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: $\left\{ |00\rangle, |01\rangle, |10\rangle, |11\rangle \right\}$. 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 $\left\{ |0\rangle\langle 0|, |0\rangle\langle 1|, |1\rangle\langle 0|, |1\rangle\langle 1| \right\}$ 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 Entanglement

A set of qubits is considered quantum entangled when their probabilities are dependent on each other, preventing their separate expression. Entanglement can be described using its two fundamental properties:

1. State of entangled qubits cannot be described individually.
2. Measuring one qubit of the entangled qubits reveals information about the others.

2.1 Bell Basis

Entangled states for two qubits are famously known as Bell states, collectively forming the Bell basis. These states are also referred to as EPR states, named after the pioneering scientists Einstein, Podolsky, and Rosen, who first discovered them.

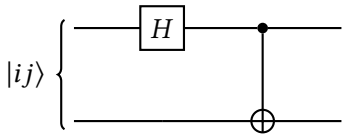


Figure 2.1: Circuit Generating the Bell Basis

Bell Basis :

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$
$$|\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$
$$|\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$
$$|\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

The circuit that generates all the Bell states is shown in Figure 8.1. A Bell state is entangled because the qubits within it depend on each other, making it impossible to express them separately. This implies that any two entangled qubits cannot be written in the form $(\alpha|0\rangle + \beta|1\rangle)(\gamma|0\rangle + \delta|1\rangle)$. Let's prove this for the Bell state β_{00}.

2.2 Entanglement Proof

Theorem 2.1. *For any valid α, β, γ, and δ, the equation*

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \neq (\alpha|0\rangle + \beta|1\rangle)(\gamma|0\rangle + \delta|1\rangle)$$

holds, demonstrating the entanglement of these qubits.

Proof. We prove this by contradiction. Let's assume that

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} = (\alpha|0\rangle + \beta|1\rangle)(\gamma|0\rangle + \delta|1\rangle)$$
$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle$$

For equality to hold, $\alpha\delta = 0$ must be true. This means that at least one of α and δ must be zero. If $\alpha = 0$, the amplitude of $|00\rangle$ becomes zero instead of $\frac{1}{\sqrt{2}}$, so α cannot be zero. Similarly, if $\gamma = 0$, the amplitude of $|11\rangle$ becomes zero instead of $\frac{1}{\sqrt{2}}$, so γ cannot be zero either. This contradiction proves that our assumption is incorrect; hence, $\frac{|00\rangle+|11\rangle}{\sqrt{2}} \neq (\alpha|0\rangle + \beta|1\rangle)(\gamma|0\rangle + \delta|1\rangle)$. □

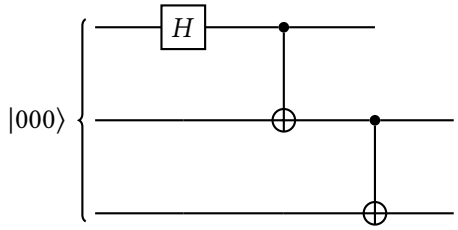


Figure 2.2: Quantum circuit to produce GHZ states

2.3 GHZ States

In addition to two-qubit entanglement, we have tripartite entanglement, referred to as GHZ states, named after scientists Daniel **G**reenberger, Michael **H**orne, and Anton **Z**eilinger, who studied four-particle entanglement and explained GHZ states. The circuit to create GHZ states is shown in Figure 8.2. In this case, measuring any qubit will reveal information about the others with certainty. Furthermore, the amplitudes of these qubits cannot be expressed separately.

2.4 Quantum Teleportation

Quantum teleportation enables the transmission of a **single qubit** by conveying only two classical bits, provided that both parties share a Bell state. For a more in-depth understanding, you can refer to this video: Quantum Teleportation.

2.4.1 The Story

Imagine Ali and Babar, who have previously shared a Bell state denoted as β_{00}. Ali possesses the first qubit of this Bell state, while Babar holds the second qubit. Now, let's introduce a twist to the story – Babar relocates to North Korea. At some point, Ali desires to transmit a highly valuable qubit, denoted as $|\psi\rangle$, to Babar, all while keeping this transfer clandestine. Achieving this seemingly impossible task involves Ali measuring his portion of the Bell state and the valuable qubit $|\psi\rangle$. Based on the measurement results, Ali sends two classical bits to Babar, who then performs specific operations on his Bell state to miraculously recreate $|\psi\rangle$.

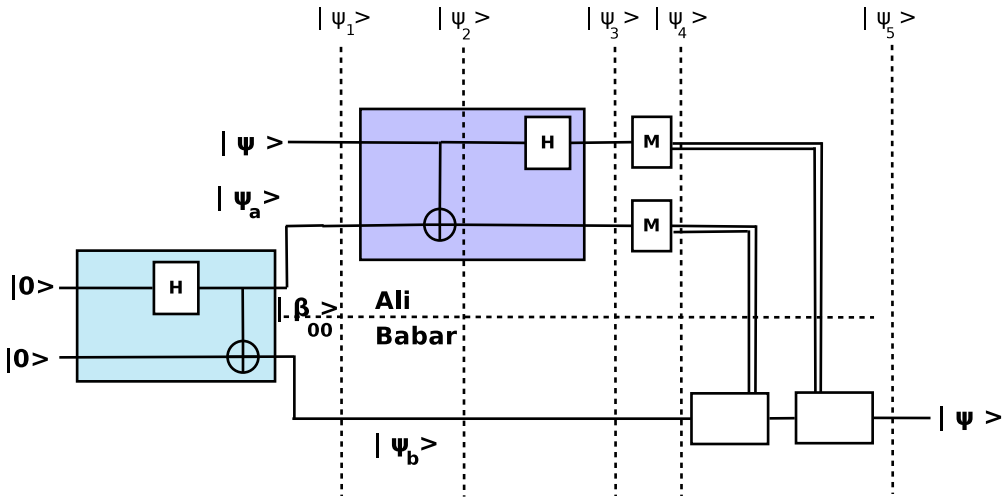


Figure 2.3: Quantum Teleportation

2.4.2 Circuit and Mathematics

The quantum teleportation process is depicted in Figure 8.3 above. To understand how this circuit operates, let's examine how the input qubit transforms as it passes through the circuit. Suppose the qubit Ali wishes to transmit to Babar is $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

Initially, Ali and Babar have the following qubits:

$$
\begin{aligned}
|\psi_1\rangle &= |\psi\rangle\,|\beta_{00}\rangle \\
|\psi_1\rangle &= (\alpha|0\rangle + \beta|1\rangle)\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right) \\
|\psi_1\rangle &= \frac{\alpha}{\sqrt{2}}|000\rangle + \frac{\alpha}{\sqrt{2}}|011\rangle + \frac{\beta}{\sqrt{2}}|100\rangle + \frac{\beta}{\sqrt{2}}|111\rangle
\end{aligned}
$$

Note that the first two qubits belong to Ali, while the last qubit belongs to Babar. Ali then passes his qubit through a CNOT gate, resulting in:

$$
|\psi_2\rangle = \frac{\alpha}{\sqrt{2}}|000\rangle + \frac{\alpha}{\sqrt{2}}|011\rangle + \frac{\beta}{\sqrt{2}}|110\rangle + \frac{\beta}{\sqrt{2}}|101\rangle
$$

Next, Ali applies a Hadamard operation to his first qubit:

$$
\begin{aligned}
|\psi_3\rangle &= \frac{\alpha}{\sqrt{2}}\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}|00\rangle\right) + \frac{\alpha}{\sqrt{2}}\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}|11\rangle\right) + \frac{\beta}{\sqrt{2}}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}|10\rangle\right) + \frac{\beta}{\sqrt{2}}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}|01\rangle\right) \\
|\psi_3\rangle &= \frac{1}{2}\left[\alpha\Big(|0\rangle + |1\rangle\Big)|00\rangle + \alpha\Big(|0\rangle + |1\rangle\Big)|11\rangle + \beta\Big(|0\rangle - |1\rangle\Big)|10\rangle + \beta\Big(|0\rangle - |1\rangle\Big)|01\rangle\right] \\
|\psi_3\rangle &= \frac{1}{2}\Big[\alpha|000\rangle + \alpha|100\rangle + \alpha|011\rangle + \alpha|111\rangle + \beta|010\rangle - \beta|110\rangle + \beta|001\rangle - \beta|101\rangle\Big] \\
|\psi_3\rangle &= \frac{1}{2}\Big[|00\rangle\Big(\alpha|0\rangle + \beta|1\rangle\Big) + |01\rangle\Big(\alpha|1\rangle + \beta|0\rangle\Big) + |10\rangle\Big(\alpha|0\rangle - \beta|1\rangle\Big) + |11\rangle\Big(\alpha|1\rangle - \beta|0\rangle\Big)\Big]
\end{aligned}
$$

Ali then measures his first two qubits, and Table 2 below shows Ali's possible measurements and the resulting superposition of Babar's unmeasured qubit.

Based on Ali's measurements, Babar determines the operations to apply to his superposition without measuring his qubit. Babar's logic for applying operations and the corresponding operations are provided in Table 3.

Thus, after applying operations, the $|\psi_5\rangle$ that Babar creates will be exactly the intended qubit $|\psi\rangle$ that Ali wanted to send. Magical!

Ali's Measurement	Babar's Superposition
00	$\alpha \|0\rangle + \beta \|1\rangle$
01	$\alpha \|1\rangle + \beta \|0\rangle$
10	$\alpha \|0\rangle - \beta \|1\rangle$
11	$\alpha \|1\rangle - \beta \|0\rangle$

Table 2.1: $|\psi_4\rangle$ after partial measurements

Classical Bits Received	Babar's Logic	Babar's Operations
00	My superposition will be exactly $\|\psi\rangle$, so no further action is needed.	$\|\psi_5\rangle = I \|\psi_b\rangle$
01	My superposition needs to swap amplitudes, achieved using a NOT (i.e., X) gate.	$\|\psi_5\rangle = X \|\psi_b\rangle$
10	My superposition requires changing the sign of the amplitude associated with $\|1\rangle$ while keeping the rest unchanged. This is accomplished using a Z gate.	$\|\psi_5\rangle = Z \|\psi_b\rangle$
11	My superposition needs to be first swapped using an X gate and then have the sign of $\|1\rangle$ changed with a Z gate.	$\|\psi_5\rangle = ZX \|\psi_b\rangle$

Table 2.2: $|\psi_5\rangle$ Babar operations

2.4.3 What Quantum Teleportation is NOT!

1. **Qubit Cloning**: It does not clone a qubit as a qubit that Ali had was destroyed in the process.
2. **Faster than Speed of Light Communication**: It does not give us faster-than-speed-of-light communication as we have to transmit two classical bits using the same old method. Without transmitting those classical bits, Babar has no way of knowing what operations to perform to create $|\psi\rangle$.

2.5 Superdense Coding

The protocol of Superdense coding allows sending **two classical bits** by transmitting only a **single qubit**. It is explained in video https://youtu.be/o2AuL6mxGiE.

The circuit diagram of Superdense coding is shown in Figure 8.4. Let's calculate the outcomes of each $|\psi_i\rangle$ to see how the Superdense coding circuit works.

$$|\psi_1\rangle = |00\rangle$$
$$|\psi_2\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

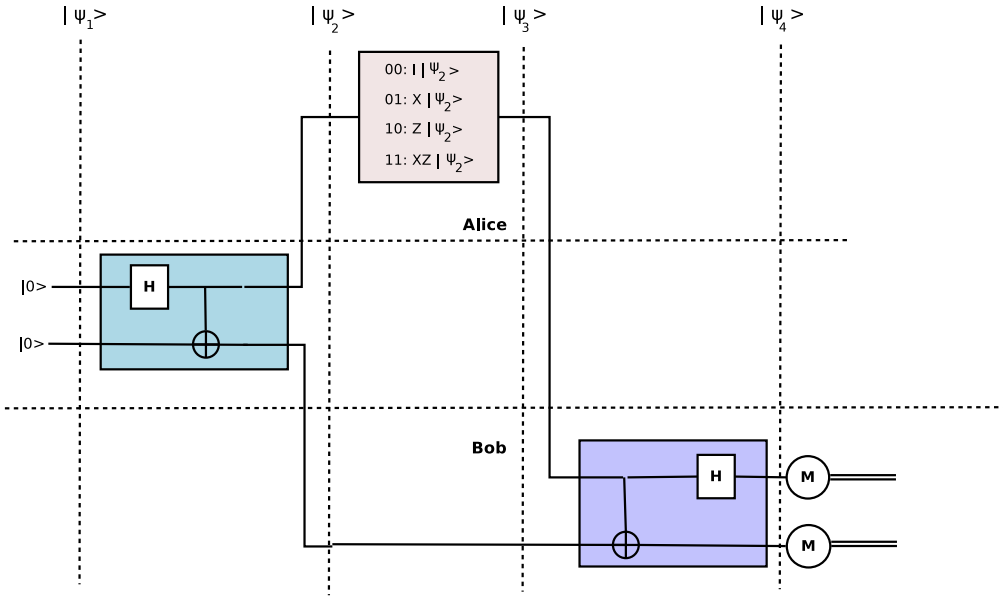


Figure 2.4: Circuit diagram of Superdense coding

Alice applies different transformation depending upon what he wants to send. These transformations are shown in Table 8.3.

Bob applies final transformations as shown in Table 8.4.

Finally, Bob measures qubits and gets the output send by Alice with 1 probability.

Alice is sending	**Result**
00	$\frac{\|00\rangle+\|11\rangle}{\sqrt{2}}$
01	$\frac{X\|0\rangle\|0\rangle+X\|1\rangle\|1\rangle}{\sqrt{2}} = \frac{\|1\rangle\|0\rangle+\|0\rangle\|1\rangle}{\sqrt{2}} = \frac{\|10\rangle+\|01\rangle}{\sqrt{2}}$
10	$\frac{Z\|0\rangle\|0\rangle+Z\|1\rangle\|1\rangle}{\sqrt{2}} = \frac{\|0\rangle\|0\rangle-\|1\rangle\|1\rangle}{\sqrt{2}} = \frac{\|00\rangle-\|11\rangle}{\sqrt{2}}$
11	$\frac{XZ\|0\rangle\|0\rangle+XZ\|1\rangle\|1\rangle}{\sqrt{2}} = \frac{X\|0\rangle\|0\rangle-X\|1\rangle\|1\rangle}{\sqrt{2}} = \frac{\|10\rangle-\|01\rangle}{\sqrt{2}}$

Table 2.3: $|\psi_3\rangle$.

Bob has received	**CNOT**	**H on 1st qubit**
$\frac{\|00\rangle+\|11\rangle}{\sqrt{2}}$	$\frac{\|00\rangle+\|10\rangle}{\sqrt{2}}$	$\|00\rangle$
$\frac{\|10\rangle+\|01\rangle}{\sqrt{2}}$	$\frac{\|11\rangle+\|01\rangle}{\sqrt{2}}$	$\|01\rangle$
$\frac{\|00\rangle-\|11\rangle}{\sqrt{2}}$	$\frac{\|00\rangle-\|10\rangle}{\sqrt{2}}$	$\|10\rangle$
$\frac{\|10\rangle-\|01\rangle}{\sqrt{2}}$	$\frac{\|11\rangle-\|01\rangle}{\sqrt{2}}$	$-\|11\rangle$

Table 2.4: $|\psi_4\rangle$.

