}\right)} |j\rangle \\ &= \sum_{j=0}^{M-1} \left(\frac{1}{M} \sum_{x=0}^{M-1} e^{2\pi i x\left(\theta - \frac{j}{M}\right)}\right) |j\rangle \end{aligned}$$

Thus, probability of measuring each $j \in \{0, 1, ..., M-1\}$ is

$$p_j = \frac{1}{M}\left|\sum_{x=0}^{M-1} e^{2\pi i x\left(\theta - \frac{j}{M}\right)}\right|^2$$

We will show that with high probability $\theta \approx \frac{j}{M}$.

Recall, the geometric series formula

$$\sum_{k=0}^{n-1} x^k = \frac{x^n - 1}{x - 1}$$

Applying it, we get

$$p_j = \frac{1}{M}\left|\frac{e^{2\pi i M\left(\theta - \frac{j}{M}\right)} - 1}{e^{2\pi i\left(\theta - \frac{j}{M}\right)} - 1}\right|^2$$

We calculate probability of **best possible** θ where it is almost equal to $\frac{j}{M}$. That is $\theta = \frac{j}{M} + \epsilon$ where $|\epsilon| \leq \frac{1}{2^{m+1}}$. Let say

$$p_j = \frac{1}{M}\frac{a^2}{b^2} \tag{4.1}$$

where

$$\begin{aligned} a &= |e^{2\pi i M\left(\theta - \frac{j}{M}\right)} - 1| = |e^{2\pi i M\epsilon} - 1| \\ b &= |e^{2\pi i\left(\theta - \frac{j}{M}\right)} - 1| = |e^{2\pi i\epsilon} - 1| \end{aligned}$$

We now calculate **lower-bound** of p_j for that the **best possible** θ. The lower-bound of p_j can be calculated by finding the minimum value of a and the maximum value of b.

Background revision:

Given an arc that makes angle α at the center of the circle whose radius is r. We have following formulas:

arc length = $r\alpha$

If the radius $r = 1$ (unit circle) then
arc length = α

chord length = $2r\sin(\frac{\alpha}{2})$

$\frac{arc\ length}{chord\ length} = \frac{r\alpha}{2r\sin(\frac{\alpha}{2})} = \frac{\alpha}{2\sin(\frac{\alpha}{2})}$ As for minor arc value of angle α cannot be at most π. Therefore,

$\frac{arc\ length}{chord\ length} \leq \frac{\pi}{2}$

Not complete yet!

4.5 Example

You are given a simple unitary matrix $U = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix}$, and its one eigenvector $|v\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, you are asked to use phase estimation to estimate θ of the corresponding eigenvalue $\lambda = e^{2\pi i\theta}$.
[PS: The corresponding eigenvalue (that we do not know at this point) is $\lambda = e^{\frac{i\pi}{4}}$]

Solution Here we have $n = 2$ hence we take $m = 2 \times \lceil \log_2 2 \rceil + 1 = 3$

Initialize the two registers.

$$|\psi_1\rangle = |000\rangle\,|v\rangle$$

Creating superposition in the first register.

$$|\psi_2\rangle = \frac{1}{\sqrt{8}}\sum_{x=0}^{7}|x\rangle\,|v\rangle$$

Apply U multiple times on the second register contents.

$$
\begin{aligned}
|\psi_3\rangle &= \frac{1}{\sqrt{8}} \sum_{x=0}^{7} |x\rangle\, U^x\, |v\rangle \\
&= \frac{1}{\sqrt{8}} \sum_{x=0}^{7} e^{\frac{ix\pi}{4}}\, |x\rangle\, |v\rangle
\end{aligned}
$$

We drop the second register from here (like a used tissue-paper).

$$
\begin{aligned}
|\psi_3\rangle = \frac{1}{\sqrt{8}} \sum_{x=0}^{7} e^{\frac{ix\pi}{4}}\, |x\rangle &= \frac{1}{\sqrt{8}} \sum_{x=0}^{7} \omega_8^x\, |x\rangle \\
&= \frac{1}{\sqrt{8}} \Big(|0\rangle + \omega_8\, |1\rangle + \omega_8^2\, |2\rangle + \omega_8^3\, |3\rangle + \omega_8^4\, |4\rangle + \omega_8^5\, |5\rangle + \omega_8^6\, |6\rangle + \omega_8^7\, |7\rangle \Big)
\end{aligned}
$$

