Introduction to Quantum Computation and Quantum Algorithms

January 8, 2024

Part I : Foundations, Protocols and Algorithms

1. Axioms of Quantum Mechanics
2. Quantum Gates
3. Quantum Protocols
4. Quantum Algorithms

Focus on Ideas. Contrast with Conventional (Classical) bits

1. Simplicity and Ideas at the cost of Generality
   - Ex. $\mathbb{R}^2, \mathbb{R}^3$ or Finite Dim. Inner product spaces instead of Hilbert spaces.
2. Comparison with classical bits, notions - A Running Thread.
3. Pictorial. Dont get bogged down by the math.
   - Fine to not grasp text on a slide.

The Power of Quantum Algorithms, Quantum Cryptography

crucially relies on

Unique Behaviour of Quantum Systems - Superposition, Entanglement, etc.

To understand, design, leverage this power,

An Understanding of the Behaviour of Quantum Systems is Necessary.

Behaviour of Quantum Systems described through

Axioms of Quantum Mechanics $\longleftarrow$ Our First Topic

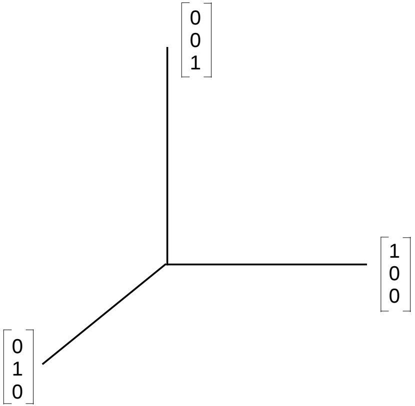
Axioms of Quantum Mechanics

A bit lives in $\{0, 1\}$ (it's state space). It is 0 or 1.

Where does a Qubit live?

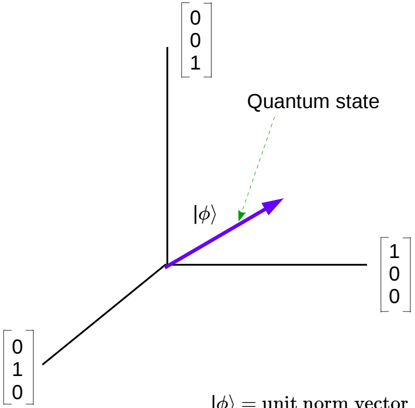
Axiom 1

Axiom 1 : How is a Quantum system described?



State Space of a quantum system is an Inner Product Space (IPS).

Axiom 1 : How is a Quantum system described?



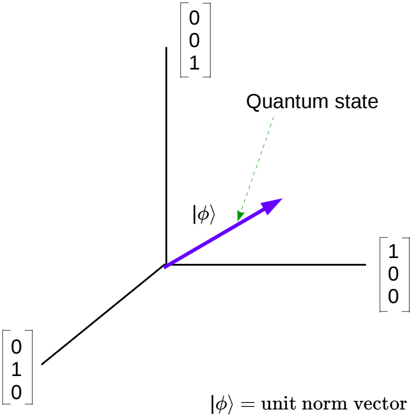
$|\phi\rangle = \text{unit norm vector}$

$|\phi\rangle$: unit vector in $\mathcal{H}$.

State Space of a quantum system is an Inner Product Space (IPS).

The state of a quantum system is described through a Unit vector in an IPS $\mathcal{H}$.

Axiom 1 : How is a Quantum system described?



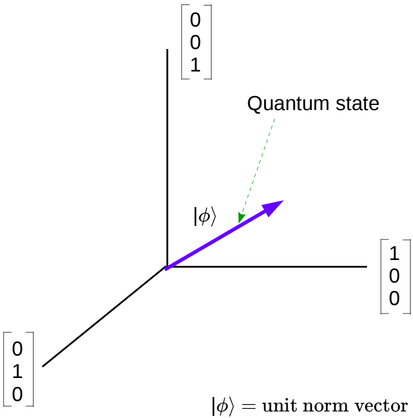
$|\phi\rangle$: unit vector in $\mathcal{H}$.

Ex. : $|\phi\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \in \mathcal{H} = \mathbb{R}^2$.

State Space of a quantum system is an Inner Product Space (IPS).

The state of a quantum system is described through a Unit vector in an IPS $\mathcal{H}$.

Axiom 1 : How is a Quantum system described?



$|\phi\rangle$: unit vector in $\mathcal{H}$.

Ex. : $|\phi\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \in \mathcal{H} = \mathbb{R}^2$.

Polarization of photon, spin of electron.

State Space of a quantum system is an Inner Product Space (IPS).

The state of a quantum system is described through a Unit vector in an IPS $\mathcal{H}$.

Why $\mathcal{H}$? What is the General Theory?

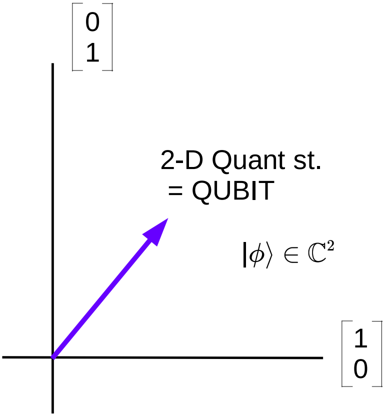
General Quantum Theory is based on a Hilbert space. Hence $\mathcal{H}$.

Mathematician : Hilbert space is a complete $\infty-$dimensional inner product space.

This tutorial : Euclidean space with std. inner product suffices $\leftarrow$ our Hilbert space.

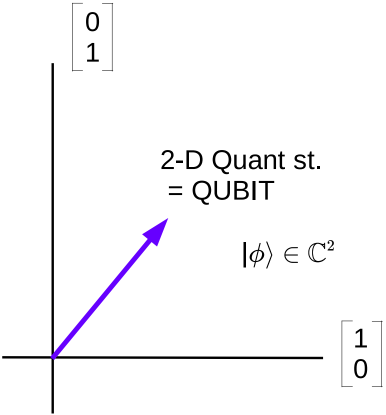
$\mathbb{R}^d$ suffices. But we denote it as $\mathbb{C}^d$. Pretend $\mathbb{C} = \mathbb{R}$.

Axiom 1 : How is a Quantum system described?



A $2-$ dimensional quantum state is a QUBIT.

Axiom 1 : How is a Quantum system described?

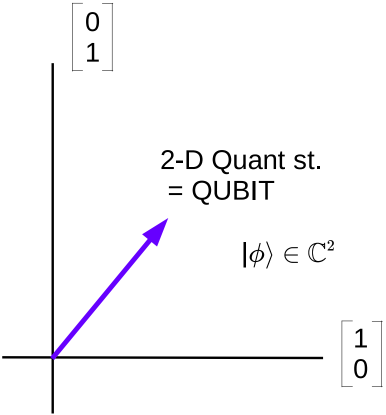


A $2-$ dimensional quantum state is a QUBIT.

Two Special Qubits

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{and} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Axiom 1 : How is a Quantum system described?



A $2-$ dimensional quantum state is a QUBIT.

Two Special Qubits

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{and} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

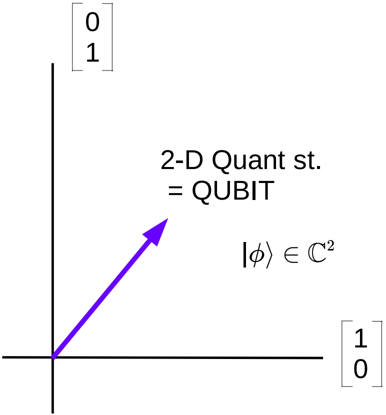
CAUTION

For any $\alpha, \beta \in \mathbb{C}$ s.t $|\alpha|^2 + |\beta|^2 = 1$

$\alpha|0\rangle + \beta|1\rangle$ is valid qubit

Valid state of a quantum system.

Axiom 1 : How is a Quantum system described?



Two Special Qubits

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{and} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

CAUTION

For any $\alpha, \beta \in \mathbb{C}$ s.t $|\alpha|^2 + |\beta|^2 = 1$

$\alpha|0\rangle + \beta|1\rangle$ is valid qubit

Valid state of a quantum system.

A $2-$ dimensional quantum state is a QUBIT.

Incorrect ilustration : Scalars are Complex numbers.

Correct illustration via 3-dimensional Bloch sphere.

Axiom 1 : Superposition and Inner Products.

Suppose System is in state $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$. $|\phi\rangle$ is a Superposition state.

INCORRECT: System is in state $|0\rangle$ with prob. $|\alpha|^2$ and in state $|1\rangle$ with prob. $|\beta|^2$.

Axiom 1 : Superposition and Inner Products.

Suppose System is in state $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$. $|\phi\rangle$ is a Superposition state.

INCORRECT: System is in state $|0\rangle$ with prob. $|\alpha|^2$ and in state $|1\rangle$ with prob. $|\beta|^2$.

The inner product (IP) between $|x\rangle \in \mathcal{H}$ and $|y\rangle \in \mathcal{H}$ is denoted $\langle y|x\rangle$.

Example : $|x\rangle = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \in \mathbb{C}^2$, $\qquad |y\rangle = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \in \mathbb{C}^2$,

$\langle y|x\rangle = y_1^* x_1 + y_2^* x_2$. Note : First argument is $\mathbb{C}$–conjugated. Physics Notation.

Axiom 1 : Superposition and Inner Products.

Suppose System is in state $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$. $|\phi\rangle$ is a Superposition state.

INCORRECT: System is in state $|0\rangle$ with prob. $|\alpha|^2$ and in state $|1\rangle$ with prob. $|\beta|^2$.

The inner product (IP) between $|x\rangle \in \mathcal{H}$ and $|y\rangle \in \mathcal{H}$ is denoted $\langle y|x\rangle$.

Example : $|x\rangle = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \in \mathbb{R}^2$, $\qquad |y\rangle = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} \in \mathbb{R}^2$,

$$\langle y|x\rangle = y_1 x_1 + y_2 x_2.$$

Qubits are our Information Carriers. Analogous to Bits.

Axiom 1 : Contrasting Quantum and Classical Worlds

Quantum World

Qubit : Unit vector in a Inner product space.

$\mathcal{H} \equiv$ Inner product space.

$|\phi\rangle$: where we encode our information.

$|\phi\rangle \in \mathbb{R}^2$ is a qubit.

Classical World

Bit : Element in a Finite Set

$\mathcal{X}$ - Our Finite set

$x \equiv$ the information we wish to encode.

x in $\mathcal{X} = \{0, 1\}$ is a bit.

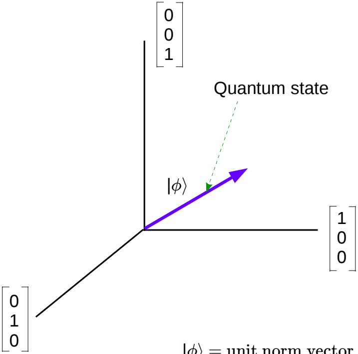
Points to Keep in Mind

Unit norm.

Acronyms, Abbreviations and Short Forms

IP FDIPS dim.

Our Universe and Its Contents

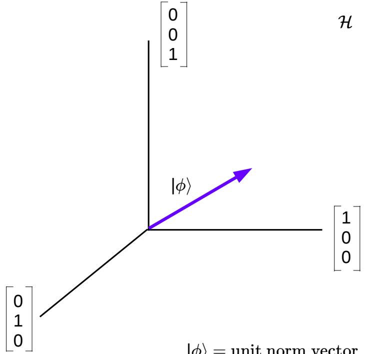


$|\phi\rangle = \text{unit norm vector}$

Our Universe and Its Contents

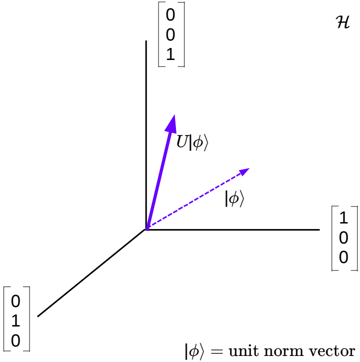
Linear Transformation (LT) : $T : \mathcal{H} \to \mathcal{H}$

$$T\,|\phi\rangle$$



$|\phi\rangle$ = unit norm vector

Our Universe and Its Contents



$|\phi\rangle$ = unit norm vector

Linear Transformation (LT) : $T : \mathcal{H} \to \mathcal{H}$

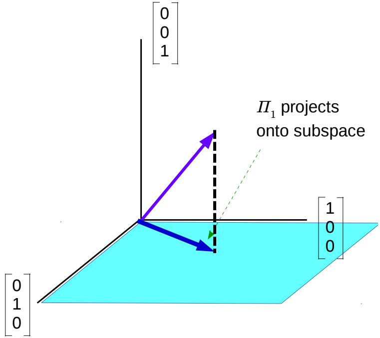
$$T\,|\phi\rangle$$

Unitary Transf. : LT that preserves length.