3 Assignment 3: Entanglement

Q 1: Prove whether the following qubits are entangled or not. In case they are not entangled, **express each qubit state separately**.

a) $\frac{1}{\sqrt{3}}|00\rangle + \sqrt{\frac{2}{3}}|11\rangle$

b) $\frac{1}{\sqrt{3}}\big(|001\rangle + |010\rangle + |100\rangle\big)$

c) $\sqrt{\frac{2}{5}}|000\rangle + \sqrt{\frac{3}{5}}|111\rangle$

d) $\frac{|{+}{+}\rangle + |{-}{-}\rangle}{\sqrt{2}}$

e) $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{3}}|01\rangle + \frac{1}{\sqrt{6}}|10\rangle$

Q 2: In the quantum teleportation circuit, if we use the Bell state B_{11} instead of B_{00}, can we still achieve quantum teleportation? Show all the steps while highlighting any changes needed to make it work.

Q 3: What will be the output of the quantum circuits given in Figure 9.1 and 9.2? Does they produce entangled qubits or not? What are these entangled qubits called?

Q 4: What is maximal entanglement? Write a four-qubit state that is maximally entangled and another four-qubit state that is entangled but not maximally entangled.

Q 5: Show that $\frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{|{+}{+}\rangle + |{-}{-}\rangle}{\sqrt{2}}$

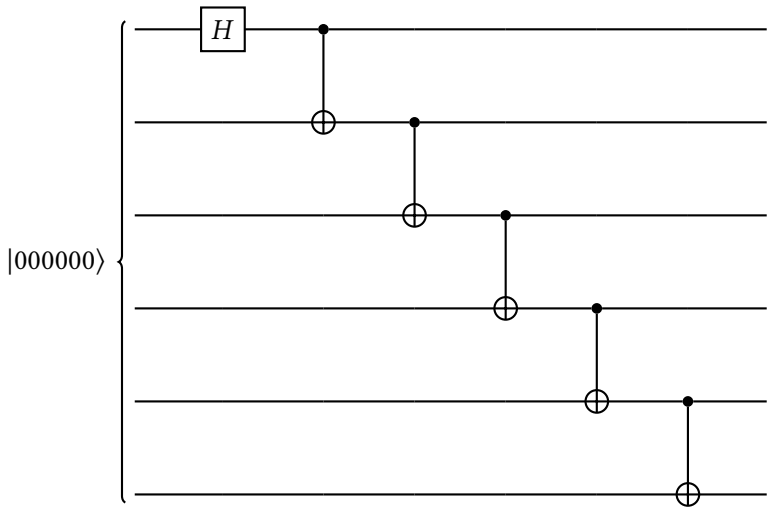


Figure 3.1: Quantum circuit

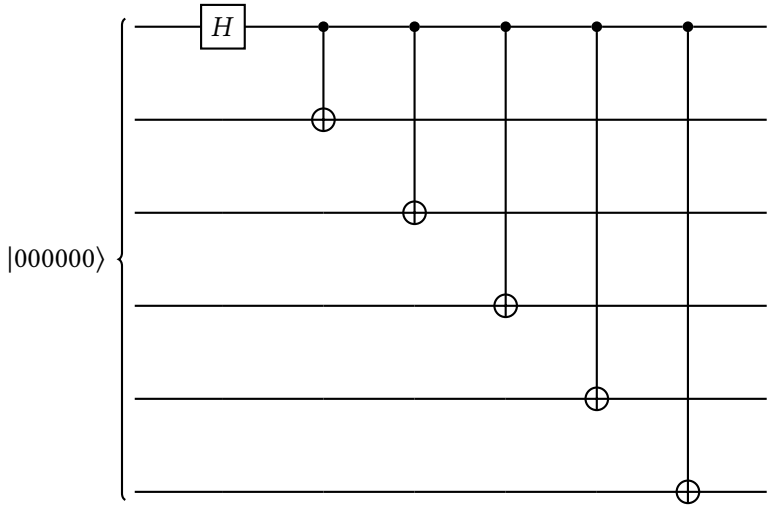


Figure 3.2: Quantum circuit

4 Qubits and their Measurements

4.1 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.

4.1.1 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 $|\frac{i}{\sqrt{3}}|^2 = \frac{-i}{\sqrt{3}} \times \frac{i}{\sqrt{3}} = \frac{1}{3}$

4.1.2 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.

4.2 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.

4.3 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.

4.3.1 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.

4.4 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.

4.4.1 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.

4.4.2 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.

4.5 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.

4.5.1 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.

4.6 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.

4.6.1 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 $\frac{1}{2}$.

5 Assignment # 1: Dirac's Notation and Qubits

Please solve it by hand and submit well before the deadline.

Q 1: Write vector $\begin{pmatrix} 0 \\ 2 \\ 0 \\ 0 \\ -1 \\ 3 \\ 9 \\ 0 \end{pmatrix}$ in Bra-Ket notation. **[1 Mark]**

Q 2: Verify if $|\psi\rangle = \sqrt{\frac{3+i4}{7}}\,|0\rangle + \sqrt{\frac{2}{7}}\,|1\rangle$ is a valid qubit. If so, what are the probabilities of measuring 0 and 1? **[2 Mark]**

Q 3: What are the probabilities of measuring $|\psi\rangle = \sqrt{\frac{3+i4}{7}}\,|0\rangle + \sqrt{\frac{2}{7}}\,|1\rangle$ in basis $\left\{ |+\rangle, |-\rangle \right\}$? **[2 Mark]**

Q 4: What are the probabilities of measuring $|\psi\rangle = \sqrt{\frac{3+i4}{7}}\,|0\rangle + \sqrt{\frac{2}{7}}\,|1\rangle$ in basis $\left\{ \begin{pmatrix} 0 \\ i \end{pmatrix}, \begin{pmatrix} -i \\ 0 \end{pmatrix} \right\}$?

[2 Mark]

Q 5: Write matrix $\begin{pmatrix} -1 & 0 & 9 & 0 \\ 0 & 0 & 0 & 7 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ using Bra-Ket notation. [**2 Mark**]

Q 6: Given $|\psi\rangle = \sqrt{\frac{3+i4}{7}}\,|0\rangle + \sqrt{\frac{2}{7}}\,|1\rangle$ and $|-\rangle$. Find

1. $\langle\psi|-\rangle$ [**2 Mark**]
2. $|\psi\rangle\langle-|$ [**2 Mark**]
3. $\langle\psi|\langle-|$ [**2 Mark**]
4. $|\psi\rangle|-\rangle$ [**2 Mark**]

Q 7) What is $A \otimes B \otimes C$, where $A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $B = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$, and $C = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ [**4 Mark**]

Q 8) Normalized the vector $\begin{pmatrix} 1 \\ 2 \\ 3 \\ 0 \end{pmatrix}$ [**2 Mark**]

Q 9) Given the qubits $|\psi\rangle = \frac{1}{2}|0000\rangle + \frac{1}{2}|0001\rangle + \frac{1}{\sqrt{6}}|0011\rangle + \frac{1}{\sqrt{3}}|1111\rangle$. Create table showing probablity of measurements and resultant states for: **1)** First two qubits measured are 00, **2)** last two qubits measured are 11, **3)** first and fourth qubits measured are 0 and 1 respectively, and **4)** qubits being measured are 0000. **[8 Marks]**

6 Quantum Gates

6.1 Unitary Matrices and Their Properties

Unitary matrices play a fundamental role in quantum computing as they can represent all quantum gates. One of the key reasons for their ubiquity in quantum computations is their ability to preserve the norm of a quantum state vector, ensuring that the sum of probabilities remains equal to 1 even after a quantum gate is applied to a quantum register. Moreover, quantum mechanics demands that all quantum operations must be reversible, a constraint upheld by unitary operations. In this section, we will define unitary matrices and explore their essential properties.

6.1.1 Definition

A square matrix $\mathbf{U}$ is said to be unitary if its conjugate transpose (also known as the Hermitian transpose) is equal to its inverse. Mathematically, a matrix $\mathbf{U}$ is unitary if:

$$\mathbf{U}^\dagger\mathbf{U} = \mathbf{U}\mathbf{U}^\dagger = \mathbf{I},$$

where $\mathbf{U}^\dagger$ represents the conjugate transpose of matrix $\mathbf{U}$, $\mathbf{I}$ is the identity matrix, and $\mathbf{U}^\dagger$ is the inverse of $\mathbf{U}$.

Example: Proving Matrix G is Unitary

To illustrate the concept, let's prove that the matrix

$$G = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

is unitary.

Solution:

To prove that the matrix is unitary, we must show that $G^\dagger G = I$. That is:

$$G^\dagger G = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$$= \frac{1}{4}\begin{pmatrix} \frac{1}{4} & 0 & 0 & 0 \\ 0 & \frac{1}{4} & 0 & 0 \\ 0 & 0 & \frac{1}{4} & 0 \\ 0 & 0 & 0 & \frac{1}{4} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

This proves that G is indeed unitary.

6.1.2 Helpful Videos

There are a series of YouTube videos about properties of unitary matrices that could be very helpful for better understanding:

- Quantum Computing: Properties of Unitary Matrices
- [Quantum Computing: Eigenvalues of a Unitary Matrix Lie on the Unit Circle
- Quantum Computing: What is Diagonalization by a Unitary Similarity?
- Quantum Computing: Example of Diagonalization by Unitary Similarity

Some of the concepts from these videos are explained below.

6.1.3 Reversible Operation

As mentioned earlier, the inverse of a unitary matrix is its conjugate transpose, which is computationally efficient to calculate compared to the inverse of a general matrix. Unitary matrices represent reversible operations in quantum computing. This means that when we apply a unitary operator to a quantum state represented as $|\psi\rangle$, we can always undo or revert that operation. Mathematically, for a unitary operation $|\psi\rangle\, U = |\phi\rangle$, we can reverse it by applying the adjoint (also known as the conjugate transpose) of the unitary operator, denoted as $U^\dagger$, to $|\phi\rangle$, resulting in $|\phi\rangle\, U^\dagger = |\psi\rangle$.

The reversibility of unitary matrices is a fundamental property in quantum computing, and it implies that every quantum gate is reversible. This property is essential in quantum computation because it allows us to manipulate quantum states without losing information, making quantum algorithms inherently reversible.

Furthermore, when we construct a quantum circuit by composing various quantum gates and operations, the entire quantum circuit also represents a reversible operation. This reversibility is a distinguishing feature of quantum computation compared to classical computation, where irreversible operations are common.

6.1.4 Norm Preserving

Unitary matrices exhibit a crucial property known as norm preservation. This property signifies that the magnitude or norm of a quantum state vector remains unchanged after undergoing a unitary operation. In other words, applying a unitary matrix to a quantum state does not alter the length or normalization of that state. Let's delve into the proof of this important property.

Theorem 6.1. *A unitary matrix* **U** *preserves the norm of a vector. Specifically, for a quantum state* $|\psi\rangle$*, we have* $||\,|\psi\rangle\,|| = ||U\,|\psi\rangle\,||$.

Proof. Let's examine both the left-hand side and the right-hand side of the equation to demonstrate their equality.

$$
\begin{aligned}
||\,|\psi\rangle\,|| &= ||U\,|\psi\rangle\,|| \\
\sqrt{\langle\psi|\psi\rangle} &= \sqrt{(U\,|\psi\rangle)^{\dagger}U\,|\psi\rangle} \\
\sqrt{\langle\psi|\psi\rangle} &= \sqrt{\langle\psi|\,U^{\dagger}U\,|\psi\rangle} \\
\sqrt{\langle\psi|\psi\rangle} &= \sqrt{\langle\psi|\,I\,|\psi\rangle} \\
\sqrt{\langle\psi|\psi\rangle} &= \sqrt{\langle\psi|\psi\rangle}
\end{aligned}
$$

By the definition of unitary matrices, we know that $U^{\dagger}U = I$. Substituting this property into the right-hand side of the equation, we observe that both sides are indeed equal. This rigorous proof establishes that unitary matrices maintain the norm of a quantum state vector. □

The norm preserving property of unitary matrices holds great significance in quantum computing. It ensures that the fundamental normalization constraint of qubits remains intact, even as they undergo a series of unitary operations. This property is fundamental to the stability and reliability of quantum algorithms and quantum information processing, as it guarantees that quantum states remain valid and consistent throughout quantum computations.

6.1.5 Orthonormal Columns and Row Basis

Unitary matrices possess a remarkable property where both their columns and rows form orthonormal bases. This implies that each column of a unitary matrix satisfies the following conditions:

- It is a unit vector (i.e., its magnitude is 1).
- It is orthogonal to all the other columns in the matrix.
- It is linearly independent from the other columns.

Similarly, the rows of a unitary matrix also constitute an orthonormal basis. Let's provide a formal proof of this property:

Theorem 6.2. *The cols of a unitary matrix U are orthonormal.*

Proof. By the definition of a unitary matrix: $U^\dagger U = I$, let's expand upon this definition. Assume c_i donates the ith column of the matrix

$$U^\dagger U = I$$

$$\begin{pmatrix} c_1 & c_2 & c_3 & \vdots \\ c_n & & & \end{pmatrix}^\dagger \begin{pmatrix} c_1 & c_2 & c_3 & \vdots \\ c_n & & & \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

$$\begin{pmatrix} \langle c_1|c_1\rangle & \langle c_1|c_2\rangle & \langle c_1|c_3\rangle & \cdots & \langle c_1|c_n\rangle \\ \langle c_2|c_1\rangle & \langle c_2|c_2\rangle & \langle c_2|c_3\rangle & \cdots & \langle c_2|c_n\rangle \\ \langle c_3|c_1\rangle & \langle c_3|c_2\rangle & \langle c_3|c_3\rangle & \cdots & \langle c_3|c_n\rangle \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \langle c_n|c_1\rangle & \langle c_n|c_2\rangle & \langle c_n|c_3\rangle & \cdots & \langle c_n|c_n\rangle \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

From the expansion of the unitary matrix definition, we deduce that the inner product of two distinct columns, i.e., $\langle c_i|c_j\rangle$ where $i \neq j$, is always equal to zero. This implies that the columns are orthogonal to each other. Furthermore, the inner product of a column with itself, i.e., $\langle c_i|c_i\rangle$, is always equal to 1. This implies that each column is a unit vector. Thus, we conclude that the columns of a unitary matrix collectively form an orthonormal set. □

This property underscores the significance of unitary matrices in quantum computing, as they provide a foundation for constructing orthonormal bases and facilitating various quantum operations and transformations.