We know that F_8 is equal to:

$$
F_8 = \frac{1}{\sqrt{8}} \begin{bmatrix}
\omega^0 & \omega^0 & \omega^0 & \omega^0 & \omega^0 & \omega^0 & \omega^0 & \omega^0 \\
\omega^0 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\
\omega^0 & \omega^2 & \omega^4 & \omega^6 & \omega^8 & \omega^{10} & \omega^{12} & \omega^{14} \\
\omega^0 & \omega^3 & \omega^6 & \omega^9 & \omega^{12} & \omega^{15} & \omega^{18} & \omega^{21} \\
\omega^0 & \omega^4 & \omega^8 & \omega^{12} & \omega^{16} & \omega^{20} & \omega^{24} & \omega^{28} \\
\omega^0 & \omega^5 & \omega^{10} & \omega^{15} & \omega^{20} & \omega^{25} & \omega^{30} & \omega^{35} \\
\omega^0 & \omega^6 & \omega^{12} & \omega^{18} & \omega^{24} & \omega^{30} & \omega^{36} & \omega^{42} \\
\omega^0 & \omega^7 & \omega^{14} & \omega^{21} & \omega^{28} & \omega^{35} & \omega^{42} & \omega^{49}
\end{bmatrix}
= \frac{1}{\sqrt{8}} \begin{bmatrix}
\omega^0 & \omega^0 & \omega^0 & \omega^0 & \omega^0 & \omega^0 & \omega^0 & \omega^0 \\
\omega^0 & \omega^1 & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\
\omega^0 & \omega^2 & \omega^4 & \omega^6 & \omega^0 & \omega^2 & \omega^4 & \omega^6 \\
\omega^0 & \omega^3 & \omega^6 & \omega & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\
\omega^0 & \omega^4 & \omega^0 & \omega^4 & \omega^0 & \omega^4 & \omega^0 & \omega^4 \\
\omega^0 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega & \omega^6 & \omega^3 \\
\omega^0 & \omega^6 & \omega^4 & \omega^2 & \omega^0 & \omega^6 & \omega^4 & \omega^2 \\
\omega^0 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1
\end{bmatrix}
$$

$$
= \frac{1}{\sqrt{8}} \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & \omega & -i & -i\omega & -1 & -\omega & i & i\omega \\
1 & -i & -1 & i & 1 & -i & -1 & i \\
1 & -i\omega & i & \omega & -1 & i\omega & -i & -\omega \\
1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\
1 & -\omega & -i & i\omega & -1 & \omega & i & -i\omega \\
1 & i & -1 & -i & 1 & i & -1 & -i \\
1 & i\omega & i & -\omega & -1 & -i\omega & -i & \omega
\end{bmatrix}
= \frac{1}{\sqrt{8}} \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & e^{\frac{\pi i}{4}} & -i & -ie^{\frac{\pi i}{4}} & -1 & -e^{\frac{\pi i}{4}} & i & ie^{\frac{\pi i}{4}} \\
1 & -i & -1 & i & 1 & -i & -1 & i \\
1 & -ie^{\frac{\pi i}{4}} & i & e^{\frac{\pi i}{4}} & -1 & ie^{\frac{\pi i}{4}} & -i & -e^{\frac{\pi i}{4}} \\
1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\
1 & -e^{\frac{\pi i}{4}} & -i & ie^{\frac{\pi i}{4}} & -1 & e^{\frac{\pi i}{4}} & i & -ie^{\frac{\pi i}{4}} \\
1 & i & -1 & -i & 1 & i & -1 & -i \\
1 & ie^{\frac{\pi i}{4}} & i & -e^{\frac{\pi i}{4}} & -1 & -ie^{\frac{\pi i}{4}} & -i & e^{\frac{\pi i}{4}}
\end{bmatrix}
$$

The inverse of the matrix F_8 will be

$$F_8^{-1} = \frac{1}{\sqrt{8}} \begin{bmatrix} \omega^0 & \omega^0 & \omega^0 & \omega^0 & \omega^0 & \omega^0 & \omega^0 & \omega^0 \\ \omega^0 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega \\ \omega^0 & \omega^6 & \omega^4 & \omega^2 & \omega^0 & \omega^6 & \omega^4 & \omega^2 \\ \omega^0 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega^1 & \omega^6 & \omega^3 \\ \omega^0 & \omega^4 & \omega^0 & \omega^4 & \omega^0 & \omega^4 & \omega^0 & \omega^4 \\ \omega^0 & \omega^3 & \omega^6 & \omega & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ \omega^0 & \omega^2 & \omega^4 & \omega^6 & \omega^0 & \omega^2 & \omega^4 & \omega^6 \\ \omega^0 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \end{bmatrix} = \frac{1}{\sqrt{8}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -i\omega & i & -\omega & -1 & -i\omega & -i & \omega \\ 1 & i & -1 & -i & 1 & i & -1 & -i \\ 1 & -\omega & -i & -i\omega & -1 & \omega & i & -i\omega \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -i\omega & i & \omega & -1 & -i\omega & -i & -\omega \\ 1 & -i & -1 & i & 1 & -i & -1 & i \\ 1 & \omega & -i & -i\omega & -1 & -\omega & i & i\omega \end{bmatrix}$$