Just a rotation

$$U : \mathcal{H} \to \mathcal{H}$$

Our Universe and Its Contents



Linear Transformation (LT) : $T : \mathcal{H} \to \mathcal{H}$

$$T\,|\phi\rangle$$

Unitary Transf. : LT that preserves length.

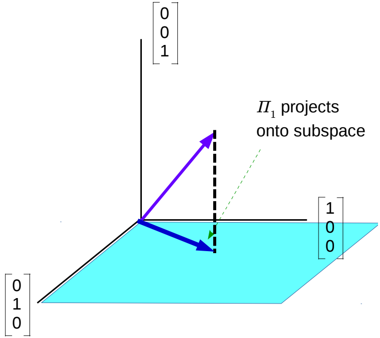
Just a rotation

$$U : \mathcal{H} \to \mathcal{H}$$

Projection : LT that projects.

Just a projection $\Pi_1 : \mathcal{H} \to \mathcal{H}$

Our Universe and Its Contents



Linear Transformation (LT) : $T : \mathcal{H} \to \mathcal{H}$

$$T\,|\phi\rangle$$

Unitary Transf. : LT that preserves length.

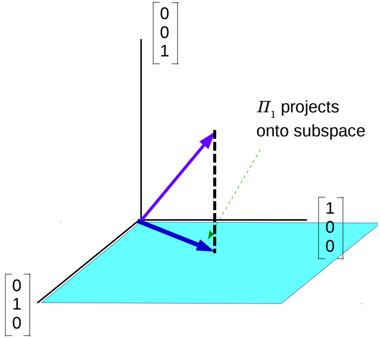
Just a rotation

$$U : \mathcal{H} \to \mathcal{H}$$

Projection : LT that projects.

Just a projection $\Pi_1 : \mathcal{H} \to \mathcal{H}$

$$\Pi_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$



Linear Transformation (LT) : $T : \mathcal{H} \to \mathcal{H}$

$$T\,|\phi\rangle$$

Unitary Transf. : LT that preserves length.

Just a rotation

$$U : \mathcal{H} \to \mathcal{H}$$

Projection : LT that projects.

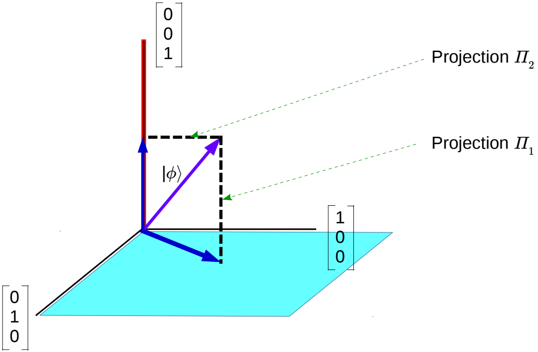
Just a projection $\Pi_1 : \mathcal{H} \to \mathcal{H}$

$$\Pi_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

Important

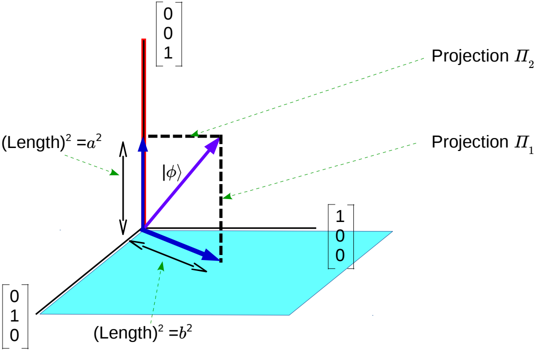
Any projector Π satisfies $\Pi^2 = \Pi^\dagger = \Pi$.

More on Projections



Projections $\Pi_1, \ \Pi_2 : \mathcal{H} \to \mathcal{H}$.

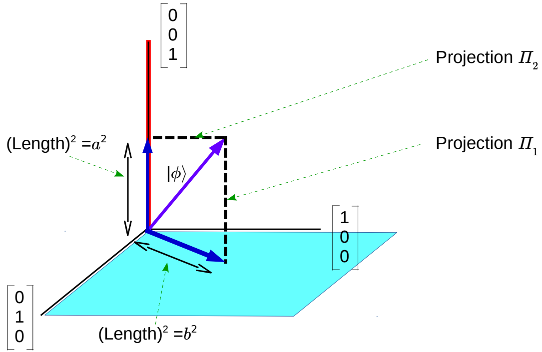
More on Projections



Projections $\Pi_1,\ \Pi_2 : \mathcal{H} \to \mathcal{H}$.

$$\Pi_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \quad \Pi_2 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

More on Projections

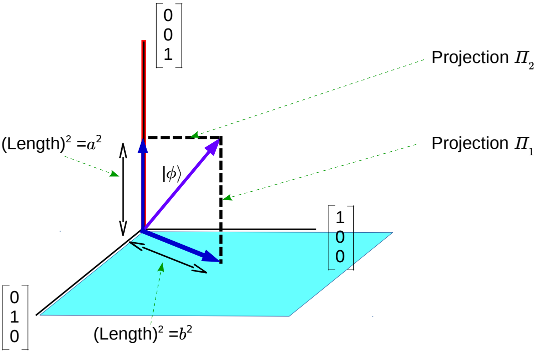


Projections $\Pi_1,\ \Pi_2 : \mathcal{H} \to \mathcal{H}$.

$$\Pi_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \quad \Pi_2 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\Pi_1 + \Pi_2 = I \Rightarrow a^2 + b^2 = 1$$

More on Projections



Projections $\Pi_1, \ \Pi_2 : \mathcal{H} \to \mathcal{H}$.

$$\Pi_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \quad \Pi_2 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\Pi_1 + \Pi_2 = I \Rightarrow a^2 + b^2 = 1$$

$$\begin{aligned} a^2 + b^2 &= (\text{length of } |\phi\rangle)^2 \\ &= |\langle\phi|\phi\rangle|^2 = 1 \end{aligned}$$

Axiom 2 : How does a Closed system evolve?

The evolution of a closed (isolated) quantum system evolves through a Unitary Transformation.

$|x\rangle_{t_1} \equiv$ State of System at time t_1, $|x\rangle_{t_2} \equiv$ State of System at time t_2

$|x\rangle_{t_2}$ is related to $|x\rangle_{t_1}$ through a Unitary transformation U.

$$|x\rangle_{t_2} = U|x\rangle_{t_1}$$

Axiom 3 :

Our Interaction with a Quantum System and the Rules that Govern this Interaction

Axiom 3 is the Measurement Axiom

Axiom 3 - The Measurement Axiom - A Very Important Axiom

Can eye-ball/read-out a bit. Cannot eye-ball/stare at qubit.

Your interaction is via a Measurement.

Axiom 3 describes this interaction and the rules governing this interaction.

Axiom 3 : The Measurement Axiom

A measurement is described through

a collection $\{\Pi_{\alpha_1}, \Pi_{\alpha_2}, \cdots, \Pi_{\alpha_K}\}$ of projectors acting on inner product Space $\mathcal{H}$

that satify the Completeness Relation

$$\sum_{k=1}^{K} \Pi_{\alpha_k} = \Pi_{\alpha_1} + \cdots + \Pi_{\alpha_K} = I \quad (I \equiv \text{ the Identity on } \mathcal{H}).$$

Axiom 3 : The Measurement Axiom

A measurement is described through

a collection $\{\Pi_{\alpha_1}, \Pi_{\alpha_2}, \cdots, \Pi_{\alpha_K}\}$ of projectors acting on inner product Space $\mathcal{H}$

that satify the Completeness Relation

$$\sum_{k=1}^{K} \Pi_{\alpha_k} = \Pi_{\alpha_1} + \cdots + \Pi_{\alpha_K} = I \quad (I \equiv \text{ the Identity on } \mathcal{H}).$$

What are these operators and the indices $\alpha_1, \cdots, \alpha_K$?

Axiom 3 : The Measurement Axiom

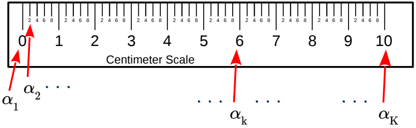
A measurement is described through

a collection $\{\Pi_{\alpha_1}, \Pi_{\alpha_2}, \cdots, \Pi_{\alpha_K}\}$ of projectors acting on inner product Space $\mathcal{H}$

that satify the Completeness Relation

$$\sum_{k=1}^{K} \Pi_{\alpha_k} = \Pi_{\alpha_1} + \cdots + \Pi_{\alpha_K} = I \quad (I \equiv \text{ the Identity on } \mathcal{H}).$$

What are these operators and the indices $\alpha_1, \cdots, \alpha_K$?



Indices $\alpha_1, \cdots, \alpha_K$: possible outcomes.

Each Projector Π_{α_k} corresponds to its outcome α_k.

Completeness Relation "You must get atleast one of the possible outcomes."

Simplify, Simplify, Simplify, $\cdots$

Just call $\alpha_1, \alpha_2, \alpha_K$ as $1, 2, \cdots, K$

Outcomes are $1, 2, \cdots, K$.

Reduce notation.

Axiom 3 : The Measurement Axiom

When a measurement $\{\Pi_1, \Pi_2, \cdots, \Pi_K\}$ is performed on a state $|\phi\rangle \in \mathcal{H}$

Axiom 3 : The Measurement Axiom

When a measurement $\{\Pi_1, \Pi_2, \cdots, \Pi_K\}$ is performed on a state $|\phi\rangle \in \mathcal{H}$

1. You get outcome k with probability

$$P(\text{Outcome } = k) = (\text{Length of proj. } \Pi_k|\phi\rangle)^2 = \text{Inn. prod. between } \Pi_k|\phi\rangle \text{ and } \Pi_k|\phi\rangle$$

Axiom 3 : The Measurement Axiom

When a measurement $\{\Pi_1, \Pi_2, \cdots, \Pi_K\}$ is performed on a state $|\phi\rangle \in \mathcal{H}$

1. You get outcome k with probability

$$\begin{aligned} P(\text{Outcome } = k) &= (\text{Length of proj. } \Pi_k|\phi\rangle)^2 = \text{Inn. prod. between } \Pi_k|\phi\rangle \text{ and } \Pi_k|\phi\rangle \\ &= \langle\phi|\Pi_k^\dagger \mid \Pi_k\phi\rangle = \langle\phi|\Pi_k \mid \Pi_k\phi\rangle = \langle\phi|\ \Pi_k\phi\rangle \end{aligned}$$

Axiom 3 : The Measurement Axiom

When a measurement $\{\Pi_1, \Pi_2, \cdots, \Pi_K\}$ is performed on a state $|\phi\rangle \in \mathcal{H}$

1. You get outcome k with probability

$$\begin{aligned}
P(\text{Outcome } = k) &= (\text{Length of proj. } \Pi_k|\phi\rangle)^2 = \text{Inn. prod. between } \Pi_k|\phi\rangle \text{ and } \Pi_k|\phi\rangle \\
&= \langle\phi|\Pi_k^\dagger \mid \Pi_k\phi\rangle = \langle\phi|\Pi_k \mid \Pi_k\phi\rangle = \langle\phi| \ \Pi_k\phi\rangle \\
&= (\text{Length of projection } \Pi_k|\phi\rangle)^2
\end{aligned}$$