6.1.6 Other properties

There are many other unitary matrices properties that will be useful to master quantum computing. Below we breify mention those properties without going in details. **Students are encouraged to do an example of each of these property as a question may come in the midterm.**

1. **Eigenvalues**: The eigenvalues of a unitary matrix have a magnitude of 1. This property is a direct consequence of the definition of unitary matrices. Eigenvalues with magnitude 1 are often associated with rotations or phase shifts. Please see this video for proof of it.
2. **Determinant**: The determinant of a unitary matrix has a magnitude of 1. This follows from the property that the product of eigenvalues is equal to the determinant, and since the eigenvalues have a magnitude of 1, the determinant must also have a magnitude of 1.
3. **Angle Preserving** The angle-preserving property of a unitary matrix is a fundamental characteristic that plays a vital role in quantum computing. Essentially, it signifies that when a unitary matrix operates on vectors, it preserves the angles between those vectors. In other words, if you have two quantum states represented as vectors and you apply a unitary transformation to them, the relative angles between these vectors will remain unchanged. This property is significant because it ensures that the geometric relationships and structural properties of quantum states are conserved during quantum computations. Angle preservation contributes to the stability and predictability of quantum algorithms and is one of the key reasons unitary matrices are a fundamental tool in quantum information processing. Please see this video for proof of it.

6.2 Hermitian Matrices

In quantum computing, Hermitian matrices play a fundamental role, especially in the context of quantum mechanics and quantum algorithms. A Hermitian matrix is a complex square matrix that is equal to its own conjugate transpose. Mathematically, a matrix H is Hermitian if it satisfies the following condition:

$$H = H^\dagger$$

Here, $H^\dagger$ denotes the conjugate transpose of matrix H.

Hermitian matrices are crucial for several reasons in quantum computing:

6.2.1 Observables

In quantum mechanics, physical observables such as position, momentum, and energy are represented by Hermitian operators. These operators have real eigenvalues, and their eigenvectors correspond to the possible states of a quantum system. Observables are at the heart of quantum measurements and are used to extract information from quantum states.

6.2.2 Quantum States

Quantum states are typically represented as complex vectors in a Hilbert space. Density matrices, which describe mixed quantum states, are Hermitian matrices. They are essential for modeling the behavior of quantum systems when there is uncertainty or a statistical mixture of pure quantum states.

> The above concepts will be explained in detail in a separate chapter dedicated to observables and density matrices.

6.2.3 Quantum Gates

In quantum computing, unitary operators are used to perform quantum operations, and many of these operators are represented by Hermitian matrices. For example, Hadamard, Pauli-X, Pauli-Y, and Pauli-Z gates are Hermitian operators. Hermitian gates are also used in quantum error correction and various quantum algorithms.

> When a quantum gate is Hermitian, the unitary matrix representing that gate is the inverse of itself.

6.2.4 Quantum Algorithms

Several quantum algorithms, such as quantum eigensolvers and quantum phase estimation, heavily rely on Hermitian matrices. These algorithms leverage the properties of Hermitian matrices to solve complex computational problems more efficiently than classical counterparts.

In summary, Hermitian matrices are a foundational concept in quantum computing, forming the basis for representing physical observables, quantum states, and quantum gates. Understanding Hermitian matrices is essential for anyone studying or working in the field of quantum computing.

6.3 Vital Quantum Gates

There are numerous quantum gates, and covering all of them is beyond the scope of these notes. This section limits itself to discussing some of the most vital and commonly used quantum gates that form the foundation of quantum computing.

6.3.1 Hadamard Gate (H)

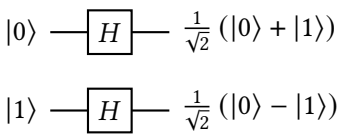
The Hadamard gate is one of the fundamental gates in quantum computing. It is represented by the matrix:

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

It creates superposition. Applying the Hadamard gate to the pure states of $|0\rangle$ and $|1\rangle$ results in a equal superposition states of $|+\rangle$ and $|-\rangle$, respectively:

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

Graphically, the Hadamard gate is represented as follows:



6.3.2 Pauli-X Gate (X)

The Pauli-X gate, also known as the quantum NOT gate, is represented by the matrix:

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

It flips the quantum state. Applying the Pauli-X gate to $|0\rangle$ and $|1\rangle$ results in:

$$X|0\rangle = |1\rangle$$
$$X|1\rangle = |0\rangle$$

6.3.3 Pauli-Y Gate (Y)

The Pauli-Y gate is represented by the matrix:

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

It introduces a phase change and a bit flip. Applying the Pauli-Y gate to $|0\rangle$ and $|1\rangle$ results in:

$$Y|0\rangle = i|1\rangle$$
$$Y|1\rangle = -i|0\rangle$$

6.3.4 Pauli-Z Gate (Z)

The Pauli-Z gate is represented by the matrix:

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

It introduces a phase change without altering the basis states. Applying the Pauli-Z gate to $|0\rangle$ and $|1\rangle$ results in:

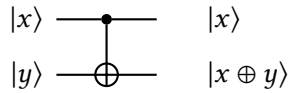
$$Z|0\rangle = |0\rangle$$
$$Z|1\rangle = -|1\rangle$$

6.3.5 CNOT Gate (CNOT)

The Controlled-NOT (CNOT) gate is a two-qubit gate that performs an X gate on the second qubit (target) if the first qubit (control) is in the $|1\rangle$ state. It is represented as:

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

The CNOT gate is crucial for implementing entanglement and building quantum circuits for various quantum algorithms.



Applying the CNOT gate to different initial states produces different results:

$$\text{CNOT}(|00\rangle) = |00\rangle$$
$$\text{CNOT}(|01\rangle) = |01\rangle$$
$$\text{CNOT}(|10\rangle) = |11\rangle$$
$$\text{CNOT}(|11\rangle) = |10\rangle$$

These are just a few of the vital quantum gates that serve as building blocks for quantum algorithms and quantum computation. Understanding their properties and how to apply them is essential for harnessing the power of quantum computing.

6.4 Hadamard Gate Generalization

For this section please watch Hadamard Gate's General Expression. A single hadamard gate works a follows:

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{6.1}$$

We can write above two equations of Hadamard gate into a single equation as follows:

Given $a \in \{0, 1\}$

$$H|a\rangle = \frac{|0\rangle + (-1)^a |1\rangle}{\sqrt{2}}, \tag{6.2}$$
$$H|a\rangle = \frac{1}{\sqrt{2}} \sum_{b\in\{0,1\}} (-1)^{a\cdot b} |b\rangle \tag{6.3}$$
$$\tag{6.4}$$

6.4.1 Multiple Qubits Gates

For two qubits we build on the single qubits as follows:

Given $x \in \{0, 1\}^2$

$$(H \otimes H)|x\rangle = H^{\otimes 2}|x\rangle = \left(\frac{1}{\sqrt{2}} \sum_{y_1\in\{0,1\}} (-1)^{x_1\cdot y_1} |y_1\rangle\right) \cdot \left(\frac{1}{\sqrt{2}} \sum_{y_2\in\{0,1\}} (-1)^{x_2\cdot y_2} |y_2\rangle\right)$$

Combining both together we get:

$$H^{\otimes 2}|x\rangle = \frac{1}{\sqrt{2^2}} \sum_{y\in\{0,1\}^2} (-1)^{x_1\cdot y_1 + x_2\cdot y_2} |y\rangle$$

We may write $x_1 \cdot y_1 + ... + x_n \cdot y_n = x \cdot y$ thus above becomes

$$H^{\otimes 2} |x\rangle = \frac{1}{\sqrt{2^2}} \sum_{y \in \{0,1\}^2} (-1)^{x \cdot y} |y\rangle$$

Similarly, for n-qubits

Given $x \in \{0,1\}^n$

$$H^{\otimes n} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle$$

6.4.2 Example

What is $H^{\otimes 3} |101\rangle =$?

Solution

$$H^{\otimes 3} |x\rangle = \frac{1}{\sqrt{2^3}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle$$

$$H^{\otimes 3} |101\rangle = \frac{1}{\sqrt{2^3}} \Big[(-1)^{1.0+0.0+1.0} |000\rangle + (-1)^{1.0+0.0+1.1} |001\rangle + (-1)^{1.0+0.1+1.0} |010\rangle + (-1)^{1.0+0.1+1.1} |011\rangle +$$
$$(-1)^{1.1+0.0+1.0} |100\rangle + (-1)^{1.1+0.0+1.1} |101\rangle + (-1)^{1.1+0.1+1.0} |110\rangle + (-1)^{1.1+0.1+1.1} |111\rangle \Big]$$

$$H^{\otimes 3} |101\rangle = \frac{1}{\sqrt{2^3}} \Big[|000\rangle - |001\rangle + |010\rangle - |011\rangle - |100\rangle + |101\rangle - |110\rangle + |111\rangle \Big]$$

Lets verify above answer using matrices. Longer and more painful alternative method.

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad H \otimes H = \frac{1}{\sqrt{2^2}} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$$H \otimes H \otimes H = \frac{1}{\sqrt{2^3}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}$$

I have to find $H^{\otimes 3} |101\rangle$ which be

$$\frac{1}{\sqrt{2^3}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2^3}} \begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \\ -1 \\ 1 \\ -1 \\ 1 \end{pmatrix}$$

Answers from both methods are the same. Hence, verified that our solution is correct.

7 Assignment 2: Quantum Gates and Circuits

Please solve the following tasks manually and ensure timely submission well before the deadline. Kindly refrain from requesting a late submission, as such requests will not be accommodated. This video might help in solving this assignment Quantum Computing #8: Quantum Circuit Example

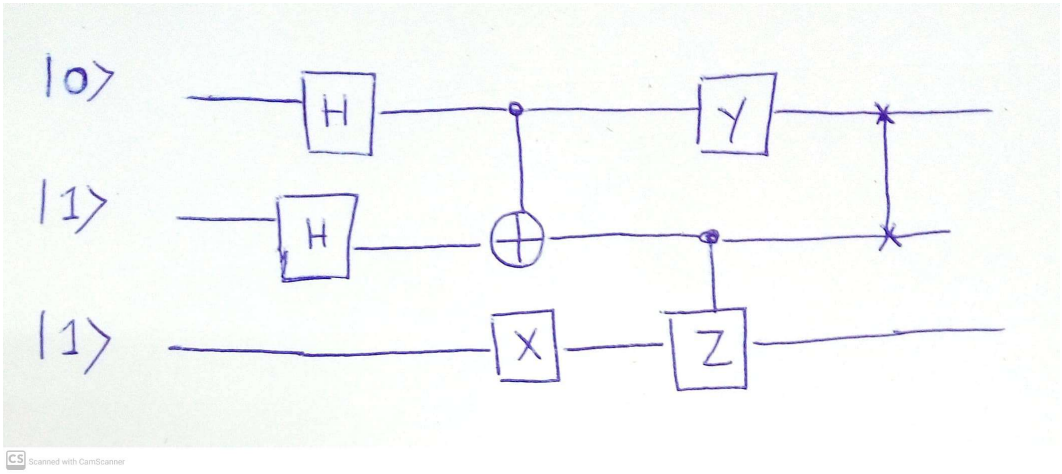


Figure 7.1: A simple quantum circuit

Question 1: Determine the output of the quantum circuit depicted in Figure 7.1.

a) Present your calculations using Bra-ket notation. **[5 Marks]**

b) Demonstrate your calculations using matrices. **[5 Marks]**

Question 2: Construct a unitary matrix that represents the aforementioned circuit. **[5 Marks]**

Question 3: Develop a reverse quantum circuit. **[5 Marks]**

Question 4: Create a unitary matrix that represents the reverse quantum circuit. **[5 Marks]**

Question 5: Write a brief explanation regarding the inherent reversibility of quantum circuits. Additionally, design a concise classical circuit that is not reversible. **[5 Marks]**

Question 6: Calculate the output of $H^{\otimes 3} |110\rangle$. **[5 Marks]**

8 Entanglement

A set of qubits is considered quantum entangled when their probabilities are dependent on each other, preventing their separate expression. Entanglement can be described using its two fundamental properties:

1. State of entangled qubits cannot be described individually.
2. Measuring one qubit of the entangled qubits reveals information about the others.

8.1 Bell Basis

Entangled states for two qubits are famously known as Bell states, collectively forming the Bell basis. These states are also referred to as EPR states, named after the pioneering scientists Einstein, Podolsky, and Rosen, who first discovered them.

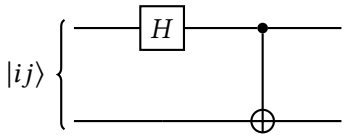


Figure 8.1: Circuit Generating the Bell Basis

Bell Basis :

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$
$$|\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$
$$|\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$
$$|\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

The circuit that generates all the Bell states is shown in Figure 8.1. A Bell state is entangled because the qubits within it depend on each other, making it impossible to express them separately. This implies that any two entangled qubits cannot be written in the form $(\alpha|0\rangle + \beta|1\rangle)(\gamma|0\rangle + \delta|1\rangle)$. Let's prove this for the Bell state β_{00}.

8.2 Entanglement Proof

Theorem 8.1. *For any valid α, β, γ, and δ, the equation*

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \neq (\alpha|0\rangle + \beta|1\rangle)(\gamma|0\rangle + \delta|1\rangle)$$

holds, demonstrating the entanglement of these qubits.

Proof. We prove this by contradiction. Let's assume that

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} = (\alpha|0\rangle + \beta|1\rangle)(\gamma|0\rangle + \delta|1\rangle)$$
$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle$$

For equality to hold, $\alpha\delta = 0$ must be true. This means that at least one of α and δ must be zero. If $\alpha = 0$, the amplitude of $|00\rangle$ becomes zero instead of $\frac{1}{\sqrt{2}}$, so α cannot be zero. Similarly, if $\gamma = 0$, the amplitude of $|11\rangle$ becomes zero instead of $\frac{1}{\sqrt{2}}$, so γ cannot be zero either. This contradiction proves that our assumption is incorrect; hence, $\frac{|00\rangle+|11\rangle}{\sqrt{2}} \neq (\alpha|0\rangle + \beta|1\rangle)(\gamma|0\rangle + \delta|1\rangle)$. □

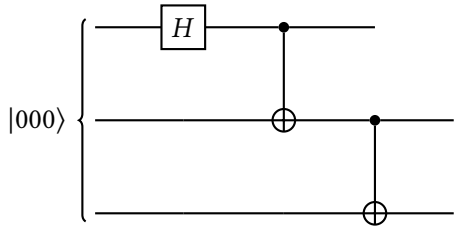


Figure 8.2: Quantum circuit to produce GHZ states

8.3 GHZ States

In addition to two-qubit entanglement, we have tripartite entanglement, referred to as GHZ states, named after scientists Daniel **G**reenberger, Michael **H**orne, and Anton **Z**eilinger, who studied four-particle entanglement and explained GHZ states. The circuit to create GHZ states is shown in Figure 8.2. In this case, measuring any qubit will reveal information about the others with certainty. Furthermore, the amplitudes of these qubits cannot be expressed separately.