$$|\psi_4\rangle = \frac{1}{8}\left[\begin{pmatrix}1\\1\\1\\1\\1\\1\\1\\1\end{pmatrix} + \omega_8\begin{pmatrix}1\\i\omega\\i\\-\omega\\-1\\-i\omega\\-i\\\omega\end{pmatrix} + \omega_8^2\begin{pmatrix}1\\i\\-1\\-i\\1\\i\\-1\\-i\end{pmatrix} + \omega_8^3\begin{pmatrix}1\\-\omega\\-i\\i\omega\\-1\\\omega\\i\\-i\omega\end{pmatrix} + \omega_8^4\begin{pmatrix}1\\-1\\1\\-1\\1\\-1\\1\\-1\end{pmatrix} + \omega_8^5\begin{pmatrix}1\\-i\omega\\i\\\omega\\-1\\i\omega\\-i\\-\omega\end{pmatrix} + \omega_8^6\begin{pmatrix}1\\-i\\-1\\i\\1\\-i\\-1\\i\end{pmatrix} + \omega_8^7\begin{pmatrix}1\\\omega\\-i\\-i\omega\\-1\\-\omega\\i\\i\omega\end{pmatrix}\right]$$

$$= \frac{1}{8}\left[\begin{pmatrix}1\\1\\1\\1\\1\\1\\1\\1\end{pmatrix} + \omega_8\begin{pmatrix}1\\i\omega\\i\\-\omega\\-1\\-i\omega\\-i\\\omega\end{pmatrix} - i\begin{pmatrix}1\\i\\-1\\-i\\1\\i\\-1\\-i\end{pmatrix} - i\omega_8\begin{pmatrix}1\\-\omega\\-i\\i\omega\\-1\\\omega\\i\\-i\omega\end{pmatrix} - 1\begin{pmatrix}1\\-1\\1\\-1\\1\\-1\\1\\-1\end{pmatrix} - \omega_8\begin{pmatrix}1\\-i\omega\\i\\\omega\\-1\\i\omega\\-i\\-\omega\end{pmatrix} + i\begin{pmatrix}1\\-i\\-1\\i\\1\\-i\\-1\\i\end{pmatrix} + i\omega_8\begin{pmatrix}1\\\omega\\-i\\-i\omega\\-1\\-\omega\\i\\i\omega\end{pmatrix}\right]$$

$$= \frac{1}{8}\begin{pmatrix}1+\omega-i-i\omega-1-\omega+i+i\omega\\1+1+1+1+1+1+1+1\\1+i\omega+i-\omega-1-i\omega-i+\omega\\1+i-1-i+1+i-1-i\\1-\omega-i+i\omega-1+\omega+i-i\omega\\1-1+1-1+1-1+1-1\\1-i\omega+i+\omega-1+i\omega-i-\omega\\1-i-1+i+1-i-1+i\end{pmatrix} = \frac{1}{8}\begin{pmatrix}0\\8\\0\\0\\0\\0\\0\\0\end{pmatrix}$$

Lets say we measure the output with highest amplitude (probability).

We got $x = 1$. As in eigenvalue $e^{2i\pi\theta}$, $\theta = \frac{x}{2^m} = \frac{1}{8}$. Which is indeed the right answer.

5 Order Finding Algorithm

5.1 Background Abstract Algebra

5.1.1 Group

A group is a set G, with some operation o, that fulfills the following properties:

- **Closed:** If $a, b \in G$, then $aob \in G$.
- **Associative:** For $a, b, c \in G$, $(aob)oc = ao(boc)$.
- **Identity:** There exist an element $i \in G$, such that $\forall a \in G$, $aoi = a$.
- **Inverse:** Each element $a \in G$, there exit an element $r \in G$ such that $aor = i$, where i is identity element.
- *Abelian* group also have **Commutative** property: That is for $a, b \in G$, $aob = boa$

5.1.2 Euler's Phi or Totient function

Euler Totient function, $\varphi(x)$, tells us that how many numbers for the set $\{1, 2, ..., x\}$ are relative prime to x. Example, for the set $\mathbb{Z}_{10} = \{0, 1, 2, ..., 10\}$, $\varphi(10) = 4$.