Note :

$$\sum_{k=1}^{K} P(\text{Outcome } = k) \quad = \quad \sum_{k=1}^{K}\langle\phi|\Pi_k|\phi\rangle = \langle\phi|\sum_{k=1}^{K}\Pi_k|\phi\rangle = \langle\phi|I|\phi\rangle = 1$$

Completeness
+ unit-norm

Axiom 3 : The Measurement Axiom

When a measurement $\{\Pi_1, \Pi_2, \cdots, \Pi_K\}$ is performed on a state $|\phi\rangle \in \mathcal{H}$

1. You get outcome k with probability

$$\begin{aligned} P(\text{Outcome } = k) &= (\text{Length of proj. } \Pi_k|\phi\rangle)^2 = \text{Inn. prod. between } \Pi_k|\phi\rangle \text{ and } \Pi_k|\phi\rangle \\ &= \langle\phi|\Pi_k^{\dagger} \mid \Pi_k\phi\rangle = \langle\phi|\Pi_k \mid \Pi_k\phi\rangle = \langle\phi|\ \Pi_k\phi\rangle \\ &= (\text{Length of projection } \Pi_k|\phi\rangle)^2 \end{aligned}$$

2. The quantum system collapses to one of the following states

$$\frac{\Pi_k|\phi\rangle}{\sqrt{\langle\phi|\Pi_k|\phi\rangle}} \qquad : k = 1, 2 \cdots, K$$

Axiom 3 : The Measurement Axiom

When a measurement $\{\Pi_1, \Pi_2, \cdots, \Pi_K\}$ is performed on a state $|\phi\rangle \in \mathcal{H}$

1. You get outcome k with probability

$$\begin{aligned} P(\text{Outcome } = k) &= (\text{Length of proj. } \Pi_k|\phi\rangle)^2 = \text{Inn. prod. between } \Pi_k|\phi\rangle \text{ and } \Pi_k|\phi\rangle \\ &= \langle\phi|\Pi_k^\dagger \mid \Pi_k\phi\rangle = \langle\phi|\Pi_k \mid \Pi_k\phi\rangle = \langle\phi| \Pi_k\phi\rangle \\ &= (\text{Length of projection } \Pi_k|\phi\rangle)^2 \end{aligned}$$

2. The quantum system collapses to one of the following states

$$\frac{\Pi_k|\phi\rangle}{\sqrt{\langle\phi|\Pi_k|\phi\rangle}} = \frac{\Pi_k|\phi\rangle}{\sqrt{\text{Length of } \Pi_k|\phi\rangle}} : k = 1, 2 \cdots, K$$

Axiom 3 : The Measurement Axiom

When a measurement $\{\Pi_1, \Pi_2, \cdots, \Pi_K\}$ is performed on a state $|\phi\rangle \in \mathcal{H}$

1. You get outcome k with probability

$$
\begin{aligned}
P(\text{Outcome } = k) &= (\text{Length of proj. } \Pi_k|\phi\rangle)^2 = \text{Inn. prod. between } \Pi_k|\phi\rangle \text{ and } \Pi_k|\phi\rangle \\
&= \langle\phi|\Pi_k^\dagger \mid \Pi_k\phi\rangle = \langle\phi|\Pi_k \mid \Pi_k\phi\rangle = \langle\phi|\ \Pi_k\phi\rangle \\
&= (\text{Length of projection } \Pi_k|\phi\rangle)^2
\end{aligned}
$$

2. The quantum system collapses to one of the following states

$$
\frac{\Pi_k|\phi\rangle}{\sqrt{\langle\phi|\Pi_k|\phi\rangle}} = \frac{\Pi_k|\phi\rangle}{\sqrt{\text{Length of } \Pi_k|\phi\rangle}} : k = 1, 2 \cdots, K
$$

3. Moreover, if you observe outcome j, then the state collapses to

$$
\frac{\Pi_j|\phi\rangle}{\sqrt{\langle\phi|\Pi_j|\phi\rangle}}
$$

Understanding the Measurement Axiom : Classical World

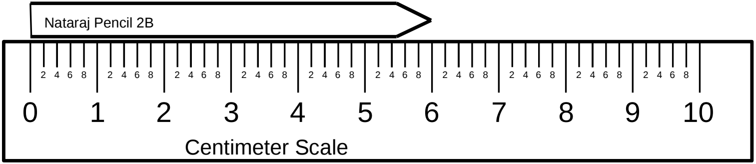
Classical world

Wish to measure pencil's length

Understanding the Measurement Axiom : Classical World

Classical world

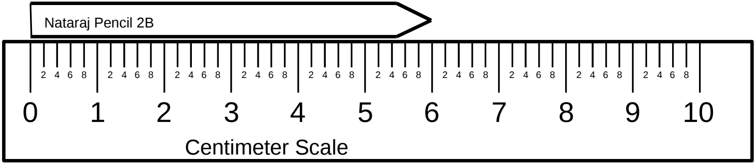
Wish to measure pencil's length



Understanding the Measurement Axiom : Classical World

Classical world

1. Length is accurately read- 6cm.
No uncertainty.



Understanding the Measurement Axiom : Classical World

Classical world

1. Length is accurately read- 6cm. No uncertainty.

2. Pencil's length does NOT change post-measurement

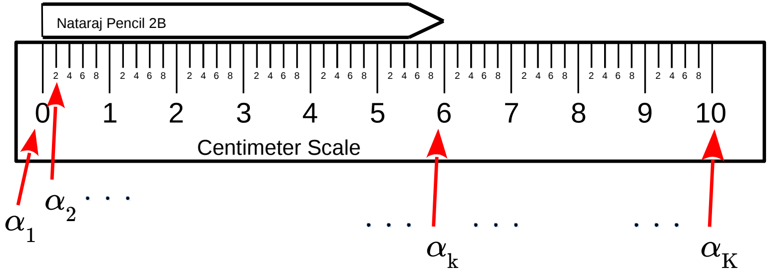
Understanding the Measurement Axiom : Quantum World

Quantum World

Wish to measure pencil's (quantum state) length

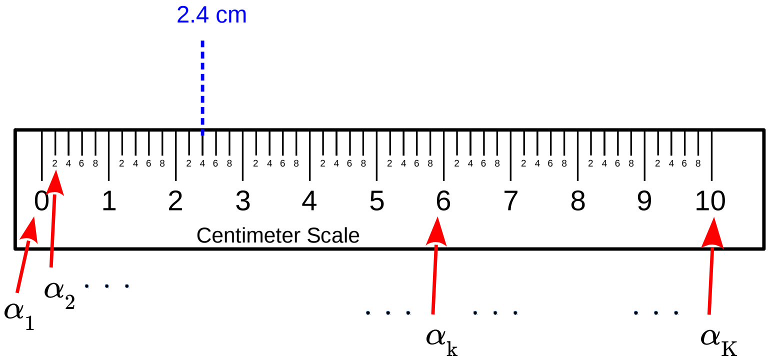
Quantum World

Wish to measure pencil's (quantum state) length



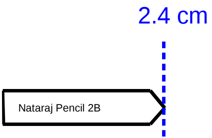
Quantum World

1. Outcome is RANDOM.



Understanding the Measurement Axiom : Quantum World

Quantum World

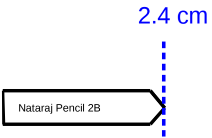


1. Outcome is RANDOM.

2. Pencil's length CHANGES post-measurement

Understanding the Measurement Axiom : Quantum World

Quantum World



1. Outcome is RANDOM.

2. Pencil's length CHANGES post-measurement

Welcome to the QUANTUM WORLD.

Measurement Axiom : An Example

Example

Quantum system in state $|\phi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \in \mathcal{H} = \mathbb{C}^2$.

Perform measurement with two outcome $\{-0.5, +0.5\}$.

Two meas. operators $\Pi_{-0.5} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$, $\Pi_{+0.5} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$.

$\Pi_{-0.5} + \Pi_{+0.5} = I$. Completeness Relation satisfied.

$$\begin{aligned} P(\text{Outcome } = -0.5) &= (\text{Length of } \Pi_{-0.5}|\phi\rangle)^2 = \left\| \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \right\|^2 \\ &= \left\| \begin{bmatrix} 0 \\ \frac{1}{\sqrt{2}} \end{bmatrix} \right\|^2 = \frac{1}{2} \\ P(\text{Outcome } = +0.5) &= \left\| \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \end{bmatrix} \right\|^2 = \frac{1}{2} \end{aligned}$$

If Outcome $= -0.5$, state collapses to $|1\rangle$. If Outcome $= +0.5$, state collapses to $|0\rangle$.

Points to Keep in Mind

- Non-orthogonal states cannot be distinguished with certainty.
- Computation/Communication results need to be projected to orthogonal states.

Axiom 4 : Description of a Joint/Composite Quantum System

Quantum World

Suppose Quantum System 1 is in state $|\phi_1\rangle \in \mathcal{H}_1$

Quantum System 2 is in state $|\phi_2\rangle \in \mathcal{H}_2$

$$\vdots$$

Quantum System n is in state $|\phi_n\rangle \in \mathcal{H}_n$

State space of composite Quant Sys. is the tensor product

$\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n$ of constituent state spaces.

Composite System is described by State

$$|\phi_1\rangle \otimes |\phi_2\rangle \otimes \cdots \otimes |\phi_n\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n.$$

Axiom 4 : Description of a Joint/Composite Quantum System

Quantum World	Classical World
Suppose Quantum System 1 is in state $\|\phi_1\rangle \in \mathcal{H}_1$	System 1 in state $x_1 \in \mathcal{X}_1$
Quantum System 2 is in state $\|\phi_2\rangle \in \mathcal{H}_2$	System 2 in state $x_2 \in \mathcal{X}_2$
$\vdots$	$\vdots$
Quantum System n is in state $\|\phi_n\rangle \in \mathcal{H}_n$	System n in state $x_n \in \mathcal{X}_n$
State space of composite Quant Sys. is the tensor product	Cartesian product
$\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n$ of constituent state spaces.	$\mathcal{X}_1 \times \mathcal{X}_2 \times \cdots \times \mathcal{X}_n$.
Composite System is described by State	n−tuple
$\|\phi_1\rangle \otimes \|\phi_2\rangle \otimes \cdots \otimes \|\phi_n\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n$.	$(x_1, \cdots, x_n) \in \mathcal{X}_1 \times \cdots \times \mathcal{X}_n$.

What is a Tensor Product and what are the rules governing it?

Quantum World

Suppose V is a $m-$dimensional IPS,

W is a $n-$dimensional IPS.

$V \otimes W$ is $mn-$dimensional IPS.

What is a Tensor Product and what are the rules governing it?

Quantum World	Classical World
Suppose V is a $m-$dimensional IPS,	$x \in \mathcal{X}$, $\lvert\mathcal{X}\rvert = m$
W is a $n-$dimensional IPS.	$y \in \mathcal{Y}$, $\lvert\mathcal{Y}\rvert = n$
$V \otimes W$ is $mn-$dimensional IPS.	$(x, y) \in \mathcal{X} \times \mathcal{Y}$, $\lvert\mathcal{X} \times \mathcal{Y}\rvert = mn$

What is a Tensor Product and what are the rules governing it?

Quantum World	Classical World
Suppose V is a $m-$dimensional IPS,	$x \in \mathcal{X}$, $\lvert\mathcal{X}\rvert = m$
W is a $n-$dimensional IPS.	$y \in \mathcal{Y}$, $\lvert\mathcal{Y}\rvert = n$
$V \otimes W$ is $mn-$dimensional IPS.	$(x, y) \in \mathcal{X} \times \mathcal{Y}$, $\lvert\mathcal{X} \times \mathcal{Y}\rvert = mn$

Alert : NOT a direct sum. direct sum if $m + n$-dim.

What is a Tensor Product and what are the rules governing it?