8.4 Quantum Teleportation

Quantum teleportation enables the transmission of a **single qubit** by conveying only two classical bits, provided that both parties share a Bell state. For a more in-depth understanding, you can refer to this video: Quantum Teleportation.

8.4.1 The Story

Imagine Ali and Babar, who have previously shared a Bell state denoted as β_{00}. Ali possesses the first qubit of this Bell state, while Babar holds the second qubit. Now, let's introduce a twist to the story – Babar relocates to North Korea. At some point, Ali desires to transmit a highly valuable qubit, denoted as $|\psi\rangle$, to Babar, all while keeping this transfer clandestine. Achieving this seemingly impossible task involves Ali measuring his portion of the Bell state and the valuable qubit $|\psi\rangle$. Based on the measurement results, Ali sends two classical bits to Babar, who then performs specific operations on his Bell state to miraculously recreate $|\psi\rangle$.

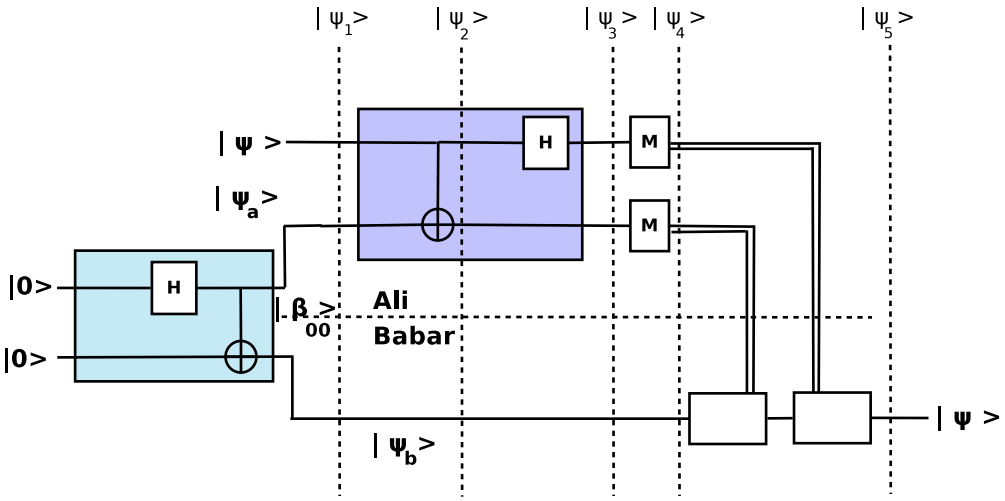


Figure 8.3: Quantum Teleportation

8.4.2 Circuit and Mathematics

The quantum teleportation process is depicted in Figure 8.3 above. To understand how this circuit operates, let's examine how the input qubit transforms as it passes through the circuit. Suppose the qubit Ali wishes to transmit to Babar is $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

Initially, Ali and Babar have the following qubits:

$$
\begin{aligned}
|\psi_1\rangle &= |\psi\rangle\,|\beta_{00}\rangle \\
|\psi_1\rangle &= (\alpha|0\rangle + \beta|1\rangle)\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right) \\
|\psi_1\rangle &= \frac{\alpha}{\sqrt{2}}|000\rangle + \frac{\alpha}{\sqrt{2}}|011\rangle + \frac{\beta}{\sqrt{2}}|100\rangle + \frac{\beta}{\sqrt{2}}|111\rangle
\end{aligned}
$$

Note that the first two qubits belong to Ali, while the last qubit belongs to Babar. Ali then passes his qubit through a CNOT gate, resulting in:

$$
|\psi_2\rangle = \frac{\alpha}{\sqrt{2}}|000\rangle + \frac{\alpha}{\sqrt{2}}|011\rangle + \frac{\beta}{\sqrt{2}}|110\rangle + \frac{\beta}{\sqrt{2}}|101\rangle
$$

Next, Ali applies a Hadamard operation to his first qubit:

$$
\begin{aligned}
|\psi_3\rangle &= \frac{\alpha}{\sqrt{2}}\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}|00\rangle\right) + \frac{\alpha}{\sqrt{2}}\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}|11\rangle\right) + \frac{\beta}{\sqrt{2}}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}|10\rangle\right) + \frac{\beta}{\sqrt{2}}\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}|01\rangle\right) \\
|\psi_3\rangle &= \frac{1}{2}\left[\alpha\left(|0\rangle + |1\rangle\right)|00\rangle + \alpha\left(|0\rangle + |1\rangle\right)|11\rangle + \beta\left(|0\rangle - |1\rangle\right)|10\rangle + \beta\left(|0\rangle - |1\rangle\right)|01\rangle\right] \\
|\psi_3\rangle &= \frac{1}{2}\left[\alpha|000\rangle + \alpha|100\rangle + \alpha|011\rangle + \alpha|111\rangle + \beta|010\rangle - \beta|110\rangle + \beta|001\rangle - \beta|101\rangle\right] \\
|\psi_3\rangle &= \frac{1}{2}\left[|00\rangle\left(\alpha|0\rangle + \beta|1\rangle\right) + |01\rangle\left(\alpha|1\rangle + \beta|0\rangle\right) + |10\rangle\left(\alpha|0\rangle - \beta|1\rangle\right) + |11\rangle\left(\alpha|1\rangle - \beta|0\rangle\right)\right]
\end{aligned}
$$

Ali then measures his first two qubits, and Table 2 below shows Ali's possible measurements and the resulting superposition of Babar's unmeasured qubit.

Based on Ali's measurements, Babar determines the operations to apply to his superposition without measuring his qubit. Babar's logic for applying operations and the corresponding operations are provided in Table 3.

Thus, after applying operations, the $|\psi_5\rangle$ that Babar creates will be exactly the intended qubit $|\psi\rangle$ that Ali wanted to send. Magical!

Ali's Measurement	Babar's Superposition
00	$\alpha \|0\rangle + \beta \|1\rangle$
01	$\alpha \|1\rangle + \beta \|0\rangle$
10	$\alpha \|0\rangle - \beta \|1\rangle$
11	$\alpha \|1\rangle - \beta \|0\rangle$

Table 8.1: $|\psi_4\rangle$ after partial measurements

Classical Bits Received	Babar's Logic	Babar's Operations
00	My superposition will be exactly $\|\psi\rangle$, so no further action is needed.	$\|\psi_5\rangle = I \|\psi_b\rangle$
01	My superposition needs to swap amplitudes, achieved using a NOT (i.e., X) gate.	$\|\psi_5\rangle = X \|\psi_b\rangle$
10	My superposition requires changing the sign of the amplitude associated with $\|1\rangle$ while keeping the rest unchanged. This is accomplished using a Z gate.	$\|\psi_5\rangle = Z \|\psi_b\rangle$
11	My superposition needs to be first swapped using an X gate and then have the sign of $\|1\rangle$ changed with a Z gate.	$\|\psi_5\rangle = ZX \|\psi_b\rangle$

Table 8.2: $|\psi_5\rangle$ Babar operations

8.4.3 What Quantum Teleportation is NOT!

1. **Qubit Cloning**: It does not clone a qubit as a qubit that Ali had was destroyed in the process.
2. **Faster than Speed of Light Communication**: It does not give us faster-than-speed-of-light communication as we have to transmit two classical bits using the same old method. Without transmitting those classical bits, Babar has no way of knowing what operations to perform to create $|\psi\rangle$.

8.5 Superdense Coding

The protocol of Superdense coding allows sending **two classical bits** by transmitting only a **single qubit**. It is explained in video https://youtu.be/o2AuL6mxGiE.

The circuit diagram of Superdense coding is shown in Figure 8.4. Let's calculate the outcomes of each $|\psi_i\rangle$ to see how the Superdense coding circuit works.

$$|\psi_1\rangle = |00\rangle$$
$$|\psi_2\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

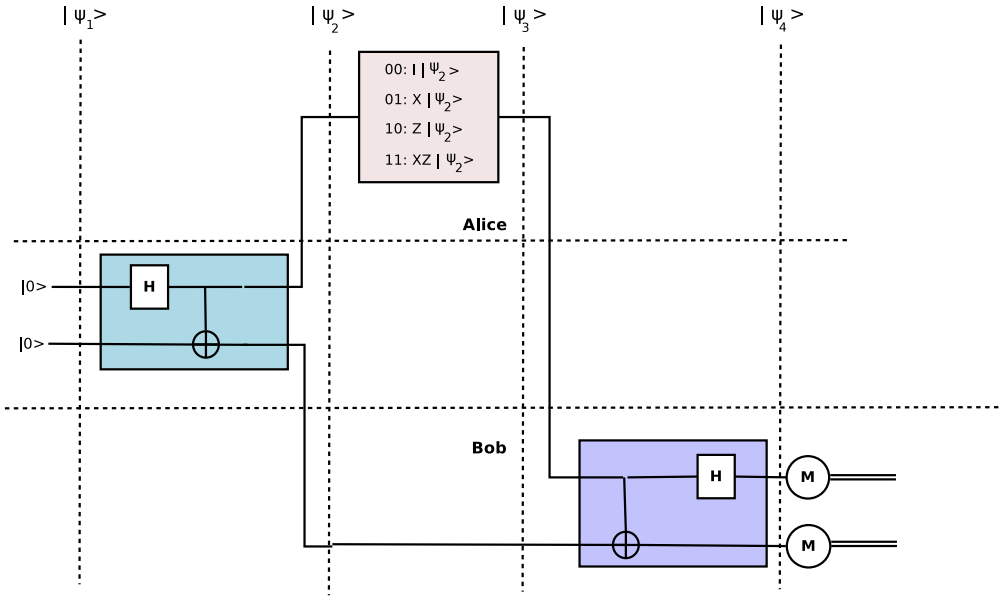


Figure 8.4: Circuit diagram of Superdense coding

Alice applies different transformation depending upon what he wants to send. These transformations are shown in Table 8.3.

Bob applies final transformations as shown in Table 8.4.

Finally, Bob measures qubits and gets the output send by Alice with 1 probability.

Alice is sending	**Result**
00	$\frac{\|00\rangle+\|11\rangle}{\sqrt{2}}$
01	$\frac{X\|0\rangle\|0\rangle+X\|1\rangle\|1\rangle}{\sqrt{2}} = \frac{\|1\rangle\|0\rangle+\|0\rangle\|1\rangle}{\sqrt{2}} = \frac{\|10\rangle+\|01\rangle}{\sqrt{2}}$
10	$\frac{Z\|0\rangle\|0\rangle+Z\|1\rangle\|1\rangle}{\sqrt{2}} = \frac{\|0\rangle\|0\rangle-\|1\rangle\|1\rangle}{\sqrt{2}} = \frac{\|00\rangle-\|11\rangle}{\sqrt{2}}$
11	$\frac{XZ\|0\rangle\|0\rangle+XZ\|1\rangle\|1\rangle}{\sqrt{2}} = \frac{X\|0\rangle\|0\rangle-X\|1\rangle\|1\rangle}{\sqrt{2}} = \frac{\|10\rangle-\|01\rangle}{\sqrt{2}}$

Table 8.3: $|\psi_3\rangle$.

Bob has received	**CNOT**	**H on 1st qubit**
$\frac{\|00\rangle+\|11\rangle}{\sqrt{2}}$	$\frac{\|00\rangle+\|10\rangle}{\sqrt{2}}$	$\|00\rangle$
$\frac{\|10\rangle+\|01\rangle}{\sqrt{2}}$	$\frac{\|11\rangle+\|01\rangle}{\sqrt{2}}$	$\|01\rangle$
$\frac{\|00\rangle-\|11\rangle}{\sqrt{2}}$	$\frac{\|00\rangle-\|10\rangle}{\sqrt{2}}$	$\|10\rangle$
$\frac{\|10\rangle-\|01\rangle}{\sqrt{2}}$	$\frac{\|11\rangle-\|01\rangle}{\sqrt{2}}$	$-\|11\rangle$

Table 8.4: $|\psi_4\rangle$.

9 Assignment 3: Entanglement

Q 1: Prove whether the following qubits are entangled or not. In case they are not entangled, **express each qubit state separately**.

a) $\frac{1}{\sqrt{3}}|00\rangle + \sqrt{\frac{2}{3}}|11\rangle$

b) $\frac{1}{\sqrt{3}}\big(|001\rangle + |010\rangle + |100\rangle\big)$

c) $\sqrt{\frac{2}{5}}|000\rangle + \sqrt{\frac{3}{5}}|111\rangle$

d) $\frac{|{+}{+}\rangle + |{-}{-}\rangle}{\sqrt{2}}$

e) $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{3}}|01\rangle + \frac{1}{\sqrt{6}}|10\rangle$

Q 2: In the quantum teleportation circuit, if we use the Bell state B_{11} instead of B_{00}, can we still achieve quantum teleportation? Show all the steps while highlighting any changes needed to make it work.

Q 3: What will be the output of the quantum circuits given in Figure 9.1 and 9.2? Does they produce entangled qubits or not? What are these entangled qubits called?

Q 4: What is maximal entanglement? Write a four-qubit state that is maximally entangled and another four-qubit state that is entangled but not maximally entangled.

Q 5: Show that $\frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{|{+}{+}\rangle + |{-}{-}\rangle}{\sqrt{2}}$

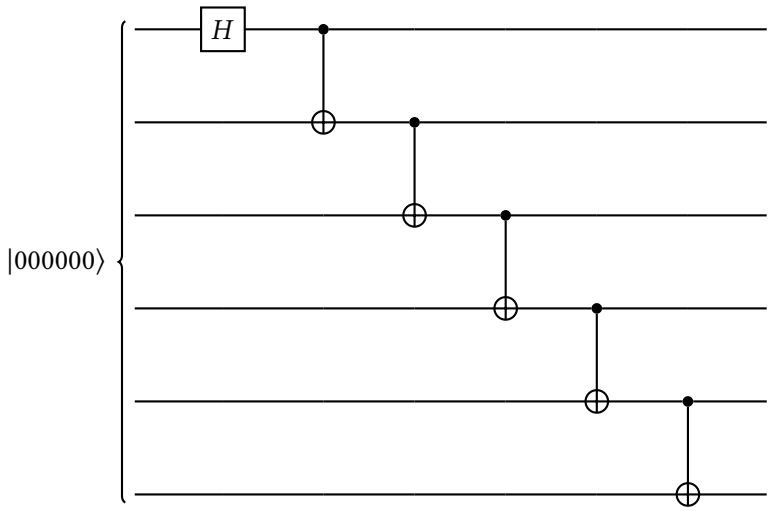


Figure 9.1: Quantum circuit

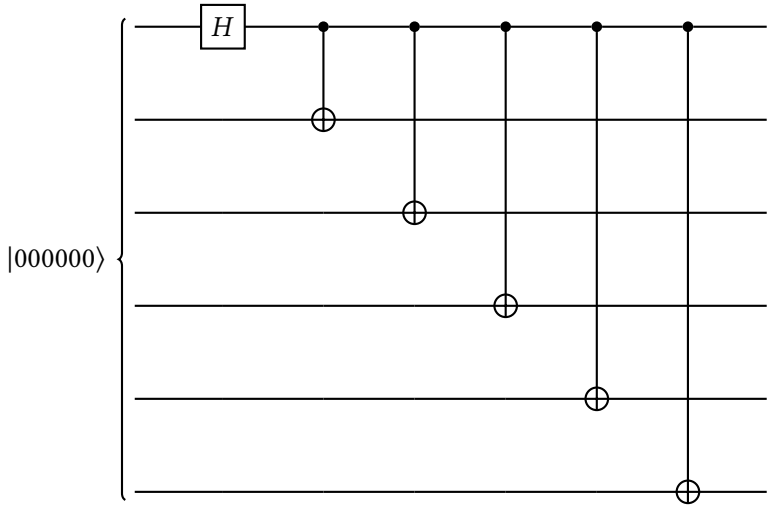


Figure 9.2: Quantum circuit

10 Simon's Algorithm

Simon's algorithm addresses Simon's Problem, defined as follows:

10.1 Simon's Problem

Given a function $f : \{0,1\}^n \rightarrow \{0,1\}^n$, the objective is to find $s \in \{0,1\}^n$ such that $f(x) = f(x \oplus s)$. If $f(x) \neq f(x')$, then $x \oplus x' \neq s$.

x	$f(x)$
000	101
001	101
010	110
011	110
100	101
101	101
110	110
111	110

Table 10.1: Example function f with $s = 101$

Special case: In the event $s = 000$, the function will be one-to-one, with each output being unique and not matching any other input's output.