It is because, we have $gcd(1, 10) = 1$, $gcd(3, 10) = 1$, $gcd(7, 10) = 1$, $gcd(9, 10) = 1$. We can use the following formula to calculate totatives of a number:

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) \tag{5.1}$$

Example

What is Euler's Totient of 20.

Solution
I use the formula given in Equation 5.1. Prime factors of 20 are $2^2 \times 5$.

Thus,

$$\varphi(20) = 20 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{5}\right) = 20 \times \frac{1}{2} \times \frac{4}{5} = 20 \times \frac{4}{10} = 8$$

Example

What is Euler's Totient of 100.

Solution
I use the formula given in Equation 5.1. Prime factors of 100 are $2^2 \times 5^5$.

Thus,

$$\varphi(100) = 100 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{5}\right) = 100 \times \frac{1}{2} \times \frac{4}{5} = 100 \times \frac{4}{10} = 40$$

5.1.3 Euler's Theorem

If α and n are relative prime numbers. Then $\alpha^{\varphi(n)} \equiv 1 \mod n$.

The implication

> The number of elements in a G, composed of $\mathbb{Z}_n^*$, over operation × are equal to $\varphi(n)$.

Hence, $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, however the set $\mathbb{Z}_{10}^*$ contains only elements that form group under operation ×. The number of elements in $|\mathbb{Z}_{10}^*| = \varphi(10) = 4$. That is, $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$.

5.1.4 Continued Fractions

Any number x can be written as continued fraction

$$x = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{6 + \cdots}}}}}}$$

A continued fraction may be composed of real or complex numbers. The number of terms are infinite when x is irrational other they are finite. It has lots of application in various fields of mathematics. One of those application is to find approximation fraction of a irrational number.

Example

We know that famous irrational Euler's number is $e = 2.71828182845...$, we wish to find a fraction that represents it correctly up to 4 decimal places. This can be accomplished using continued fraction as follows.

$$e = 2 + (0.71828182845) = 2$$

$$e = 2 + \cfrac{1}{1 + 0.39221119118} = 2$$

$$e = 2 + \cfrac{1}{1 + \cfrac{1}{2 + 0.54964677829}} = \frac{8}{3} = 2.6666..$$

$$e = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + 0.81935024364}}} = \frac{11}{4} = 2.75$$

$$e = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + 0.22047928558}}}} = \frac{19}{7} = 2.71428\ldots$$

$$e = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + 0.53557347743}}}}} = \frac{87}{32} = 2.71875$$

$$e = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{1 + 0.8671574343}}}}}} = \frac{106}{39} = 2.71794\ldots$$

$$e = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{1 + 0.15319313477}}}}}}} = \frac{193}{71} = 2.71830\ldots$$

$$e = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{6 + 0..52770766459}}}}}}}} = \frac{1264}{465} = 2.71827\ldots$$

More iterations we have more better we have the fraction that represent e. That is, 2, $\frac{8}{3}$, $\frac{11}{4}$, $\frac{19}{7}$, $\frac{87}{32}$, $\frac{106}{39}$, $\frac{193}{71}$, $\frac{1264}{465}$. Where, the last fraction, $\frac{1264}{456}$, correctly represents e up to 4 decimal places.

5.2 Order finding problem

Given a positive integer $\alpha \in \mathbb{Z}_n^*$ for $n \geq 1$. The order finding problem ask you to find the smallest possible positive number $r \in \mathbb{Z}_n^*$ such that

$$\alpha^r \equiv 1 \mod n$$

5.2.1 Classical computer

First note that order finding problem always has a solution as we know from Euler's theorem (Section 5.1.3) that $\alpha^{\varphi(n)} \equiv 1 \mod n$, that might not be the smallest possible number. For classical computer we do not know any solution that can solve this problem in polynomial time, although there is no proof that it cannot be done. It implies that no solution exist that can solve problem in $O(G)$ where G are the number of bits needed to represent n, i.e. $G = \lceil \log_2 n \rceil$. The only solution currently known is to try all possibilities to find r. Thus, the problem take exponential time with respect to the size of n.