Quantum World	Classical World
Suppose V is a $m-$dimensional IPS,	$x \in \mathcal{X}$, $\lvert\mathcal{X}\rvert = m$
W is a $n-$dimensional IPS.	$y \in \mathcal{Y}$, $\lvert\mathcal{Y}\rvert = n$
$V \otimes W$ is $mn-$dimensional IPS.	$(x, y) \in \mathcal{X} \times \mathcal{Y}$, $\lvert\mathcal{X} \times \mathcal{Y}\rvert = mn$

Alert : NOT a direct sum. direct sum if $m + n$-dim.

Elements of $V \otimes W$ — All possible linear combinations of tensor product $|v\rangle \otimes |w\rangle$ of elements $|v\rangle \in V$ and $|w\rangle \in W$.

$|v\rangle \otimes |w\rangle$ — Just an (ordered) pair of vectors from respective spaces

What is a Tensor Product and what are the rules governing it?

Quantum World	Classical World
Suppose V is a $m-$dimensional IPS,	$x \in \mathcal{X}$, $\lvert\mathcal{X}\rvert = m$
W is a $n-$dimensional IPS.	$y \in \mathcal{Y}$, $\lvert\mathcal{Y}\rvert = n$
$V \otimes W$ is $mn-$dimensional IPS.	$(x, y) \in \mathcal{X} \times \mathcal{Y}$, $\lvert\mathcal{X} \times \mathcal{Y}\rvert = mn$

Alert : NOT a direct sum. direct sum if $m + n$-dim.

Elements of $V \otimes W$ — All possible ?linear combinations? of ?tensor product? $|v\rangle \otimes |w\rangle$ of elements $|v\rangle \in V$ and $|w\rangle \in W$.

$|v\rangle \otimes |w\rangle$ — Just an (ordered) pair of vectors from respective spaces

Rules Governing Linear Combinations in Tensor Product Spaces

Rules governing Linear combination

$$|v_1\rangle \otimes \underbrace{|w\rangle}_{\uparrow} + |v_2\rangle \otimes \underbrace{|w\rangle} = (|v_1\rangle + |v_2\rangle) \otimes \underbrace{|w\rangle} \qquad \text{State Distrbtv Law (SDL) 1}$$

$$\underbrace{|v\rangle} \otimes |w_1\rangle + \underbrace{|v\rangle} \otimes |w_2\rangle = \underbrace{|v\rangle} \otimes (|w_1\rangle + |w_2\rangle) \qquad \text{State Distrbtv Law (SDL) 2}$$

$$\alpha \cdot (|v\rangle \otimes |w\rangle) = (\alpha \cdot |u\rangle) \otimes |w\rangle = |v\rangle \otimes (\alpha \cdot |w\rangle) \qquad \text{State Distrbtv Law (SDL) 3}$$

The above rules tell you how and when to combine terms.

In general, if the above rules do not apply, the sum

$$|v_1\rangle \otimes |w_1\rangle + |v_2\rangle \otimes |w_2\rangle = |v_1\rangle \otimes |w_1\rangle + |v_2\rangle \otimes |w_2\rangle$$

is a distinct element of $V \otimes W$.

Rules Governing Operations on Tensor Products and Inner Products

What are the linear transformations/operators acting on $V \otimes W$?

Rules Governing Operations on Tensor Products and Inner Products

What are the linear transformations/operators acting on $V \otimes W$?

Suppose $A : V \to V$ and $B : W \to W$ are LTs.

$$(A \otimes B)(|v\rangle \otimes |w\rangle) = A\,|v\rangle \otimes B\,|w\rangle \qquad \text{Operator Dist. Law (ODL) 1}$$

$$(A \otimes B)(\sum_i |v_i\rangle \otimes |w_i\rangle) = \sum_i A\,|v_i\rangle \otimes B\,|w_i\rangle \qquad \text{Operator Dist. Law (ODL) 2}$$

$$A \otimes (B_1 + B_2) = A \otimes B_1 + A \otimes B_2 \qquad \text{Operator Dist. Law (ODL) 3}$$

Rules Governing Operations on Tensor Products and Inner Products

What are the linear transformations/operators acting on $V \otimes W$?

Suppose $A : V \to V$ and $B : W \to W$ are LTs.

$$(A \otimes B)(|v\rangle \otimes |w\rangle) = A|v\rangle \otimes B|w\rangle \qquad \text{Operator Dist. Law (ODL) 1}$$

$$(A \otimes B)(\sum_i |v_i\rangle \otimes |w_i\rangle) = \sum_i A|v_i\rangle \otimes B|w_i\rangle \qquad \text{Operator Dist. Law (ODL) 2}$$

$$A \otimes (B_1 + B_2) = A \otimes B_1 + A \otimes B_2 \qquad \text{Operator Dist. Law (ODL) 3}$$

What about the inner product on $V \otimes W$

Ans : Product of inner products.

IP between $|v_1\rangle \otimes |w_1\rangle$ and $|v_2\rangle \otimes |w_2\rangle = \langle v_1|v_2\rangle \langle w_1|w_2\rangle$.

Tensor Product : A Concrete Example

$$V = \mathbb{C}^2, W = \mathbb{C}^2, \quad |v\rangle = \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \quad |w\rangle = \begin{bmatrix} 3 \\ 4 \end{bmatrix}, \quad |v\rangle \otimes |w\rangle = \begin{bmatrix} 1 \times 3 \\ 1 \times 4 \\ 2 \times 3 \\ 2 \times 4 \end{bmatrix}$$

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}, \quad B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \quad A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B \\ a_{21}B & a_{22}B \end{bmatrix}$$

Simple Consequences

1. $\dim(V \otimes W) = \dim(V) \times \dim(W)$.

Tensor Product : A Concrete Example

$$V = \mathbb{C}^2, W = \mathbb{C}^2, \quad |v\rangle = \begin{bmatrix} 1 \\ 2 \end{bmatrix}, \quad |w\rangle = \begin{bmatrix} 3 \\ 4 \end{bmatrix}, \quad |v\rangle \otimes |w\rangle = \begin{bmatrix} 1 \times 3 \\ 1 \times 4 \\ 2 \times 3 \\ 2 \times 4 \end{bmatrix}$$

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}, \quad B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \quad A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B \\ a_{21}B & a_{22}B \end{bmatrix}$$

Simple Consequences

1. $\dim(V \otimes W) = \dim(V) \times \dim(W)$.

2. If $\{|\alpha_1\rangle, \cdots, |\alpha_m\rangle\}$ is orthonormal basis for V,
   $\{|\beta_1\rangle, \cdots, |\beta_n\rangle\}$ is orthonormal basis for W,

   then $\{|\alpha_i\rangle \otimes |\beta_j\rangle : 1 \le i \le m, 1 \le j \le n\}$ is orthonormal basis for $V \otimes W$.

Our Basis in $\mathbb{C}^2 \otimes \mathbb{C}^2$

Example $\quad |0\rangle, |1\rangle$ forms an orthonormal basis for $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^2$

$|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle$ forms an orthonormal basis for $\mathcal{H}_A \otimes \mathcal{H}_B$

Notational Simplification : $|0\rangle \otimes |1\rangle = |0\rangle |1\rangle = |01\rangle$

$\{\ |00\rangle,\ |01\rangle, |10\rangle, |11\rangle\}$ orthonormal basis for $\mathcal{H}_A \otimes \mathcal{H}_B$

Our Basis in $\mathbb{C}^2 \otimes \mathbb{C}^2$

Example $\quad |0\rangle, |1\rangle$ forms an orthonormal basis for $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^2$

$|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle$ forms an orthonormal basis for $\mathcal{H}_A \otimes \mathcal{H}_B$

Notational Simplification : $|0\rangle \otimes |1\rangle = |0\rangle |1\rangle = |01\rangle$

$\{\, |00\rangle, \; |01\rangle, |10\rangle, |11\rangle\}$ orthonormal basis for $\mathcal{H}_A \otimes \mathcal{H}_B$

If $|v_1\rangle, |v_2\rangle, |v_3\rangle, |v_4\rangle$ are orthonormal $\Rightarrow \left\{ \begin{matrix} \frac{1}{\sqrt{2}}|v_1\rangle + \frac{1}{\sqrt{2}}|v_2\rangle, \frac{1}{\sqrt{2}}|v_1\rangle - \frac{1}{\sqrt{2}}|v_2\rangle \\ \frac{1}{\sqrt{2}}|v_3\rangle + \frac{1}{\sqrt{2}}|v_4\rangle, \frac{1}{\sqrt{2}}|v_3\rangle - \frac{1}{\sqrt{2}}|v_4\rangle \end{matrix} \right\}$

are orthonormal.

Our Basis in $\mathbb{C}^2 \otimes \mathbb{C}^2$

Example $\quad |0\rangle, |1\rangle$ forms an orthonormal basis for $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^2$

$|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle$ forms an orthonormal basis for $\mathcal{H}_A \otimes \mathcal{H}_B$

Notational Simplification : $|0\rangle \otimes |1\rangle = |0\rangle |1\rangle = |01\rangle$

$\{\ |00\rangle,\ |01\rangle, |10\rangle, |11\rangle\}$ orthonormal basis for $\mathcal{H}_A \otimes \mathcal{H}_B$

If $|v_1\rangle, |v_2\rangle, |v_3\rangle, |v_4\rangle$ are orthonormal $\Rightarrow \left\{ \begin{matrix} \frac{1}{\sqrt{2}}|v_1\rangle + \frac{1}{\sqrt{2}}|v_2\rangle, \frac{1}{\sqrt{2}}|v_1\rangle - \frac{1}{\sqrt{2}}|v_2\rangle \\ \frac{1}{\sqrt{2}}|v_3\rangle + \frac{1}{\sqrt{2}}|v_4\rangle, \frac{1}{\sqrt{2}}|v_3\rangle - \frac{1}{\sqrt{2}}|v_4\rangle \end{matrix} \right\}$

are orthonormal.

$\frac{1}{\sqrt{2}}|00\rangle \pm \frac{1}{\sqrt{2}}|11\rangle, \qquad \frac{1}{\sqrt{2}}|01\rangle \pm \frac{1}{\sqrt{2}}|10\rangle$, are orthonormal

Secrets of the Tensor Product

More Consequences

1. $$\{\ |v\rangle \otimes |w\rangle : |v\rangle \in V, |w\rangle \in W\ \}\ \text{does NOT exhaust}\ V \otimes W$$

More Consequences

1. $$\{\ |v\rangle \otimes |w\rangle : |v\rangle \in V, |w\rangle \in W\ \} \text{ does NOT exhaust } V \otimes W$$

   Not all vectors in $V \otimes W$ can be expressed as $|v\rangle \otimes |w\rangle$. However,

   $$V \otimes W = \text{span}\{\ |v\rangle \otimes |w\rangle : |v\rangle \in V, |w\rangle \in W\ \}$$

Secrets of the Tensor Product

More Consequences

1. $$\{\ |v\rangle \otimes |w\rangle : |v\rangle \in V, |w\rangle \in W\ \}\ \text{does NOT exhaust}\ V \otimes W$$

   Not all vectors in $V \otimes W$ can be expressed as $|v\rangle \otimes |w\rangle$. However,

   $$V \otimes W = \text{span}\{\ |v\rangle \otimes |w\rangle : |v\rangle \in V, |w\rangle \in W\ \}$$

   $$\left(\frac{\sqrt{3}}{2\sqrt{2}}|00\rangle + \frac{\sqrt{3}}{2\sqrt{2}}|01\rangle + \frac{1}{2\sqrt{2}}|10\rangle + \frac{1}{2\sqrt{2}}|11\rangle\right)$$

More Consequences

1.

$$\{\ |v\rangle \otimes |w\rangle : |v\rangle \in V, |w\rangle \in W\ \}\ \text{does NOT exhaust}\ V \otimes W$$