10.2 YouTube Videos

There are three YouTube videos that describe Simon's problem, explain all of its math, and given a detailed example.

- Problem Definition
- Circuit of Simon's Algorithm
- Example of Simon's Algorithm

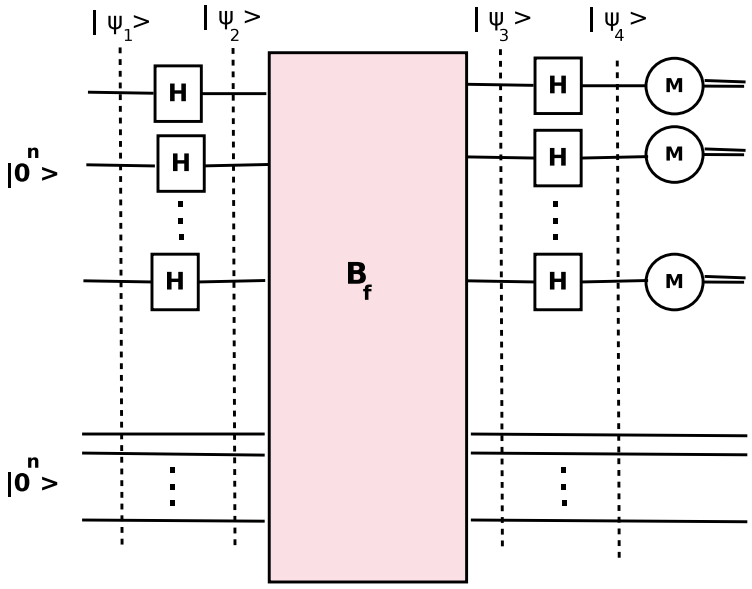


Figure 10.1: The circuit for the Simon's algorithm

10.3 Complexity

On a classical computer, solving this problem would require approximately $\Omega(\sqrt{2^n})$ operations due to the Birthday paradox when using randomized algorithms. This results in exponential running time. Conversely, a quantum computer can solve it with just $O(n)$ calls to f, providing an exponential speedup.

10.4 Circuit

The circuit for Simon's algorithm is depicted in Figure 10.1. Here, the function B_f is defined as follows:

$$B_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$$

where $x \in \{0,1\}^n$ and $y \in \{0,1\}^n$ are both n-bit numbers.

10.5 Math for Simon's Algorithm

Let's examine how the input evolves as it propagates through the circuit shown in Figure 10.1.

The initial input is:

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

Next, the first n-qubits undergo a Hadamard transformation:

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

All qubits are then subjected to the function B_f:

$$|\psi_3\rangle = B_f |\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |0^n \oplus f(x)\rangle$$

Since $0 \oplus b = b$, we simplify to:

$$|\psi_3\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle$$

Here, we measure the second register containing the last n qubits. This changes the state of the first register due to partial measurement.

Let $f(z)$ represent the measurement of the second register. Measuring the second register places the first register in a superposition with inputs to f that yield $f(z)$. Specifically, for output $f(z)$, these inputs will be z and $z \oplus s$.

$$|\psi_4\rangle = \left(\frac{1}{\sqrt{2}} |z\rangle + \frac{1}{\sqrt{2}} |z \oplus s\rangle \right) |f(z)\rangle$$

Disregarding the second register, we have:

$$|\psi_4\rangle = \left(\frac{1}{\sqrt{2}} |z\rangle + \frac{1}{\sqrt{2}} |z \oplus s\rangle \right)$$

Subsequently, we apply a Hadamard transformation to the second register:

$$|\psi_5\rangle = H^{\otimes n} |\psi_4\rangle = \frac{1}{\sqrt{2}} H |z\rangle + \frac{1}{\sqrt{2}} H |z \oplus s\rangle$$

Where:

$$H |x\rangle = \frac{1}{2^{n/2}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle$$

This simplifies to:

$$|\psi_5\rangle = \sum_{y\in\{0,1\}^n} \frac{1}{\sqrt{2^{n+1}}} \left((-1)^{y\cdot z} + (-1)^{y\cdot(z\oplus s)}\right)|y\rangle$$

And further simplifies to:

$$|\psi_5\rangle = \sum_{y\in\{0,1\}^n} \frac{1}{\sqrt{2^{n+1}}} \left((-1)^{y\cdot z} + (-1)^{(y\cdot z)\oplus(y\cdot s)}\right)|y\rangle$$

Applying Theorem **??**, which states that $x^a + x^b = x^a(1 + x^{a\oplus b})$ when $a, b \in \{0,1\}^n$, we arrive at:

$$|\psi_5\rangle = \sum_{y\in\{0,1\}^n} \frac{1}{\sqrt{2^{n+1}}}(-1)^{y\cdot z}\left(1 + (-1)^{y\cdot s}\right)|y\rangle$$

Knowing that $a \oplus a = 0$ and $a \oplus 0 = a$, we further simplify:

$$|\psi_5\rangle = \sum_{y\in\{0,1\}^n} \frac{1}{\sqrt{2^{n+1}}}(-1)^{y\cdot z}\left(1 + (-1)^{y\cdot s}\right)|y\rangle$$

Case 1: $y \cdot s = 1$

$$|\psi_5\rangle = \sum_{y\in\{0,1\}^n} \frac{1}{\sqrt{2^{n+1}}}(-1)^{y\cdot z}\left(1 + (-1)^{1}\right)|y\rangle$$
$$|\psi_5\rangle = 0\,|y\rangle$$

Therefore, the probability of $y \cdot s = 1$ is zero, meaning it cannot occur.

Case 2: $y \cdot s = 0$

$$|\psi_5\rangle = \sum_{y\in\{0,1\}^n} \frac{1}{\sqrt{2^{n+1}}}(-1)^{y\cdot z}\left(1 + (-1)^{0}\right)|y\rangle$$
$$|\psi_5\rangle = \sum_{y\in\{0,1\}^n} \frac{1}{\sqrt{2^{n+1}}}(-1)^{y\cdot z}\,|y\rangle$$

The amplitude of each y with $y \cdot s = 0$ is $\pm\frac{1}{2^{(n-1)/2}}$, indicating that each y with $y \cdot s = 0$ is equally likely, and no other value except such a y is possible.

10.6 Post-Measurement Math

The algorithm is repeated with the aim of collecting $n-1$ distinct linearly independent y values.

The system of equations to solve is:

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

This is converted into a row-echelon form:

$$\left(\begin{array}{cccc|c} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Solving it using back substitution:

$$s_4 = 1$$

(it was a free variable set to 1).

$$s_3 = s_4 = 0$$
$$s_1 + s_4 = 0$$

Solving above we get:

$$\begin{aligned} s_1 &= -s_4 \\ s_1 &= -1 \mod 2 \\ s_1 &= 1 \end{aligned}$$

Thus, the solution is $s = 1001$, as expected. In the case where $s_4 = 0$, we obtain the trivial solution $s = 0000$.

11 Assignment 4: QFT and Quantum Algorithms

Please solve the following tasks manually and ensure timely submission well before the deadline. Kindly refrain from requesting a late submission, as such requests will not be accommodated.

x	f(x)
00	1
01	1
10	1
11	1

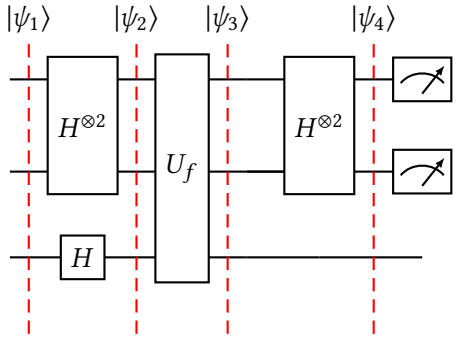


Figure 11.1: **(a)** Classical function inputs/outputs, **(b)** Deutsch-Jozsa Quantum circuit

1. A classical function $f : \{0,1\}^n \rightarrow \{0,1\}$ for the 2-bits case is described in a table in Figure 11.1-a. The quantum gate U_f implements the classical circuit such that $U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$. What will be the output of the Deutsch-Jozsa circuit of Figure 11.1-b given its input is $|00\rangle |1\rangle$? You must clearly show output of $|\psi_1\rangle$, $|\psi_2\rangle$, $|\psi_3\rangle$, and $|\psi_4\rangle$ (Otherwise no marks). [**1+2+2+2 Marks**]

2. Given a function f that takes n-bits as input and produces a single bit output, what is the exact probability of finding an input x such that $f(x) = 1$ using Grover's algorithm? Please provide your answer for n=4, n=5, n=6, and n=8. In each cases, it is known that exactly 4 inputs return 1. You must clearly show your working to derive the correct equation. [**5 Marks**]

3. Apply Simon's algorithm on 2-bits input and secret message $s = 11$.
   a) Create it quantum circuit, [**2 Marks**]
   b) Show output of each of possible five stages clearly. [**1+2+2+2+2 Marks**].
   c) Must show post output calculations including matrix transformation.[**4 Marks**]

4. What will be the outcome of the following operation. Use tablular approach discuss in class to quickly solve it. $H^{\otimes 4}(\frac{-|0000\rangle+|0101\rangle-|1101\rangle+|1110\rangle-|1111\rangle}{\sqrt{5}})$

5. Given a function $f(x) = 2x + 1 \mod 7$ where x is of 4-bits. Find its period using period

finding algorithm. Show every step clearly as there are no mark of writing period which is 4. [**10 Marks**]

6. Using an input $\frac{1}{\sqrt{3}}\begin{pmatrix}1\\1\\0\\-1\end{pmatrix}$, show that quantum Fourier transform convert linear shift to phase shift. Must show use linear shift of 1 and 3. [**5 Marks**]

7. Using an input $\frac{1}{\sqrt{3}}\begin{pmatrix}1\\1\\0\\-1\end{pmatrix}$, show that quantum Fourier transform convert phase shift to linear shift. Must show use two different phase shifts. [**5 Marks**]

8. Given a function $f(x) = 2x - 1 \mod 7$ where x is of 4-bits. Show that quantum Fourier transform changes its period. Drive and show what will be the changed period. (No mark for answer, all marks are for showing your work). [**7 Marks**]

9. Prove that quantum Fourier transform is unitary. [**5 Marks**]

10. Write inverse of quantum Fourier transform 8×8 bit matrix. Write each term as simplified as possible. [**5 Marks**]

12 Fourier Transformation

Joseph Fourier was a French mathematician born in 1768. He devised Fourier transformation which has been widely used in multiple areas and have numerous applications. This chapter explains discrete Fourier transformation.

12.1 Sinusoidal function

A sinusoidal function represents different transformations of sine function, $\sin(x)$, including, change in its amplitude, phase shift, period, and vertical shift. Figure 12.1 shows sine function it is originality without any transformation. Different parameters of the Sinusoidal Equation 12.1 may be adjusted to create desire transformation.

$$f(x) = a \cdot \sin(b(x - c)) + d \tag{12.1}$$

Amplitude Amplitude of sinusoidal function is half of the difference between maximum and minimum value of y coordinate. Thus amplitude of sine function is $\frac{1}{2}[1 - (-1)] = 1$. Amplitude of sinusoidal function may be altered by changing the value of parameter a of Equation 12.1. For instance, sinusoidal function with amplitude equals to 2 is shown in Figure 12.2a.

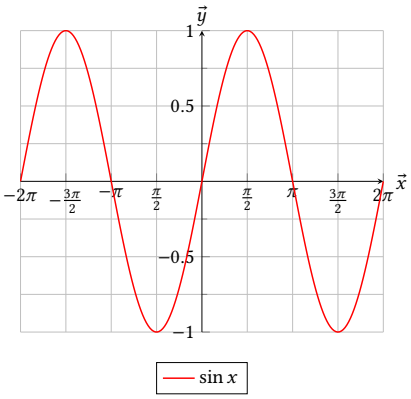
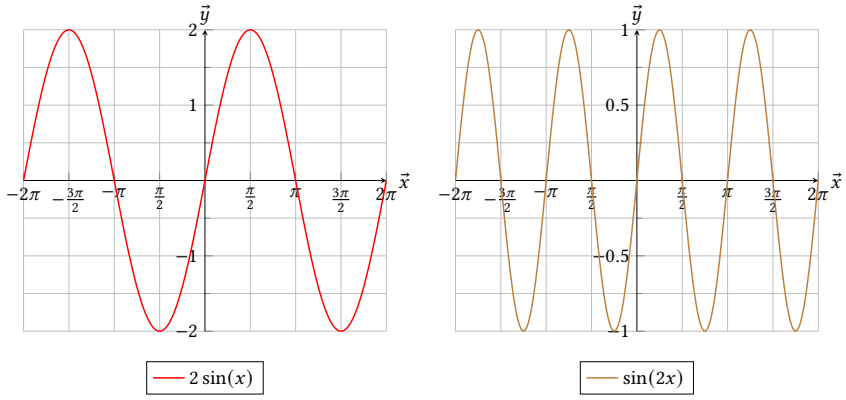
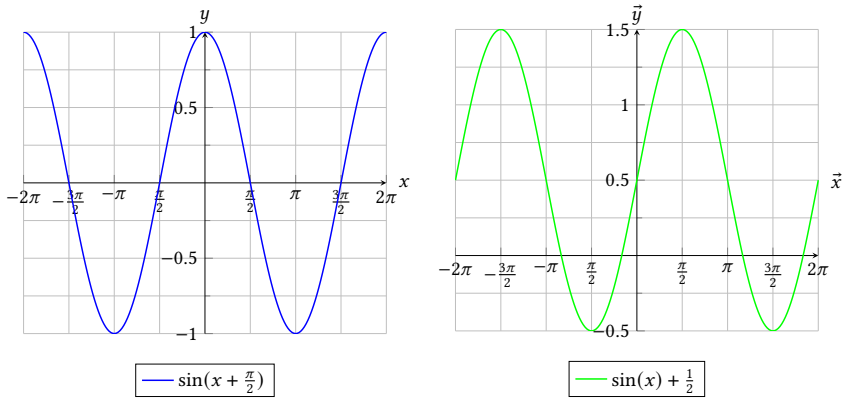


Figure 12.1: Sine function



(a) Amplitude Increased (b) Period Decreased



(c) Left Phase Shift (d) Upward Vertical Shift

Figure 12.2: Transformations of Sinusoidal function

Period Period of a function refers to the interval after which the function repeat itself. In other words it is distance on the x-axis before the function repeat itself. Thus, period of sine function (Figure 12.1) is 2π radians. The period of a sinusoidal function is given by $\frac{2\pi}{|b|}$ (recall sine base periodicity was 2π). For example, period of function $3\sin(4(x-2))+5$ is given by $\frac{2\pi}{|4|} = \frac{\pi}{2}$ or 90 degrees. Figure 12.2b draw a sinusoidal function $\sin(2x)$ which has period π which is half the period of original sine function.