5.2.2 Quantum algorithm

There is a simple polynomial times reduction of order finding problem to the phase estimation problem. That is,

$$Shor's\ factoring \leq_p Order\ finding \leq_p Phase\ estimation$$

Basic Idea:

The basic idea of order finding is to create a specific unitary operator based on input $\alpha \in \mathbb{Z}_n^*$ such that the phase of one of the operator's eigenvalue is same as the order of α. Then use that newly created unitary operator and its specific eigenvector as input to the phase estimation algorithm. Thus, by finding the phase of the eigenvalue, we are able to find the order of $\alpha \in \mathbb{Z}_n^*$.

Details

Consider the following Unitary operator U_α for $x \in \mathbb{Z}_n^*$

$$U_\alpha \left|x\right\rangle = \left|\alpha x \mod n\right\rangle$$

Eigenvectors of this special unitary operator U_α are of the form:

$$\left|\rho_j\right\rangle = \frac{1}{\sqrt{r}}\Bigg(\left|1\right\rangle + \omega_r^{-j}\left|\alpha\right\rangle + \omega_r^{-2j}\left|\alpha^2\right\rangle + \cdots + \omega_r^{-(r-1)j}\left|\alpha^{r-1}\right\rangle\Bigg) = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\omega_r^{-kj}\left|\alpha^k\right\rangle$$

It is because

$$\begin{aligned} U_\alpha\left|\rho_j\right\rangle &= \frac{1}{\sqrt{r}}\Bigg(\left|\alpha\right\rangle + \omega_r^{-j}\left|\alpha^2\right\rangle + \omega_r^{-2j}\left|\alpha^3\right\rangle + \cdots + \omega_r^{-(r-1)j}\left|\alpha^r\right\rangle\Bigg) \\ &= \frac{\omega_r^j}{\sqrt{r}}\Bigg(\omega_r^{-j}\left|\alpha\right\rangle + \omega_r^{-2j}\left|\alpha^2\right\rangle + \omega_r^{-3j}\left|\alpha^3\right\rangle + \cdots + \omega_r^{-rj}\left|\alpha^r\right\rangle\Bigg) \\ &= \frac{\omega_r^j}{\sqrt{r}}\Bigg(\omega_r^{-j}\left|\alpha\right\rangle + \omega_r^{-2j}\left|\alpha^2\right\rangle + \omega_r^{-3j}\left|\alpha^3\right\rangle + \cdots + \left|1\right\rangle\Bigg) \\ &= \omega_r^j\left|\rho_j\right\rangle \end{aligned}$$

Which proves that $\{\left|\rho_0\right\rangle, \left|\rho_1\right\rangle, \cdots, \left|\rho_{r-1}\right\rangle\}$ are indeed the valid eigenvectors of our special unitary operator U_α and the corresponding eigenvalues are $\{1, \omega_r, \omega_r^2, \cdots, \omega_r^{r-1}\}$.

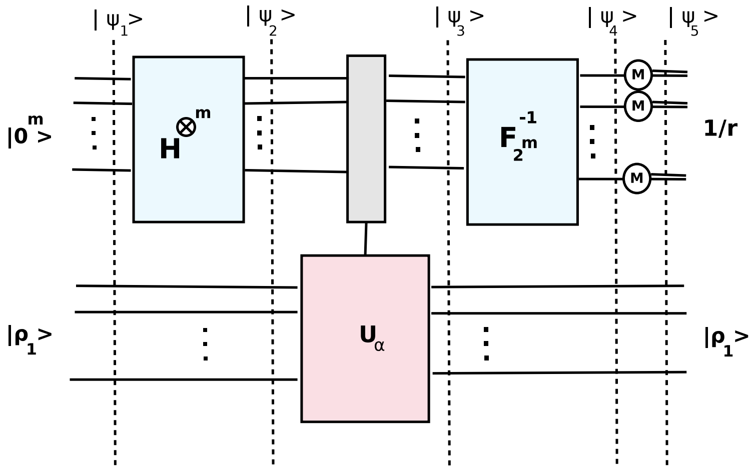

Figure 5.1: Phase estimation circuit with unitary operator U_α and eigenvector $|\rho_1\rangle$. Output will be $\frac{1}{r}$ as that is the θ of the eigenvalue

Ideally, we would like to use eigenvalue $|\rho_1\rangle$ as its eigenvector is $\omega_r = e^{2\pi i/r}$ thus the output of phase estimation algorithm will be $\frac{j}{2^m} \approx \frac{1}{r}$, $j \in \{0, 1, ..., 2^m\}$. By computing the reciprocal of the output we will get our order r. Figure 5.1 illustrates this simple case. However, unfortunately, we cannot make $|\rho_1\rangle$ without having to already know r thus this simple case is not possible.