Not all vectors in $V \otimes W$ can be expressed as $|v\rangle \otimes |w\rangle$. However,

$$V \otimes W = \text{span}\{\ |v\rangle \otimes |w\rangle : |v\rangle \in V, |w\rangle \in W\ \}$$

$$\underbrace{\left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle\right)}_{|v\rangle} \otimes \underbrace{\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)}_{|w\rangle} = \left(\frac{\sqrt{3}}{2\sqrt{2}}|00\rangle + \frac{\sqrt{3}}{2\sqrt{2}}|01\rangle + \frac{1}{2\sqrt{2}}|10\rangle + \frac{1}{2\sqrt{2}}|11\rangle\right)$$

$$\left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right)$$

More Consequences

1.

$$\{ \ |v\rangle \otimes |w\rangle : |v\rangle \in V, |w\rangle \in W \ \} \text{ does NOT exhaust } V \otimes W$$

Not all vectors in $V \otimes W$ can be expressed as $|v\rangle \otimes |w\rangle$. However,

$$V \otimes W = \text{span} \{ \ |v\rangle \otimes |w\rangle : |v\rangle \in V, |w\rangle \in W \ \}$$

$$\underbrace{\left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle\right)}_{|v\rangle} \otimes \underbrace{\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)}_{|w\rangle} = \left(\frac{\sqrt{3}}{2\sqrt{2}}|00\rangle + \frac{\sqrt{3}}{2\sqrt{2}}|01\rangle + \frac{1}{2\sqrt{2}}|10\rangle + \frac{1}{2\sqrt{2}}|11\rangle\right)$$

$$(a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) \quad \overset{??}{=} \quad \left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right)$$

More Consequences

1.

$$\{\ |v\rangle \otimes |w\rangle : |v\rangle \in V, |w\rangle \in W\ \}\ \text{does NOT exhaust } V \otimes W$$

Not all vectors in $V \otimes W$ can be expressed as $|v\rangle \otimes |w\rangle$. However,

$$V \otimes W = \text{span}\{\ |v\rangle \otimes |w\rangle : |v\rangle \in V, |w\rangle \in W\ \}$$

$$\underbrace{\left(\tfrac{\sqrt{3}}{2}|0\rangle + \tfrac{1}{2}|1\rangle\right)}_{|v\rangle} \otimes \underbrace{\left(\tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle\right)}_{|w\rangle} = \left(\frac{\sqrt{3}}{2\sqrt{2}}|00\rangle + \frac{\sqrt{3}}{2\sqrt{2}}|01\rangle + \frac{1}{2\sqrt{2}}|10\rangle + \frac{1}{2\sqrt{2}}|11\rangle\right)$$

$$(a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) \quad \stackrel{??}{=} \quad \left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right)$$

$$ad = 0, \quad ac = \frac{1}{\sqrt{2}} \quad \Rightarrow \quad d = 0 \quad \text{but need} \quad bd = \frac{1}{\sqrt{2}}$$

More Consequences

1. $$\{ \ |v\rangle \otimes |w\rangle : |v\rangle \in V, |w\rangle \in W \ \} \text{ does NOT exhaust } V \otimes W$$

Not all vectors in $V \otimes W$ can be expressed as $|v\rangle \otimes |w\rangle$. However,

$$V \otimes W = \text{span}\{ \ |v\rangle \otimes |w\rangle : |v\rangle \in V, |w\rangle \in W \ \}$$

$$\underbrace{\left(\tfrac{\sqrt{3}}{2}|0\rangle + \tfrac{1}{2}|1\rangle\right)}_{|v\rangle} \otimes \underbrace{\left(\tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle\right)}_{|w\rangle} = \left(\frac{\sqrt{3}}{2\sqrt{2}}|00\rangle + \frac{\sqrt{3}}{2\sqrt{2}}|01\rangle + \frac{1}{2\sqrt{2}}|10\rangle + \frac{1}{2\sqrt{2}}|11\rangle\right)$$

$$(a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) \quad \times \quad \left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right)$$

$$ad = 0, \quad ac = \frac{1}{\sqrt{2}} \quad \Rightarrow \quad d = 0 \quad \text{but need} \quad bd = \frac{1}{\sqrt{2}}$$

Separable and Entangled states

Definition

Consider a joint quantum system consisting of 2 constituent quantum systems. The joint state vector $|\phi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is separable if $|\phi\rangle$ can be expressed as a tensor product of constituent state vectors $|\phi_1\rangle \in \mathcal{H}_A$, $|\phi_2\rangle \in \mathcal{H}_B$, i.e,

$$|\phi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle .$$

A joint state vector is entangled if it is not separable.

Example

The state $|\Phi^-\rangle := \left(\frac{1}{\sqrt{2}} |00\rangle - \frac{1}{\sqrt{2}} |11\rangle \right)$ is entangled.

Separable and Entangled states

Definition

Consider a joint quantum system consisting of 2 constituent quantum systems. The joint state vector $|\phi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is separable if $|\phi\rangle$ can be expressed as a tensor product of constituent state vectors $|\phi_1\rangle \in \mathcal{H}_A$, $|\phi_2\rangle \in \mathcal{H}_B$, i.e,

$$|\phi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle \, .$$

A joint state vector is entangled if it is not separable.

Example

The state $|\Psi^+\rangle := \left(\frac{1}{\sqrt{2}} |01\rangle + \frac{1}{\sqrt{2}} |10\rangle \right)$ is entangled.

Separable and Entangled states

Definition

Consider a joint quantum system consisting of 2 constituent quantum systems. The joint state vector $|\phi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is separable if $|\phi\rangle$ can be expressed as a tensor product of constituent state vectors $|\phi_1\rangle \in \mathcal{H}_A$, $|\phi_2\rangle \in \mathcal{H}_B$, i.e,

$$|\phi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle \,.$$

A joint state vector is entangled if it is not separable.

Example

The state $\quad |\Psi^-\rangle := \left(\frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle\right)$ is entangled.

Separable and Entangled states

Definition

Consider a joint quantum system consisting of 2 constituent quantum systems. The joint state vector $|\phi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is separable if $|\phi\rangle$ can be expressed as a tensor product of constituent state vectors $|\phi_1\rangle \in \mathcal{H}_A$, $|\phi_2\rangle \in \mathcal{H}_B$, i.e,

$$|\phi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle .$$

A joint state vector is entangled if it is not separable.

Example

The state $|\Phi^+\rangle := \left(\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle \right)$ is entangled.

Separable and Entangled states

Definition

Consider a joint quantum system consisting of 2 constituent quantum systems. The joint state vector $|\phi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is separable if $|\phi\rangle$ can be expressed as a tensor product of constituent state vectors $|\phi_1\rangle \in \mathcal{H}_A$, $|\phi_2\rangle \in \mathcal{H}_B$, i.e,

$$|\phi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle \,.$$

A joint state vector is entangled if it is not separable.

Example

The state $|\Phi^+\rangle := \left(\frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle \right)$ is entangled.

individual constituent components have no definite description.

What is state of the first component $|\Phi^+\rangle$: Invalid Qn..

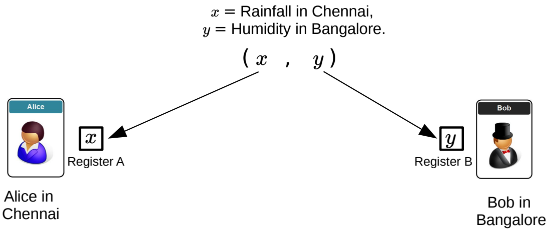
Only state of a joint system.

Entanglement has NO Classical Analogue

The entangled state $|\Phi^+\rangle = \left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right)$ represents the state of a joint system.

Analogous to a pair of registers storing the values of two quantities.

Joint System in our Classical World



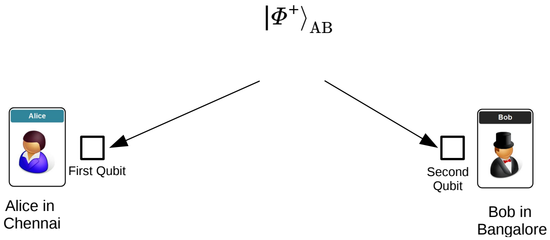
Inspite of (potentially) correlated/ or related, each element of the pair (x, y) has its identity, description.

Entanglement has NO Classical Analogue

The entangled state $|\Phi^+\rangle = \left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right)$ represents the state of a joint system.

Analogous to a pair of registers storing the values of two quantities.

Joint System in our Quantum World



Alice and Bob can share a pair of qubits describing the joint system.

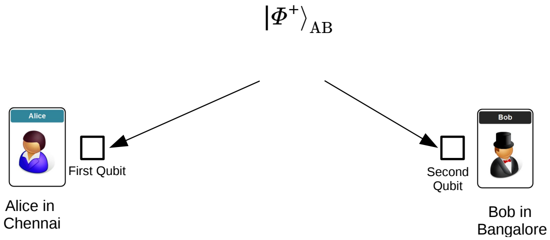
However, each qubit has no definite description, identity.

Entanglement has NO Classical Analogue

The entangled state $|\Phi^+\rangle = \left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right)$ represents the state of a joint system.

Analogous to a pair of registers storing the values of two quantities.

Joint System in our Quantum World



Alice and Bob can share a pair of qubits describing the joint system.

However, each qubit has no definite description, identity.

The joint system is in a superposition of states $|00\rangle$ and $|11\rangle$.

Entanglement

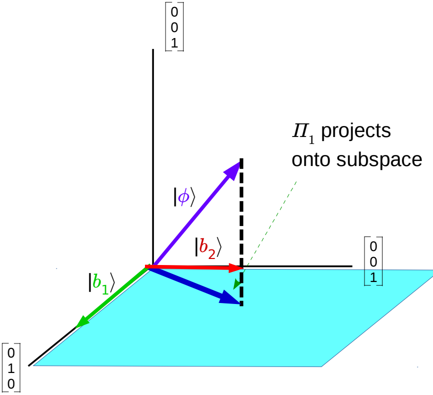
$+$

Randomness in measurement outcomes

yield new information processing resources.

Getting used to the Ket-Bra notation

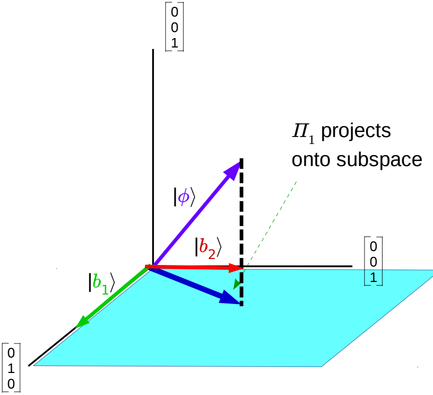
What is $\Pi_1 |\phi\rangle$?



Getting used to the Ket-Bra notation

What is $\Pi_1 |\phi\rangle$?