Phase shift The phase shift refers to the angle shifted of the graph along x-axis. In other words it is how much a graph has moved either left or right from its original location. In Equation 12.1 the variable c refers to the phase shift. The sign of variable c if positive then the function move towards right otherwise it moves towards left. For example phase shift of $-\frac{\pi}{2}$ makes the sinusoidal graph move 90 degrees to left making it a cosine graph. This is illustrated in Figure 12.2c.

Vertical shift Beside having horizontal shift along x-axis (a.k.a phase shift), we can also move sinusoidal function vertically. For this parameter d of Equation 12.1 is used. In case d is positive, the graph moves upwards otherwise it moves downwards. Figure 12.2d show a upwards vertical shift of 0.5. Note that the amplitude remains the same instead only the function has move upwards (along y-axis).

Frequency Frequency is the number of cycles that occur in 2π. A shorter period means more cycles can fit in 2π and thus a higher frequency. Period and frequency are inversely related by the equation: $period = \frac{2\pi}{frequency}$.

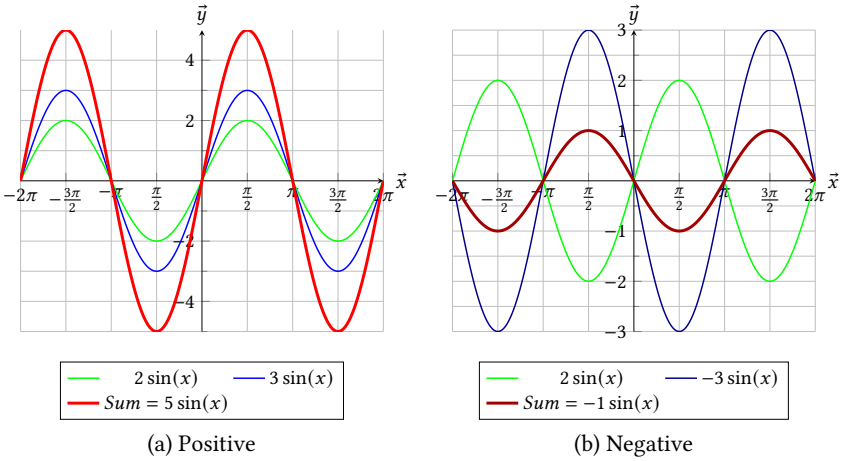
12.2 Summation of Sinusoidal function

When we add two sinusoidal waves, f_1 and f_2, then their interference produces new signals f_{1+2}. We call interference of two signal **positive interference** when the sum signal f_{1+2} has higher amplitude than amplitudes of both f_1 and f_2. Similarly, interference of two signal (f_1 and f_2) is termed as **negative interference** when the signal representing their sum, f_{1+2}, has lower amplitude. The interference of sinusoidal waves is illustrated in Figure 12.3.

Adding two sinusoidal waves of different periods or phases produces new waves which are not sine waves. In fact, using addition of multiple sinusoidal waves one can produce any possible wave of any function. However, some waves may be created only using infinite sinusoidal waves.

12.3 Key idea of Fourier transform

Given that graph of every time-domain function is composed of sinusoidal waves. Fourier transformation, decompose that function into multiple sinusoidal waves and then express it in frequency-domain. This is illustrated in Figure 12.4. Discrete Fourier transformation do that by



(a) Positive (b) Negative

Figure 12.3: Interference of Sinusoidal waves

mapping all the values of function onto a circle and taking average of the transformed values. More details about it will be added later on (*next week*).

12.4 Discrete Fourier transformation

Fourier transform has a plethora of applications in various fields, including signal processing, noise separation, and quantum computing.

n^{th} root of unity:

The equation $z^n = 1$ has n solutions, called root of unity. They all lie on the circumference of unit complex circle. These roots can be written as $\omega = e^{-2\pi i/n}$. The complex number ω is called n^{th} root of unity.

Discreet Fourier transform (DFT) is defined as:

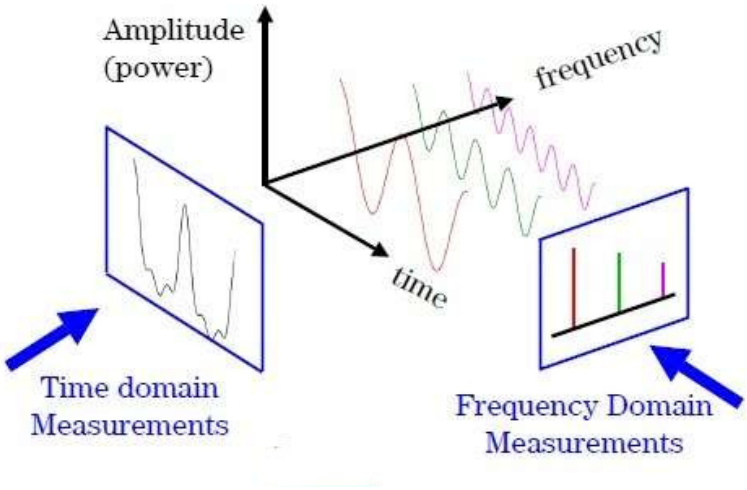


Figure 12.4: Time-domain function to Frequency-domain function conversion.

$$F_n = \frac{1}{\sqrt{n}} \begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \dots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \dots & \omega^{2n-1} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \dots & \omega^{3n-1} \\ . & . & . & . & \dots & . \\ . & . & . & . & \dots & . \\ . & . & . & . & \dots & . \\ 1 & \omega^{n-1} & \omega^{2n-2} & \omega^{3n-3} & \dots & \omega^{(n-1)(n-1)} \end{pmatrix}$$

Basically, The jkth entry of matrix is defined as $\omega^{(j-1)\times(k-1)}$. Thus,

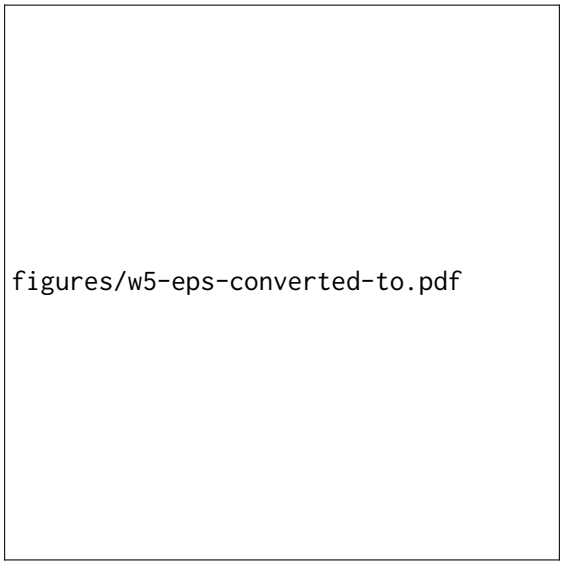


Figure 12.5: The 5 complex 5^{th} root of unity.

$$F_n = \frac{1}{\sqrt{n}} \begin{pmatrix} \omega^{0\times 0} & \omega^{0\times 1} & \omega^{0\times 2} & \omega^{0\times 3} & \dots & \omega^{0\times n-1} \\ \omega^{1\times 0} & \omega^{1\times 1} & \omega^{1\times 2} & \omega^{1\times 3} & \dots & \omega^{1\times n-1} \\ \omega^{2\times 0} & \omega^{2\times 1} & \omega^{2\times 2} & \omega^{2\times 3} & \dots & \omega^{2\times n-1} \\ . & . & . & . & \dots & . \\ . & . & . & . & \dots & . \\ . & . & . & . & \dots & . \\ \omega^{(n-1)\times 0} & \omega^{(n-1)\times 1} & \omega^{(n-1)\times 2} & \omega^{(n-1)\times 3} & \dots & \omega^{(n-1)\times (n-1)} \end{pmatrix}$$

Angles

The angle of ω is $2\pi/n$. If we square ω then angle is doubled. Similarly, if we cube ω then it angles is multiplied by three and so on.

Modular

The entries of discrete Fourier transform matrix are modular. That is all the entries in DFT matrix are from ω to ω^{n-1} where each entry of higher power can be mapped into one of such entry. In particular, for F_n

$$m^k = m^k \mod n$$

Example

All the solutions of $z^5 = 1$ are multiple of the 5^{th} root of unity is $\omega = e^{-2\pi i/5}$. As shown in Figure 12.5 these solutions lies on the complex unit circle.

For n=5 discreet Fourier matrix is as follows:

$$F_5 = \frac{1}{\sqrt{5}} \begin{pmatrix} \omega^{0\times0} & \omega^{0\times1} & \omega^{0\times2} & \omega^{0\times3} & \omega^{0\times4} \\ \omega^{1\times0} & \omega^{1\times1} & \omega^{1\times2} & \omega^{1\times3} & \omega^{1\times4} \\ \omega^{2\times0} & \omega^{2\times1} & \omega^{2\times2} & \omega^{2\times3} & \omega^{2\times4} \\ \omega^{3\times0} & \omega^{3\times1} & \omega^{3\times2} & \omega^{3\times3} & \omega^{3\times4} \\ \omega^{4\times0} & \omega^{4\times1} & \omega^{4\times2} & \omega^{4\times3} & \omega^{4\times4} \end{pmatrix} = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 \\ 1 & \omega^2 & \omega^4 & \omega^6 & \omega^8 \\ 1 & \omega^3 & \omega^6 & \omega^9 & \omega^{12} \\ 1 & \omega^4 & \omega^8 & \omega^{12} & \omega^{16} \end{pmatrix}$$

Now, we use modular arithmetic to simplify the matrix entries.

After simplification, all the entries in DFT_n will be from ω^0 to ω^{n-1}

$$F_5 = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 \\ 1 & \omega^2 & \omega^4 & \omega^1 & \omega^3 \\ 1 & \omega^3 & \omega^1 & \omega^4 & \omega^2 \\ 1 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{pmatrix} = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 \\ 1 & \omega^2 & \omega^4 & \omega & \omega^3 \\ 1 & \omega^3 & \omega & \omega^4 & \omega^2 \\ 1 & \omega^4 & \omega^3 & \omega^2 & \omega \end{pmatrix}$$

Example

Write F_8 matrix in simplified form.

Solution

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

We know that for F_8, $\omega^k = \omega^{k \mod 8}$. Applying this simplification we get:

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

where $\omega = e^{-\frac{2\pi i}{8}} = \frac{1}{\sqrt{2}} - \frac{i}{\sqrt{2}}$

12.5 Properties of DFT

Very important. To be written!

12.6 Fast Fourier transformation

Discrete Fourier transformation takes $\Theta(n^2)$ time to transform a vector of size n. Thus, may not be feasible to use of vectors of few gigabytes dimensions. Thankfully, we have Fast Fourier

transformation (FFT) that takes only $\Theta(n \log n)$ time to transform vector of size n which is significantly fast as compared to DFT. In this section, I explain the working of FFT.

FFT decompose matrix F_n into $\log_2(n) + 1$ matrices

Any DFT matrix F_{2n} may be decompose into $\log_2(2n) + 1$ matrices as:

$$F_{2n} = \begin{bmatrix} I_n & D_n \\ I_n & -D_n \end{bmatrix} \begin{bmatrix} F_n & 0 \\ 0 & F_n \end{bmatrix} P$$

Here I_n represents identity matrix of $n \times n$ dimensions. Matrix P is an $2n \times 2n$ permutation matrix is defined as follows:

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & 0 & \dots & 0 \\ & & & . & & & \\ & & & . & & & \\ & & & . & & & \\ 0 & 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1 & 0 & \dots & 0 \\ & & & . & & & \\ & & & . & & & \\ & & & . & & & \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

Matrix D is an $n \times n$ matrix:

$$D = \begin{pmatrix} \omega^0 & 0 & 0 & 0 & \dots & 0 \\ 0 & \omega^1 & 0 & 0 & \dots & 0 \\ 0 & 0 & \omega^2 & 0 & \dots & 0 \\ & & . & & & \\ & & . & & & \\ & & . & & & \\ 0 & 0 & 0 & 0 & \dots & \omega^{n-1} \end{pmatrix}$$

Example

Decompose F_4 into FFT matrices.

Solution

$$F_4 = \frac{1}{\sqrt{4}} \begin{bmatrix} I_2 & D_2 \\ I_2 & -D_2 \end{bmatrix} \begin{bmatrix} F_2 & 0 \\ 0 & F_2 \end{bmatrix} P$$

$$F_4 = \frac{1}{\sqrt{4}} \begin{pmatrix} 1 & 0 & \omega^0 & 0 \\ 0 & 1 & 0 & \omega^1 \\ 1 & 0 & -\omega^0 & 0 \\ 0 & 1 & 0 & -\omega^1 \end{pmatrix} \begin{bmatrix} F_2 & 0 \\ 0 & F_2 \end{bmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

We do not further decompose F_2. That is our recursion stops at F_2.

$$F_4 = \frac{1}{\sqrt{4}} \begin{pmatrix} 1 & 0 & \omega_4^0 & 0 \\ 0 & 1 & 0 & \omega_4^1 \\ 1 & 0 & -\omega_4^0 & 0 \\ 0 & 1 & 0 & -\omega_4^1 \end{pmatrix} \begin{pmatrix} \omega_2^0 & \omega_2^0 & 0 & 0 \\ \omega_2^0 & \omega_2^1 & 0 & 0 \\ 0 & 0 & \omega_2^0 & \omega_2^0 \\ 0 & 0 & \omega_2^0 & \omega_2^1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$F_4 = \frac{1}{\sqrt{4}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -i \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & i \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Example

Decompose F_8 into FFT matrices.