Now here is a beautiful solution, instead of running phase estimation algorithm on $|\rho_1\rangle$, we run it on superposition of all the eigenvectors. But without knowing r can we create superposition of all the eigenvectors? Fortunately, the superposition of all the eigenvector is simply $|1\rangle$ which can be prepared easily without knowing r. Mathematically,

$$\frac{1}{\sqrt{r}}\sum_{q=0}^{r-1}|\rho_q\rangle = \frac{1}{r}\sum_{q=0}^{r-1}\sum_{k=0}^{r-1}\omega_r^{-kq}\,|\alpha^k\rangle = |1\rangle$$

Giving input as the superposition state of all the eigenvalues will give us output which is also superposition of all the outputs of each eigenvalue. That is, the output of the first register before measurement will be:

$$|\psi_4\rangle = \frac{1}{\sqrt{r}}\sum_{q=0}^{r-1}|q/r\rangle\,|\rho_q\rangle$$

Now if we measure first register we will get q/r where q is random number which is uniformly distributed in the set $\{0, 1, 2, \cdots, r-1\}$. We know that $r \leq \varphi(n) \leq n$. We use this to calculate the values of q and r using continued fraction method which is explained Section 5.1.4.

5.2.3 Summary

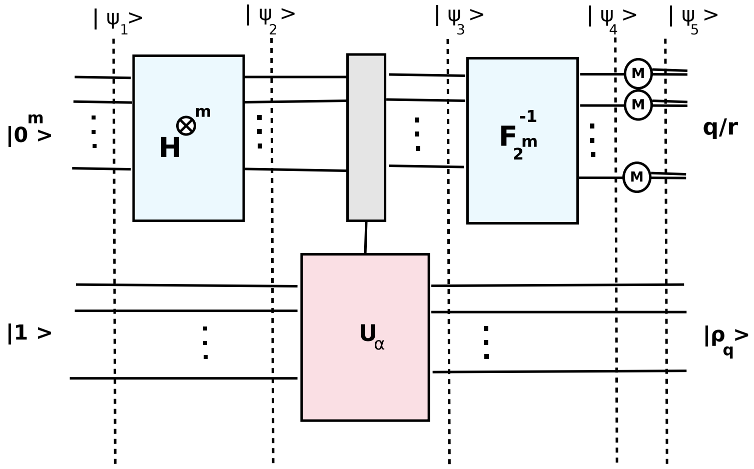

Figure 5.2: Phase estimation circuit but with unitary operator U_α and superposition of all eigenvectors $|1\rangle$. Output will be $\frac{q}{r}$, where q is uniformly distributed in the set $\{0, 1, 2, \cdots, r-1\}$

Summary of the steps carried out to compute order is illustrated by Figure 5.2 and ontlined as follows:

- Given that $G = \lceil \log_2 n \rceil$, create two registers, such that, the first register is of size $m = 2G + 1$ and the second register is of size $n = G$. (REWRITE)
- $|\psi_1\rangle = |0^m\rangle |1^n\rangle$.
- Use hadamard gates to create superpostion in the first register $|\psi_2\rangle = \frac{1}{\sqrt{2^m}} \sum_{x=0}^{2^m-1} |x\rangle |1\rangle$.
- Apply U_α for each value of x, that is, $|\psi_3\rangle = \frac{1}{\sqrt{2^m}} \sum_{x=0}^{2^m-1} |x\rangle U_\alpha^x |1\rangle = \frac{1}{\sqrt{2^m}} \sum_{x=0}^{2^m-1} |x\rangle |\alpha^j \mod n\rangle = \frac{1}{\sqrt{r2^m}} \sum_{x=0}^{2^m-1} |x\rangle \sum_{q=0}^{r-1} \omega_r^{xq} |\rho_q\rangle = \frac{1}{\sqrt{r2^m}} \sum_{q=0}^{r-1} \sum_{x=0}^{2^m-1} \omega_r^{xq} |x\rangle |\rho_q\rangle$.
- After apply inverse Fourier transform we get $|\psi_4\rangle = \frac{1}{\sqrt{r}} \sum_{q=0}^{r-1} |q/r\rangle |\rho_q\rangle$
- Measuring the first register will give us $|q/r\rangle$.
- We use continued fractions technique to find r.

Bibliography

[1] John Watrous. *CPSC 519/619: Quantum Computation.* University of Calgary.