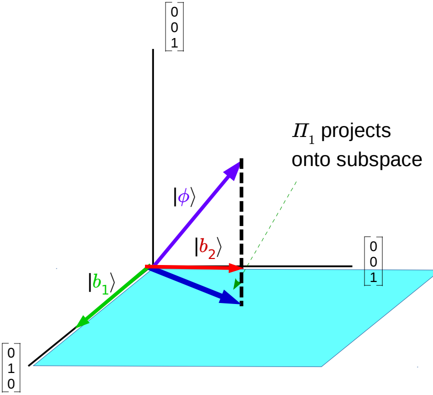
$$\Pi_1 |\phi\rangle = \underbrace{\qquad\qquad}_{\text{IP between } |b_1\rangle \text{and } |\phi\rangle} |b_1\rangle + \underbrace{\qquad\qquad}_{\text{IP between } |b_2\rangle \text{and } |\phi\rangle} |b_2\rangle$$



Getting used to the Ket-Bra notation

What is $\Pi_1 |\phi\rangle$?

$$\Pi_1 |\phi\rangle = \underbrace{\langle b_1|\phi\rangle}_{\substack{\text{IP between} \\ |b_1\rangle \text{and } |\phi\rangle}} |b_1\rangle + \underbrace{\langle b_2|\phi\rangle}_{\substack{\text{IP between} \\ |b_2\rangle \text{and } |\phi\rangle}} |b_2\rangle$$

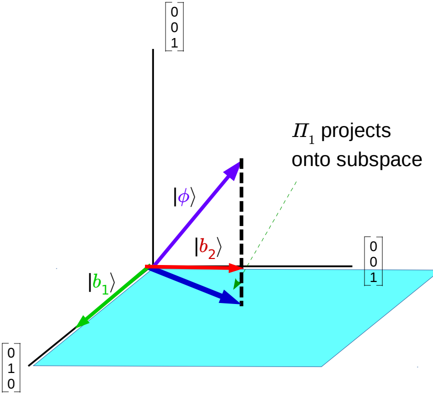


Getting used to the Ket-Bra notation

What is $\Pi_1 |\phi\rangle$?

$$\Pi_1 |\phi\rangle = \underbrace{\langle b_1|\phi\rangle}_{\substack{\text{IP between}\\ |b_1\rangle \text{and } |\phi\rangle}} |b_1\rangle + \underbrace{\langle b_2|\phi\rangle}_{\substack{\text{IP between}\\ |b_2\rangle \text{and } |\phi\rangle}} |b_2\rangle$$

$$\Pi_1 |\phi\rangle = \underbrace{\langle b_1|\phi\rangle}_{\text{scalar}} \underbrace{|b_1\rangle}_{\text{vector}} + \underbrace{\langle b_2|\phi\rangle}_{\text{scalar}} \underbrace{|b_2\rangle}_{\text{vector}}$$



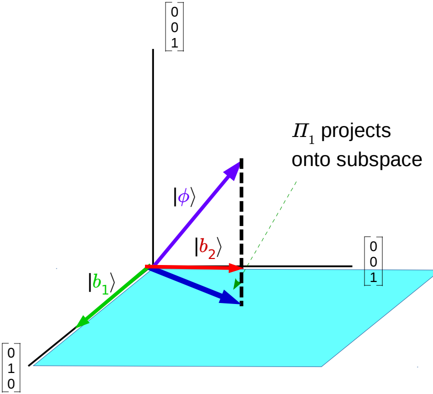
Getting used to the Ket-Bra notation

What is $\Pi_1 |\phi\rangle$?

$$\Pi_1 |\phi\rangle = \underbrace{\langle b_1|\phi\rangle}_{\substack{\text{IP between} \\ |b_1\rangle \text{and } |\phi\rangle}} \quad |b_1\rangle + \underbrace{\langle b_2|\phi\rangle}_{\substack{\text{IP between} \\ |b_2\rangle \text{and } |\phi\rangle}} \quad |b_2\rangle$$

$$\Pi_1 |\phi\rangle = \underbrace{\langle b_1|\phi\rangle}_{\text{scalar}} \underbrace{|b_1\rangle}_{\text{vector}} + \underbrace{\langle b_2|\phi\rangle}_{\text{scalar}} \underbrace{|b_2\rangle}_{\text{vector}}$$

$$\Pi_1 |\phi\rangle = \underbrace{|b_1\rangle}_{\text{vector}} \underbrace{\langle b_1|\phi\rangle}_{\text{scalar}} + \underbrace{|b_2\rangle}_{\text{vector}} \underbrace{\langle b_2|\phi\rangle}_{\text{scalar}}$$



Getting used to the Ket-Bra notation

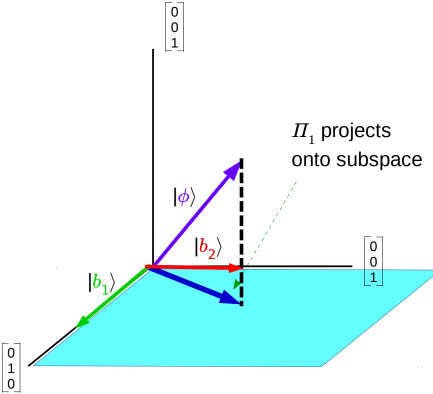
What is $\Pi_1 |\phi\rangle$?

$$\Pi_1 |\phi\rangle = \underbrace{\langle b_1|\phi\rangle}_{\substack{\text{IP between} \\ |b_1\rangle \text{and } |\phi\rangle}} |b_1\rangle + \underbrace{\langle b_2|\phi\rangle}_{\substack{\text{IP between} \\ |b_2\rangle \text{and } |\phi\rangle}} |b_2\rangle$$

$$\Pi_1 |\phi\rangle = \underbrace{\langle b_1|\phi\rangle}_{\text{scalar}} \underbrace{|b_1\rangle}_{\text{vector}} + \underbrace{\langle b_2|\phi\rangle}_{\text{scalar}} \underbrace{|b_2\rangle}_{\text{vector}}$$

$$\Pi_1 |\phi\rangle = \underbrace{|b_1\rangle}_{\text{vector}} \underbrace{\langle b_1|\phi\rangle}_{\text{scalar}} + \underbrace{|b_2\rangle}_{\text{vector}} \underbrace{\langle b_2|\phi\rangle}_{\text{scalar}}$$

$$\Pi_1 |\phi\rangle = |b_1\rangle \langle b_1|\phi\rangle + |b_2\rangle \langle b_2|\phi\rangle$$



Getting used to the Ket-Bra notation

What is $\Pi_1 |\phi\rangle$?

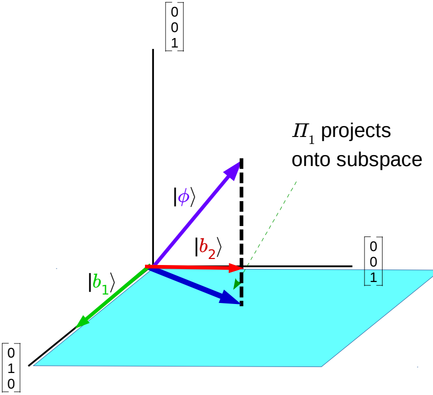
$$\Pi_1 |\phi\rangle = \underbrace{\langle b_1|\phi\rangle}_{\text{IP between } |b_1\rangle \text{and } |\phi\rangle} |b_1\rangle + \underbrace{\langle b_2|\phi\rangle}_{\text{IP between } |b_2\rangle \text{and } |\phi\rangle} |b_2\rangle$$

$$\Pi_1 |\phi\rangle = \underbrace{\langle b_1|\phi\rangle}_{\text{scalar}} \underbrace{|b_1\rangle}_{\text{vector}} + \underbrace{\langle b_2|\phi\rangle}_{\text{scalar}} \underbrace{|b_2\rangle}_{\text{vector}}$$

$$\Pi_1 |\phi\rangle = \underbrace{|b_1\rangle}_{\text{vector}} \underbrace{\langle b_1|\phi\rangle}_{\text{scalar}} + \underbrace{|b_2\rangle}_{\text{vector}} \underbrace{\langle b_2|\phi\rangle}_{\text{scalar}}$$

$$\Pi_1 |\phi\rangle = |b_1\rangle \langle b_1|\phi\rangle + |b_2\rangle \langle b_2|\phi\rangle$$

$$\Pi_1 |\phi\rangle = \underbrace{(|b_1\rangle \langle b_1| + |b_2\rangle \langle b_2|)}_{\Pi_1} |\phi\rangle$$



Getting used to the Ket-Bra notation

What is $\Pi_1 |\phi\rangle$?

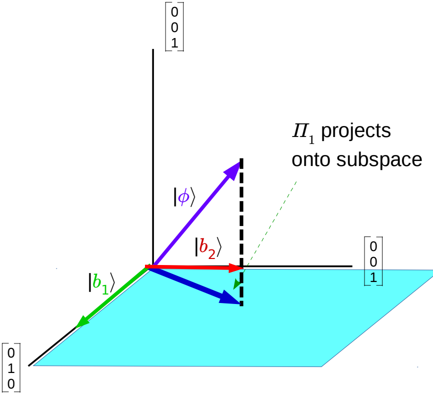
$$\Pi_1 |\phi\rangle = \underbrace{\langle b_1|\phi\rangle}_{\text{IP between } |b_1\rangle \text{and } |\phi\rangle} |b_1\rangle + \underbrace{\langle b_2|\phi\rangle}_{\text{IP between } |b_2\rangle \text{and } |\phi\rangle} |b_2\rangle$$

$$\Pi_1 |\phi\rangle = \underbrace{\langle b_1|\phi\rangle}_{\text{scalar}} \underbrace{|b_1\rangle}_{\text{vector}} + \underbrace{\langle b_2|\phi\rangle}_{\text{scalar}} \underbrace{|b_2\rangle}_{\text{vector}}$$

$$\Pi_1 |\phi\rangle = \underbrace{|b_1\rangle}_{\text{vector}} \underbrace{\langle b_1|\phi\rangle}_{\text{scalar}} + \underbrace{|b_2\rangle}_{\text{vector}} \underbrace{\langle b_2|\phi\rangle}_{\text{scalar}}$$

$$\Pi_1 |\phi\rangle = |b_1\rangle \langle b_1|\phi\rangle + |b_2\rangle \langle b_2|\phi\rangle$$

$$\Pi_1 |\phi\rangle = \underbrace{(|b_1\rangle \langle b_1| + |b_2\rangle \langle b_2|)}_{\Pi_1} |\phi\rangle$$



$$\underbrace{\langle a|b\rangle}_{\text{bra-ket}} \quad \underbrace{\langle a|}_{\text{bra}} \quad \underbrace{|b\rangle}_{\text{ket}} \quad \underbrace{|b\rangle\langle b|}_{\text{ket-bra}}$$

Ket-Bra Notation

The ket-bra notation is very useful in simplifying computation.

Suppose Π is a projection onto subspace $\mathcal{W} \subseteq \mathcal{H}$.

Suppose $\{|v_1\rangle, \cdots, |v_r\rangle\} \in \mathcal{W}$ is an orthonormal basis (ONB).

$$\Pi = |v_1\rangle\langle v_1| + |v_2\rangle\langle v_2| + \cdots |v_r\rangle\langle v_r| = \textstyle\sum_{i=1}^{r} |v_i\rangle\langle v_i|$$

$$\Pi|\phi\rangle = \textstyle\sum_i |v_i\rangle \underbrace{\langle v_i| \;\; |\phi\rangle} = \sum_i |v_i\rangle \underbrace{\langle v_i|\phi\rangle}_{\text{scalar}} = \sum_i \underbrace{\langle v_i|\phi\rangle}_{\text{scalar}} \;\; \underbrace{|v_i\rangle}_{\text{vector}}$$

$$|\langle v_i|\phi\rangle| = \text{Length of projection of } |\phi\rangle \text{ on } |v_i\rangle$$

$$\textstyle\sum_i \langle v_i|\phi\rangle \; |v_i\rangle = \text{Projection of } |\phi\rangle \text{ on subspace } \mathcal{W}$$

$$\text{Bra-ket Notation } |a\rangle\langle b|\,|c\rangle = \langle b|c\rangle\,|a\rangle$$

Suppose $\mathcal{H}_A$ has ONB $\{|v_1\rangle \cdots, |v_d\rangle\}$, then any linear transformation $T : \mathcal{H} \to \mathcal{H}$ can be expressed as

$$T = \sum_{i=1}^{d} \sum_{j=1}^{d} t_{ij} |v_i\rangle\langle v_j|.$$

Ket-Bra Notation

The ket-bra notation is very useful in simplifying computation.

Suppose Π is a projection onto subspace $\mathcal{W} \subseteq \mathcal{H}$.