Solution

$$F_8 = \frac{1}{\sqrt{8}} \begin{bmatrix} I_4 & D_4 \\ I_4 & -D_4 \end{bmatrix} \begin{bmatrix} F_4 & 0 \\ 0 & F_4 \end{bmatrix} P$$

$$F_8 = \frac{1}{\sqrt{8}} \begin{pmatrix} 1 & 0 & 0 & 0 & \omega_8^0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & \omega_8^1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & \omega_8^2 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & \omega_8^3 \\ 1 & 0 & 0 & 0 & \omega_8^4 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & \omega_8^5 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & \omega_8^6 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & \omega_8^7 \end{pmatrix} \begin{bmatrix} F_4 & 0 \\ 0 & F_4 \end{bmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

The middle matrix provides me a template to put two F_4 matrices $\begin{pmatrix} I_2 & D_2 \\ I_2 & -D_2 \end{pmatrix}$ and $\begin{pmatrix} F_2 & 0 \\ 0 & F_2 \end{pmatrix}$ in diagonals whereas the rest of entries will be zero.

$$F_8 = \frac{1}{\sqrt{8}} \begin{pmatrix} 1 & 0 & 0 & 0 & \omega_8^0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & \omega_8^1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & \omega_8^2 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & \omega_8^3 \\ 1 & 0 & 0 & 0 & \omega_8^4 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & \omega_8^5 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & \omega_8^6 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & \omega_8^7 \end{pmatrix} \begin{pmatrix} I_2 & D_2 & 0 & 0 \\ I_2 & -D_2 & 0 & 0 \\ 0 & 0 & I_2 & D_2 \\ 0 & 0 & I_2 & -D_2 \end{pmatrix} \begin{pmatrix} F_2 & 0 & 0 & 0 \\ 0 & F_2 & 0 & 0 \\ 0 & 0 & F_2 & 0 \\ 0 & 0 & 0 & F_2 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Now, we just have to fill the entries of those matrices. However, be careful that we have to write entries corresponding to F_8, F_4 and F_2 in term using the Figure 12.6. Thus, we get the following.

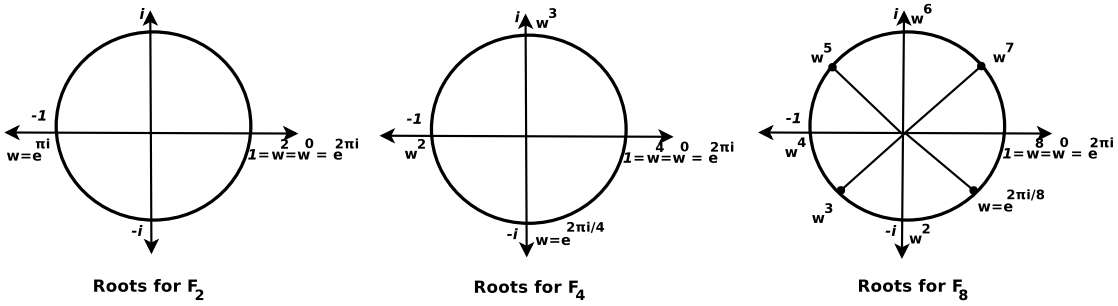


Figure 12.6: The complex roots for F_2, F_4, and F_8. Note, ω^i of F_n is equal to ω^{2i} of F_{2n}

$$F_8 = \frac{1}{\sqrt{8}} \begin{pmatrix} 1 & 0 & 0 & 0 & \omega_8^0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & \omega_8^1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & \omega_8^2 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & \omega_8^3 \\ 1 & 0 & 0 & 0 & \omega_8^4 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & \omega_8^5 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & \omega_8^6 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & \omega_8^7 \end{pmatrix} \times \begin{pmatrix} 1 & 0 & \omega_4^0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & \omega_4^1 & 0 & 0 & 0 & 0 \\ 1 & 0 & \omega_4^2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & \omega_4^3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & \omega_4^0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & \omega_4^1 \\ 0 & 0 & 0 & 0 & 1 & 0 & \omega_4^2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & \omega_4^3 \end{pmatrix} \times$$

$$\begin{pmatrix} \omega_2^0 & \omega_2^0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \omega_2^0 & \omega_2^1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \omega_2^0 & \omega_2^0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \omega_2^0 & \omega_2^1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \omega_2^0 & \omega_2^0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \omega_2^0 & \omega_2^1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \omega_2^0 & \omega_2^0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \omega_2^0 & \omega_2^1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Finally, I replace ω_l^k values.

$$F_8 = \frac{1}{\sqrt{8}} \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & \omega & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -i & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -i\omega \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & -\omega & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & i & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & i\omega \end{pmatrix} \times \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -i & 0 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & i & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -i \\ 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & i \end{pmatrix} \times$$

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

12.7 Performance of FFT

Instead of single $n \times n$ DFT matrix in FFT we have $\log_2 n + 1$ matrices each of dimension $n \times n$. That is F_8 when converted into FFT then it has $\log_2 8 + 1 = 3 + 1 = 4$ matrices. FFT create more matrices but these matrices are sparse, having all entries, but two, are zeros. In this section we show that it is actually much faster to use these multiple sparse matrices than a single dense matrix.

12.7.1 Butterfly Multiplication

Multiplication of two complex number $a + bi$ and $c + di$ requires four normal multiplications and four additions. That is $a \times c$, $a \times di$, $bi \times c$, and $bi \times di$. FFT uses Butterfuly computation where each Butterfly computation produces two new complex numbers by only performing four multiplications and six additions [?]. Butterfly computation is illustrated in Figure 12.7. In the figure p, q, and r are all complex numbers. Two new complex number are produced ($p + qr$, $p - qr$) by a single complex multiplication of $q \times r$. As we know single complex multiplication is

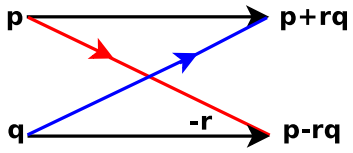
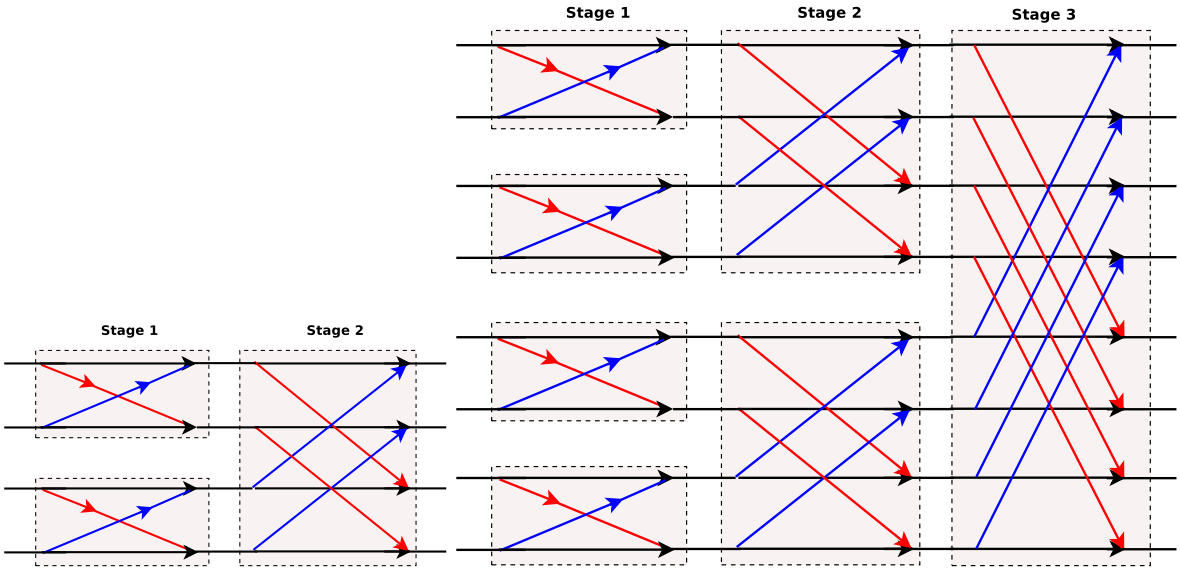


Figure 12.7: The Butterfly multiplication with complex numbers p, q, and r.

composed of four normal multiplications and four additions. Furthermore two more additions are carried out to create $p + qr$ and $p - qr$, thus making in total four multiplication and six addition in the creating of two new complex numbers.



(a) F_4 (b) F_8

Figure 12.8: Butterfly diagrams

Each fast Fourier transform can be written in terms of butterfly multiplications.

Figure 12.8a demonstrates the connections between butterfly for F_4. In the figure you can see that a butterfly at $State\ i$ makes a connection between two butterflies of $Stage\ i - 1$. Same will be the case with any state of any butterfly diagram.

To label butterfly diagram, at a $Stage\ k$, you use powers of $\omega_m = e^{\frac{2\pi i}{m}}$, where $m = 2^k$ The labeled butterfly diagram of F_8 is shown in Figure 12.9.

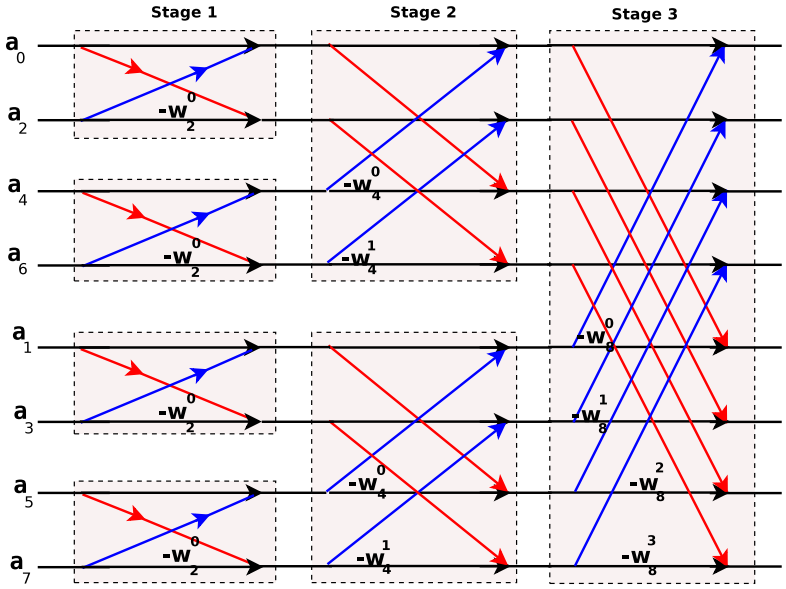


Figure 12.9: Labeled diagram for F_8.

Now, notice that for F_n we will have $\log_2 n$ stages where each stage has exactly $\frac{n}{2}$ butterflies. Thus, total number of butterflies in a complete diagram for F_n will be $\frac{n}{2} \times \log_2 n$. As each butterfly has 4 multiplication and 6 additions hence total number of multiplications and additions in the complete butterfly diagram will be $4 \times \frac{n}{2} \times \log_2 n$ and $6 \times \frac{n}{2} \times \log_2 n$, respectively.

Example

Apply butterfly of F_8 on input $|1\rangle + |3\rangle + |5\rangle + |7\rangle$ and clearly showing outputs of each stage separately.

Solution

In the following answer, I show result stage-by-stage. Please re-see Figure 12.7 to recall how a butterfly works. Furthermore, also recall that $\{w_2^0 = 1, w_2^1 = 1\}$, $\{w_4^0 = 1, w_4^1 = -i\}$, and $\{w_8^0 = 1, w_8^1 = w, w_8^2 = -i, w_8^3 = -iw\}$. The stage-by-stage output of the input on F_8 butterfly diagram is given in Figure 12.10.

The output of the butterfly diagram is $\begin{pmatrix} 4 \\ 0 \\ 0 \\ 0 \\ -4 \\ 0 \\ 0 \\ 0 \end{pmatrix}$. In case of Fourier that output will have to be divided by $\sqrt{4} \times \sqrt{8}$. It is because the input will be normalized as $\frac{|1\rangle+|3\rangle+|5\rangle+|7\rangle}{\sqrt{4}}$ whereas Fourier matrix itself will be normalized by multiplying it with $\frac{1}{\sqrt{8}}$. Thus, the output for Fourier matrix F_8 will be $\frac{|0\rangle-|4\rangle}{\sqrt{2}}$.

Lets verify that using the following example.

Example

Apply normalized input $\frac{|1\rangle+|3\rangle+|5\rangle+|7\rangle}{\sqrt{4}}$ to the F_8 matrix and show that final result will be $\frac{|0\rangle-|4\rangle}{\sqrt{2}}$.

Solution

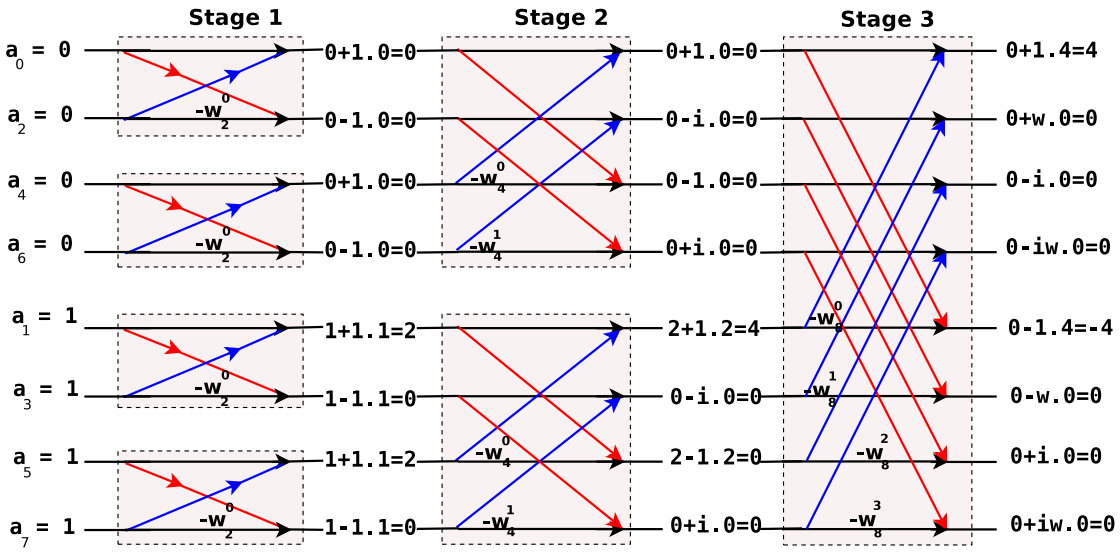


Figure 12.10: Input $|1\rangle + |3\rangle + |5\rangle + |7\rangle$ is applied on F_8 butterfly diagram.

$$F_8 \frac{|1\rangle+|3\rangle+|5\rangle+|7\rangle}{\sqrt{4}}$$

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

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 12.6.