Suppose $\{|v_1\rangle, \cdots, |v_r\rangle\} \in \mathcal{W}$ is an orthonormal basis (ONB).

$$\Pi = |v_1\rangle\langle v_1| + |v_2\rangle\langle v_2| + \cdots |v_r\rangle\langle v_r| = \sum_{i=1}^{r} |v_i\rangle\langle v_i|$$

$$\Pi|\phi\rangle = \sum_i |v_i\rangle \underbrace{\langle v_i| \quad |\phi\rangle} = \sum_i |v_i\rangle \underbrace{\langle v_i|\phi\rangle}_{\text{scalar}} = \sum_i \underbrace{\langle v_i|\phi\rangle}_{\text{scalar}} \quad \underbrace{|v_i\rangle}_{\text{vector}}$$

$|\langle v_i|\phi\rangle|$ = Length of projection of $|\phi\rangle$ on $|v_i\rangle$

$\sum_i \langle v_i|\phi\rangle \; |v_i\rangle$ = Projection of $|\phi\rangle$ on subspace $\mathcal{W}$

Bra-ket Notation $|a\rangle\langle b|\,|c\rangle = \langle b|c\rangle\,|a\rangle$

Suppose $\mathcal{H}_A$ has ONB $\{|v_1\rangle \cdots, |v_d\rangle\}$, then any linear transformation $T : \mathcal{H} \to \mathcal{H}$ can be expressed as

$$T = \sum_{i=1}^{d} \sum_{j=1}^{d} t_{ij} |v_i\rangle\langle v_j|.$$ Scalars $t_{ij} : 1 \le i, j \le d$ completely characterize T

Ket-Bra Notation

$$T = |a\rangle\langle b|$$

$$T|c\rangle = |a\rangle\langle b||c\rangle = \langle b|c\rangle|a\rangle$$

What is T doing on $|c\rangle$?

Ket-Bra Notation

$$T = |a\rangle \langle b|$$

$$T |c\rangle = |a\rangle \langle b| |c\rangle = \langle b|c\rangle |a\rangle$$

What is T doing on $|c\rangle$?

Scaling $|a\rangle$ by length of projection of $|c\rangle$ on $|b\rangle$.

Ket-Bra Notation

$$T = |a\rangle\langle b|$$

$$T|c\rangle = |a\rangle\langle b|\,|c\rangle = \langle b|c\rangle\,|a\rangle$$

What is T doing on $|c\rangle$?

Scaling $|a\rangle$ by length of projection of $|c\rangle$ on $|b\rangle$.

$|\cdot\rangle\langle\cdot|$ is an Operator

$\langle\cdot|\,|\cdot\rangle = \langle\cdot|\cdot\rangle$ is a scalar

$|\cdot\rangle$ is an vector

$\langle\cdot|$ is a linear functional

Examples of Ket-Bra notation with Tensor Products

Recall Operative Distributive Law

$$(A \otimes B)(|v\rangle \otimes |w\rangle) = A\,|v\rangle \otimes B\,|w\rangle \quad \text{Operator Dist. Law (ODL) 1}$$

Examples of Ket-Bra notation with Tensor Products

Suppose $|0\rangle\langle 0| : \mathbb{R}^2 \to \mathbb{R}^2$ (Op. on our qubit space : say A–space)

Examples of Ket-Bra notation with Tensor Products

$$\text{Suppose } |0\rangle\langle 0| : \mathbb{R}^2 \to \mathbb{R}^2 \quad (\text{Op. on our qubit space : say } A\text{–space})$$

$$\text{Suppose } I_B : \mathbb{R}^2 \to \mathbb{R}^2 \quad (\text{A second qubit space : } B\text{–space})$$

Examples of Ket-Bra notation with Tensor Products

Suppose $|0\rangle\langle 0| : \mathbb{R}^2 \to \mathbb{R}^2$ (Op. on our qubit space : say A–space)

Suppose $I_B : \mathbb{R}^2 \to \mathbb{R}^2$ (A second qubit space : B–space)

What is $|0\rangle\langle 0| \otimes I_B : \mathbb{R}^2 \otimes \mathbb{R}^2 \to \mathbb{R}^2 \otimes \mathbb{R}^2???$

Examples of Ket-Bra notation with Tensor Products

Suppose $|0\rangle\langle 0| : \mathbb{R}^2 \to \mathbb{R}^2$ (Op. on our qubit space : say A–space)

Suppose $I_B : \mathbb{R}^2 \to \mathbb{R}^2$ (A second qubit space : B–space)

What is $|0\rangle\langle 0| \otimes I_B : \mathbb{R}^2 \otimes \mathbb{R}^2 \to \mathbb{R}^2 \otimes \mathbb{R}^2$???

$$I_B = \underbrace{|0\rangle\langle 0| + |1\rangle\langle 1|}_{\text{Sum of two operators}}$$

Examples of Ket-Bra notation with Tensor Products

$$\text{Suppose } |0\rangle\langle 0| : \mathbb{R}^2 \to \mathbb{R}^2 \quad (\text{Op. on our qubit space : say } A\text{–space})$$

$$\text{Suppose } I_B : \mathbb{R}^2 \to \mathbb{R}^2 \quad (\text{A second qubit space : } B\text{–space})$$

$$\text{What is } |0\rangle\langle 0| \otimes I_B : \mathbb{R}^2 \otimes \mathbb{R}^2 \to \mathbb{R}^2 \otimes \mathbb{R}^2???$$

$$I_B = \underbrace{|0\rangle\langle 0| + |1\rangle\langle 1|}_{\text{Sum of two operators}}$$

$$\text{Recall ODL 3} \qquad A \otimes (B_1 + B_2) = A \otimes B_1 + A \otimes B_2$$

$$\begin{aligned} |0\rangle\langle 0| \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|) &= |0\rangle\langle 0| \otimes |0\rangle\langle 0| + |0\rangle\langle 0| \otimes |1\rangle\langle 1| \\ &= |00\rangle\langle 00| + |01\rangle\langle 01| \end{aligned}$$

$|0\rangle\langle 0| \otimes I_B = |00\rangle\langle 00| + |01\rangle\langle 01| =$ Projection on subspace spanned by $|00\rangle, |01\rangle$.

Points to keep in mind

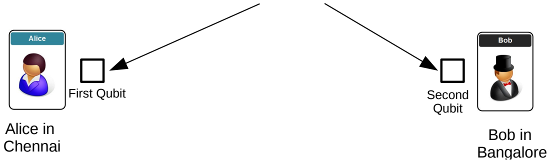
$|0\rangle\langle 0| \otimes I_B = |00\rangle\langle 00| + |01\rangle\langle 01|$ = Projection on subspace spanned by $|00\rangle, |01\rangle$.

$|1\rangle\langle 1| \otimes I_B = |10\rangle\langle 10| + |11\rangle\langle 11|$ = Projection on subspace spanned by $|10\rangle, |11\rangle$.

Entangled pair can be separated, Acted upon Individually

Components of the joint system can be separated, Acted upon Individually

$$|\Phi^+\rangle_{AB}$$



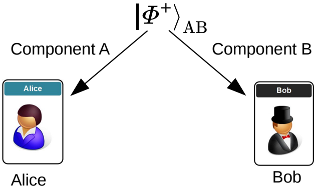
Suppose Alice performs measurement $\{\Pi_1, \cdots, \Pi_K\}$. Bob remains silent.

?? Effect on Joint system ??

Equivalent to measurement $\{\Pi_1 \otimes I_B, \cdots, \Pi_K \otimes I_B\}$ on joint system.

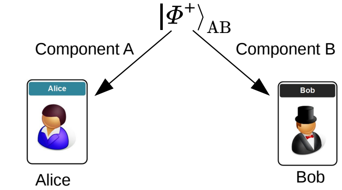
Only Alice sees outcome. Joint state collapses.

Measurement on a Distributed Entangled State



$$|\Phi^+\rangle = \left(\frac{1}{\sqrt{2}}\,|0\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle \otimes |1\rangle\right)$$

Measurement on a Distributed Entangled State



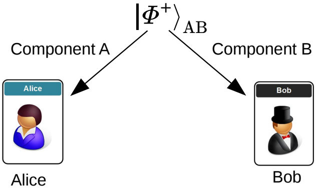
$$|\Phi^+\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle \otimes |0\rangle + \frac{1}{\sqrt{2}}|1\rangle \otimes |1\rangle\right)$$

Alice performs measurement
$\{\Pi_0 = |0\rangle\langle 0|, \Pi_1 = |1\rangle\langle 1|\}$

Bob does nothing.

Measurement on joint system
$\{|0\rangle\langle 0| \otimes I_B, |1\rangle\langle 1| \otimes I_B\}$

Measurement on a Distributed Entangled State



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

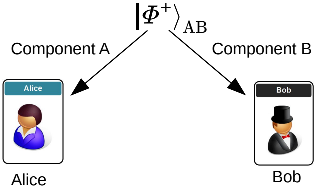
Alice performs measurement
$\{\Pi_0 = |0\rangle\langle 0|, \Pi_1 = |1\rangle\langle 1|\}$

Bob does nothing.

Measurement on joint system
$\{|0\rangle\langle 0| \otimes I_B, |1\rangle\langle 1| \otimes I_B\}$
equivalent to

$$\left\{\begin{array}{l} \Pi_0 \otimes I_B = |00\rangle\langle 00| + |01\rangle\langle 01|, \\ \Pi_1 \otimes I_B = |10\rangle\langle 10| + |11\rangle\langle 11| \end{array}\right\}$$

Measurement on a Distributed Entangled State



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

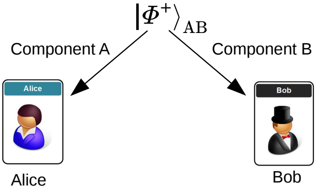
Alice performs measurement
$\{\Pi_0 = |0\rangle\langle 0|, \Pi_1 = |1\rangle\langle 1|\}$

Bob does nothing.

Measurement on joint system

$$\left\{\begin{array}{l} \Pi_0 \otimes I_B = |00\rangle\langle 00| + |01\rangle\langle 01|, \\ \Pi_1 \otimes I_B = |10\rangle\langle 10| + |11\rangle\langle 11| \end{array}\right\}$$

Measurement on a Distributed Entangled State



$$|\Phi^+\rangle = \left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right)$$

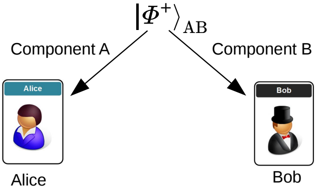
Alice performs measurement
$\{\Pi_0 = |0\rangle\langle 0|, \Pi_1 = |1\rangle\langle 1|\}$

Bob does nothing.

Measurement on joint system

$$\left\{\begin{array}{l}\Pi_0 \otimes I_B = |00\rangle\langle 00| + |01\rangle\langle 01|, \\ \Pi_1 \otimes I_B = |10\rangle\langle 10| + |11\rangle\langle 11|\end{array}\right\}$$

Measurement on a Distributed Entangled State



$$|\Phi^+\rangle = \left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right)$$

Alice performs measurement
$\{\Pi_0 = |0\rangle\langle 0|, \Pi_1 = |1\rangle\langle 1|\}$

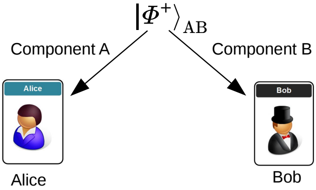
Bob does nothing.

Measurement on joint system

$$\left\{\begin{array}{l} \Pi_0 \otimes I_B = |00\rangle\langle 00| + |01\rangle\langle 01|, \\ \Pi_1 \otimes I_B = |10\rangle\langle 10| + |11\rangle\langle 11| \end{array}\right\}$$

Outcome 0 with prob. $\frac{1}{2}$.
Outcome $0 \Rightarrow$ State collapses to $|00\rangle$

Measurement on a Distributed Entangled State



$$|\Phi^+\rangle = \left(\frac{1}{\sqrt{2}}{\color{red}|00\rangle} + \frac{1}{\sqrt{2}}{\color{green}|11\rangle}\right)$$

Alice performs measurement
$\{\Pi_0 = |0\rangle\langle 0|, \Pi_1 = |1\rangle\langle 1|\}$

Bob does nothing.

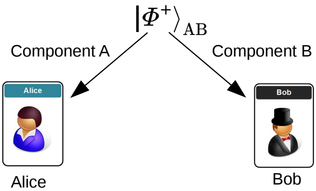
Measurement on joint system

$$\begin{Bmatrix} \Pi_0 \otimes I_B = {\color{red}|00\rangle\langle 00|} + |01\rangle\langle 01|, \\ \Pi_1 \otimes I_B = |10\rangle\langle 10| + {\color{green}|11\rangle\langle 11|} \end{Bmatrix}$$

Outcome 0 with prob. $\frac{1}{2}$.
Outcome $0 \Rightarrow$ State collapses to $|00\rangle$

Outcome 1 with prob. $\frac{1}{2}$.
Outcome $0 \Rightarrow$ State collapses to $|11\rangle$

Measurement on a Distributed Entangled State



$$|\Phi^+\rangle = \left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right)$$

Alice performs measurement
$\{\Pi_0 = |0\rangle\langle 0|, \Pi_1 = |1\rangle\langle 1|\}$

Bob does nothing.