Thus, after applying above two simplification we get:

$$\frac{1}{\sqrt{32}} \begin{pmatrix} 1+1+1+1 \\ w+\omega^3+\omega^5+\omega^7 \\ \omega^2+\omega^6+\omega^{10}+\omega^{14} \\ \omega^3+\omega^9+\omega^{15}+\omega^{21} \\ \omega^4+\omega^{12}+\omega^{20}+\omega^{28} \\ \omega^5+\omega^{15}+\omega^{25}+\omega^{35} \\ \omega^6+\omega^{18}+\omega^{30}+\omega^{42} \\ \omega^7+\omega^{21}+\omega^{35}+\omega^{49} \end{pmatrix} = \frac{1}{\sqrt{32}} \begin{pmatrix} 1+1+1+1 \\ w-iw-w+iw \\ -i-1+i+1 \\ -iw+w+iw-w \\ -1-1-1-1 \\ -w+iw+w-iw \\ i-i+i-i \\ iw-w-iw+w \end{pmatrix} = \frac{1}{\sqrt{32}} \begin{pmatrix} 4 \\ 0 \\ 0 \\ 0 \\ -4 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \sqrt{\frac{16}{32}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ -1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \frac{|0\rangle-|4\rangle}{\sqrt{2}}$$

Answer

12.8 Practice Questions

Q 1: Write F_{16} discrete Fourier matrix.

Q 2: Make butterfly diagram of F_{16} Fourier matrix from scratch and label it.

Q 3: Make butterfly diagram of F_{16} Fourier matrix using already existing blocks of F_8 butterfly diagram.

Q 4: Compute $F_8 \frac{|0\rangle+|2\rangle+|7\rangle}{\sqrt{3}}$.

Q 5: Write Fast Fourier transformation matrices for F_{16}.

Q 6: Create a table to show the total number of additions when discrete Fourier is used as compared to fast Fourier transformation. The table should have entries for $\{F_4, F_8, \ldots, F_{256}\}$.

Q 7: Compute $F_8 \frac{|0\rangle+|2\rangle+|7\rangle}{\sqrt{3}}$ by using F_8 butterfly diagram. Must show what is the output of each stage separately and clearly.

Q 8: Write as well as draw sinusoidal function whose amplitude is decreased 3 times, period is increased 2 times, shifted down by 2 times, and phase is shifted *right* by 3 times.

Solution
Use may use this site https://www.symbolab.com/graphing-calculator to confirm your answer. For you the answer is shown in Figure 12.11.

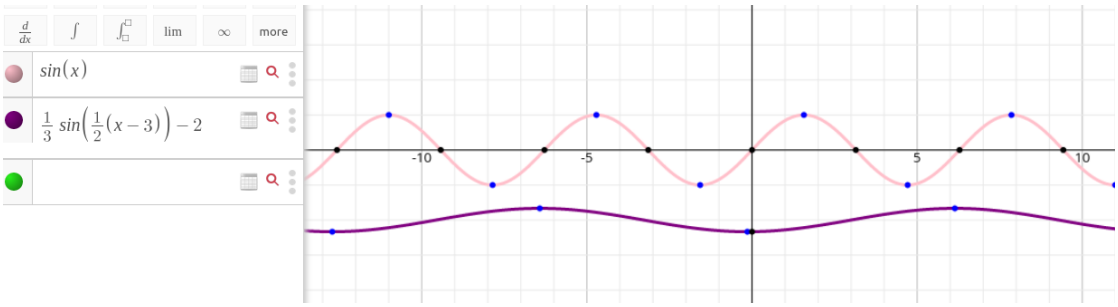


Figure 12.11: Answer of above question

Q 9: What is the period and phase of $7\sin(2x+4)-3$ sinusoidal function.

Solution:

First I convert above equation in the form $f(x) = a \cdot \sin(b(x-c)) + d$.

The above function will become $7\sin(2(x+2))-3$. Thus, the period is $\frac{2\pi}{2} = \pi$. Period of the function is π. **Answer**

13 Period Finding Algorithm

13.1 Problem definition

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

13.2 Background

Period finding is based on two of the Fourier transform properties. These properties are described in detailed in Section 12.5, and repeated briefly below.

1. In case, the period of a function $g : \{0,1\}^n \rightarrow \{0,1\}^n$ 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 $\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} = |1\rangle$

13.3 Circuit diagram

The circuit of period finding algorithm is shown in Figure 13.1. It is similar to Simon's algorithm circuit diagram Figure 10.1. 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 $H^{\otimes n}$.

13.4 Working

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

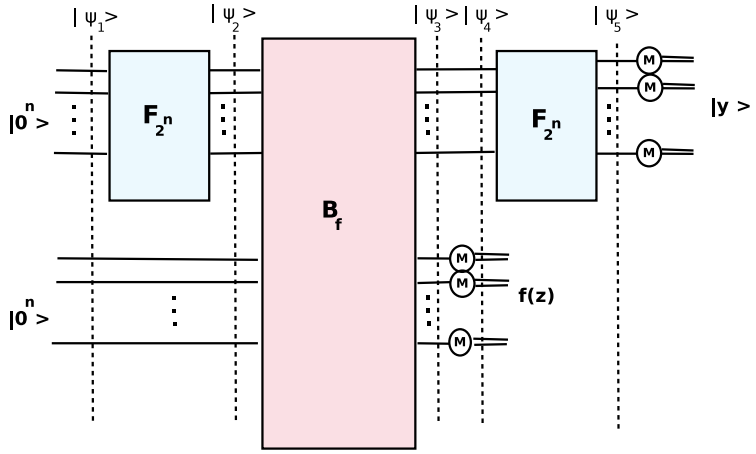


Figure 13.1: The circuit for the Period finding algorithm

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

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 13.2). 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.

13.5 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 13.1, 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 13.1: 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 $f(x) = 1$.

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

We ignore the second register now.

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

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.

$$|\psi_5\rangle = F_8 \frac{|1\rangle + |3\rangle + |5\rangle + |7\rangle}{\sqrt{4}}$$

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

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

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 12.6.

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

13.6 Longer example

You are given a black-box of function $f : \{0,1\}^4 \rightarrow \{0,1\}^4, f(x) = 2x \mod 16$. You have to find its period r. Below, in Table 13.2, 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 13.2: 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 13.2 shows the F_{16} butterfly diagram made using blocks of F_8 butterfly diagram.

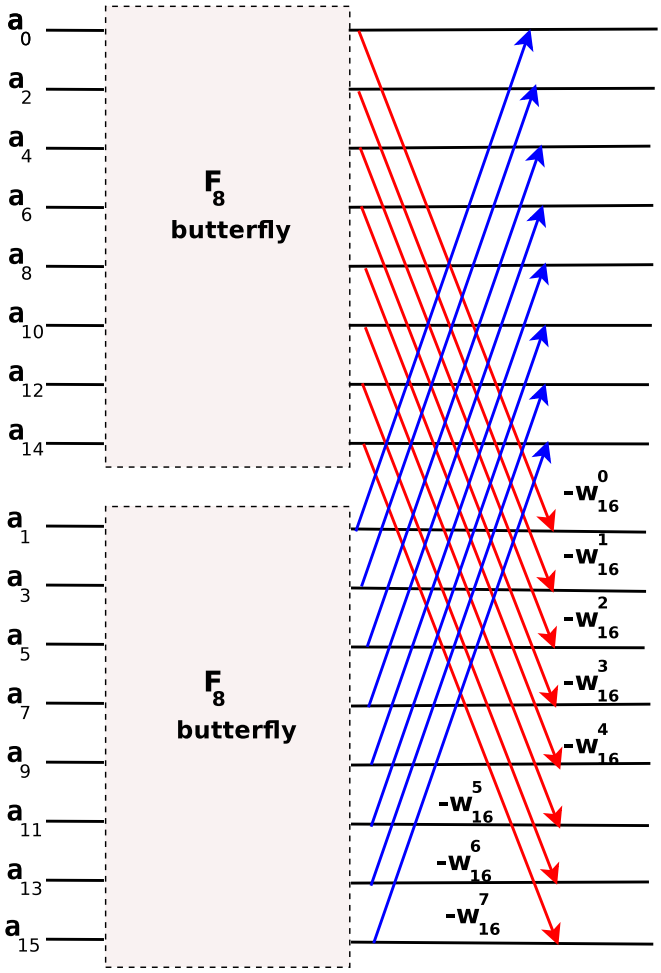


Figure 13.2: F_{16} Butterfly diagram using F_8 butterfly blocks

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.

13.7 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:

13.8 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.

14 Phase Estimation Algorithm

14.1 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, $(A - \lambda I)\vec{x} = \vec{0}$.

14.1.1 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 :).

14.2 Eigenvalues of unitary matrices

As depicted in Figure 14.1, 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.

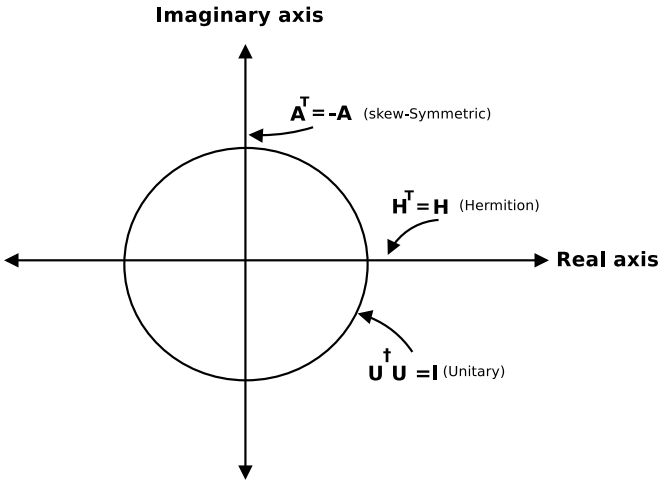


Figure 14.1: Unit complex circle: Eigenvalues of skew-symmetric, U, and H matrices.

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

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

14.3 Problem definition

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

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

14.4 Description

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

The quantum circuit of phase estimation is given in Figure 14.2. We now describe it step-by-step.

$$|\psi_1\rangle = |0^m\rangle\,|v\rangle$$

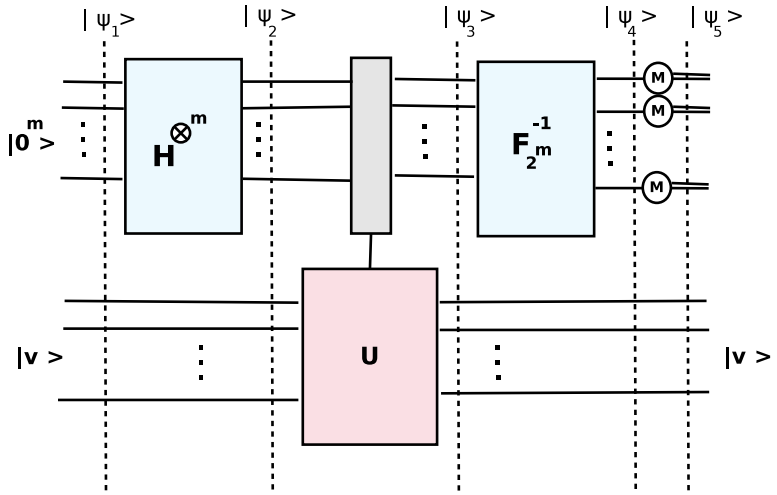


Figure 14.2: Quantum circuit for phase estimation

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:

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

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

$$p_j = \frac{1}{M}\frac{a^2}{b^2} \tag{14.1}$$

where

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

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!

14.5 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.

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

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

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

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.

15 Order Finding Algorithm

15.1 Background Abstract Algebra

15.1.1 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 $a, b \in G$, $aob = boa$

15.1.2 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:

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) \tag{15.1}$$

Example

What is Euler's Totient of 20.

Solution
I use the formula given in Equation 15.1. 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 15.1. Prime factors of 100 are $2^2 \times 5^5$.

Thus,

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

15.1.3 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 $\times$ 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 $\times$. The number of elements in $|\mathbb{Z}_{10}^*| = \varphi(10) = 4$. That is, $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$.

15.1.4 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.

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

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

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

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

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

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

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

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

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

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.

15.2 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

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

15.2.1 Classical computer

First note that order finding problem always has a solution as we know from Euler's theorem (Section 15.1.3) 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.

15.2.2 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 $x \in \mathbb{Z}_n^*$

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

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

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

It is because

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

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

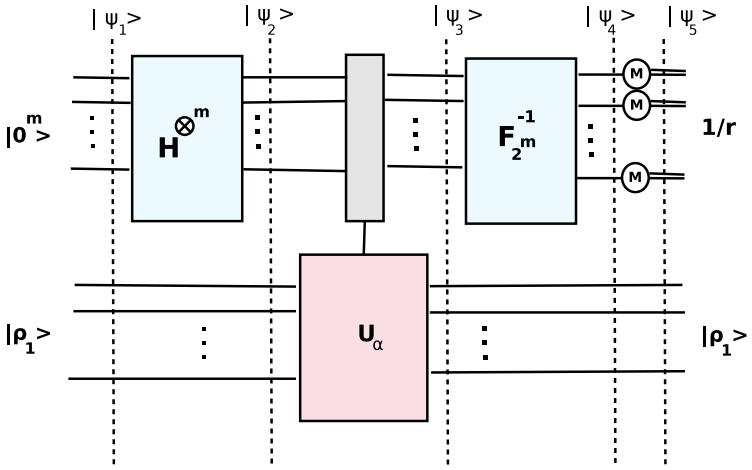


Figure 15.1: Phase estimation circuit with unitary operator U_α and eigenvector $|\rho_1\rangle$. Output will be $\frac{1}{r}$ as that is the θ of the eigenvalue

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 15.1 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 15.1.4.

15.2.3 Summary

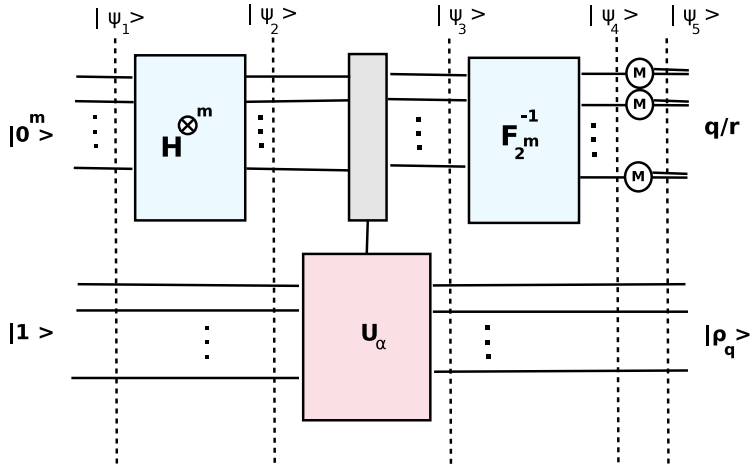


Figure 15.2: Phase estimation circuit but with unitary operator U_α and superposition of all eigenvectors $|1\rangle$. Output will be $\frac{q}{r}$, where q is uniformly distributed in the set $\{0, 1, 2, \cdots, r-1\}$

Summary of the steps carried out to compute order is illustrated by Figure 15.2 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.