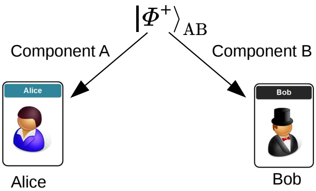
Post Measurement on joint system
Outcome 0 with prob. $\frac{1}{2}$.
State collapses to $|00\rangle$

States are UNENTANGLED

Outcome 0 and state $|0\rangle$

No Outcome. State $|0\rangle$
Meas. $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$
Sure shot outcome 0.

Distributed Generation of common randomness



$$|\Phi^+\rangle = \left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right)$$

Alice performs measurement
$\{\Pi_0 = |0\rangle\langle 0|, \Pi_1 = |1\rangle\langle 1|\}$

Bob does nothing.

Post Measurement on joint system

Outcome 1 with prob. $\frac{1}{2}$.

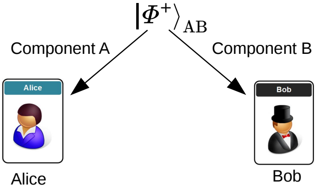
State collapses to $|11\rangle$

States are UNENTANGLED

Outcome 1 and state $|1\rangle$

No Outcome. State $|1\rangle$
Meas. $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$
Sure shot outcome 1.

Distributed Generation of common randomness



$$|\Phi^+\rangle = \left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right)$$

Alice in Nice, Bob in Paris can generate common randomness.

Experimentally, components of entangled pair are separated by 1100 kms!!!!

Idea Points to take Home

Entangled particles evolve simultanneously.

If you perturb one, the other gets perturbed.

If you wish to perturb the other, you can perturb your qubit!!!

A Quantum system cannot be Cloned - The No-Cloning Theorem

The contents of a (classical) register can be copied onto another register.

However, the state of a quantum system cannot be duplicated or cloned.

Given an arbitrary state $|\phi\rangle$, there exists no unitary transformation that can duplicate this state.

Theorem

There exists no unitary transformation $U : \mathcal{H} \otimes \mathcal{H} \to \mathcal{H} \otimes \mathcal{H}$ and a state $|\omega\rangle \in \mathcal{H}$ such that

$$U\left(|\phi\rangle \otimes |\omega\rangle\right) = |\phi\rangle \otimes |\phi\rangle$$

holds for every $|\phi\rangle \in \mathcal{H}$.

2. Quantum Gates

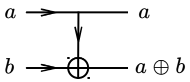
Boolean Gates

A classical computation ≡ a map $f : \{0,1\}^n \to \{0,1\}^n$.

Computation is reversible if the input bits can be determined from the output bits, i.e., f is invertible ($1:1$ and ONTO).

Example : NAND is NOT reversible.

Example : Controlled NOT (C-NOT)



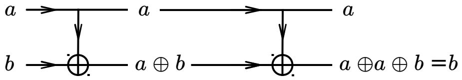
Boolean Gates

A classical computation ≡ a map $f : \{0,1\}^n \to \{0,1\}^n$.

Computation is reversible if the input bits can be determined from the output bits, i.e., f is invertible ($1:1$ and ONTO).

Example : NAND is NOT reversible.

Example : Controlled NOT (C-NOT)



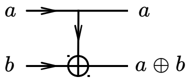
Boolean Gates

A classical computation ≡ a map $f : \{0,1\}^n \to \{0,1\}^n$.

Computation is reversible if the input bits can be determined from the output bits, i.e., f is invertible ($1:1$ and ONTO).

Example : NAND is NOT reversible.

Example : Controlled NOT (C-NOT) is reversible.



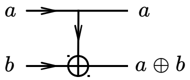
Boolean Gates

A classical computation ≡ a map $f : \{0, 1\}^n \to \{0, 1\}^n$.

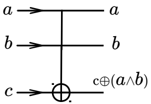
Computation is reversible if the input bits can be determined from the output bits, i.e., f is invertible ($1 : 1$ and ONTO).

Example : NAND is NOT reversible.

Example : Controlled NOT (C-NOT) is reversible.



Example : CC-NOT (C-NOT) is reversible.



Quantum Gates and Operations are Unitary Transformations

Quantum circuits map superposition of n qubits into a superposition of n qubits.

$$\text{Quantum Gate} : |\phi\rangle \mapsto |\omega\rangle.$$

Valid Transformations : 1) Norm Preservation $\langle\phi|\phi\rangle = \langle\omega|\omega\rangle$. 2) Linearity.

Non-Linearity results in physical unrealizability.

Quantum Gate is a Unitary Transformation.

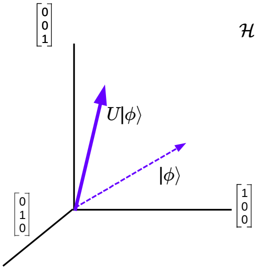
Quantum Gates and Operations are Unitary Transformations

Quantum circuits map superposition of n qubits into a superposition of n qubits.

$$\text{Quantum Gate} : |\phi\rangle \mapsto |\omega\rangle.$$

Valid Transformations : 1) Norm Preservation $\langle\phi|\phi\rangle = \langle\omega|\omega\rangle$. 2) Linearity.

Non-Linearity results in physical unrealizability.



Quantum Gate is a Unitary Transformation.

Quantum Operations : Unitary Transformations Mapping n qubits to n qubits.

Operation of a Quantum Gate : Completely specified by action on its bases.

$$\text{Only need } |0\rangle \mapsto \; ? \text{ and } |1\rangle \mapsto \; ?$$

Single Qubit Gates - Pauli gates

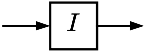
Identity Gate

$$\longrightarrow \boxed{I} \longrightarrow$$

$$I : \begin{array}{c} |0\rangle \mapsto |0\rangle \\ |1\rangle \mapsto |1\rangle \end{array}$$

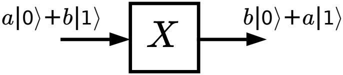
Single Qubit Gates - Pauli gates

Identity Gate



$$I : \begin{array}{l} |0\rangle \mapsto |0\rangle \\ |1\rangle \mapsto |1\rangle \end{array}$$

Pauli $X-$ Gate



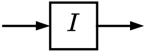
$$X : \begin{array}{l} |0\rangle \mapsto |1\rangle \\ |1\rangle \mapsto |0\rangle \end{array}$$

Matrix Representation

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

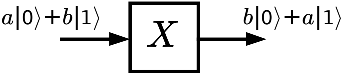
Single Qubit Gates - Pauli gates

Identity Gate



$$I : \begin{array}{l} |0\rangle \mapsto |0\rangle \\ |1\rangle \mapsto |1\rangle \end{array}$$

Pauli $X-$ Gate

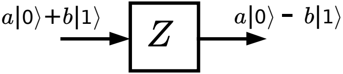


$$X : \begin{array}{l} |0\rangle \mapsto |1\rangle \\ |1\rangle \mapsto |0\rangle \end{array}$$

Matrix Representation

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

Pauli $Z-$Gate



$$Z : \begin{array}{l} |0\rangle \mapsto |0\rangle \\ |1\rangle \mapsto -|1\rangle \end{array}$$

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

Single Qubit Gates - Pauli gates

Identity Gate

$$\longrightarrow \boxed{I} \longrightarrow$$

$$I : \begin{array}{l} |0\rangle \mapsto |0\rangle \\ |1\rangle \mapsto |1\rangle \end{array}$$

Pauli $X-$ Gate

$$a|0\rangle + b|1\rangle \longrightarrow \boxed{X} \longrightarrow b|0\rangle + a|1\rangle$$

$$X : \begin{array}{l} |0\rangle \mapsto |1\rangle \\ |1\rangle \mapsto |0\rangle \end{array}$$

Matrix Representation

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

Pauli $Z-$Gate

$$a|0\rangle + b|1\rangle \longrightarrow \boxed{Z} \longrightarrow a|0\rangle - b|1\rangle$$

$$Z : \begin{array}{l} |0\rangle \mapsto |0\rangle \\ |1\rangle \mapsto -|1\rangle \end{array}$$

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

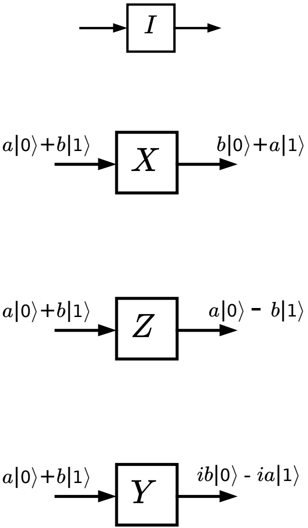
Pauli $Y-$Gate

$$a|0\rangle + b|1\rangle \longrightarrow \boxed{Y} \longrightarrow ib|0\rangle - ia|1\rangle$$

$$Y : \begin{array}{l} |0\rangle \mapsto i\,|1\rangle \\ |1\rangle \mapsto -i\,|0\rangle \end{array}$$

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

Playing with the Pauli I, X, Y, Z Gates

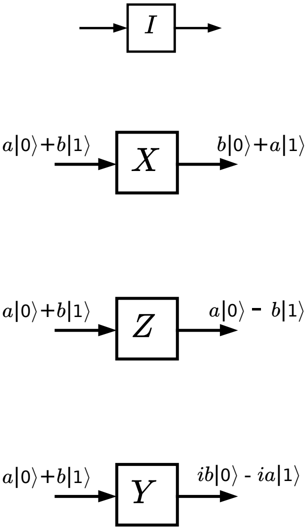


Your task is to recover the qubit $a|0\rangle + b|1\rangle$.

Which operator will you use if you are given

State you are given	Operator to use
$a\|0\rangle - b\|1\rangle$	
$b\|0\rangle + a\|1\rangle$	
$b\|0\rangle - a\|1\rangle$	

Playing with the Pauli I, X, Y, Z Gates



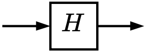
Your task is to recover the qubit $a\,|0\rangle + b\,|1\rangle$.

Which operator will you use if you are given

State you are given	Operator to use
$a\,|0\rangle - b\,|1\rangle$	Z
$b\,|0\rangle + a\,|1\rangle$	X
$b\,|0\rangle - a\,|1\rangle$	First Z, then X

The Hadamard Gate and Some Interesting Properties

Hadamard Gate



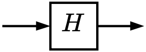
$$H: \begin{array}{l} |0\rangle \mapsto \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle =: |+\rangle \\ |1\rangle \mapsto \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle =: |-\rangle \end{array}$$

Matrix Representation

$$H = \frac{1}{\sqrt{2}}\left[\begin{array}{cc} 1 & 1 \\ 1 & -1 \end{array}\right]$$

The Hadamard Gate and Some Interesting Properties

Hadamard Gate



$$H : \begin{array}{l} |0\rangle \mapsto \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle =: |+\rangle \\ |1\rangle \mapsto \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle =: |-\rangle \end{array}$$

Matrix Representation

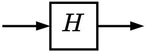
$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Property 1

$$\begin{aligned} (H \otimes H)(|0\rangle \otimes |0\rangle) &= \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \\ &= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \end{aligned}$$

The Hadamard Gate and Some Interesting Properties

Hadamard Gate



$$H : \begin{array}{l} |0\rangle \mapsto \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle =: |+\rangle \\ |1\rangle \mapsto \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle =: |-\rangle \end{array}$$

Matrix Representation

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

Property 1

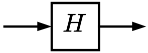
$$\begin{aligned} (H \otimes H)(|0\rangle \otimes |0\rangle) &= \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \\ &= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \end{aligned}$$

$$H^{\otimes n}|0\rangle^{\otimes n} = \sum_{\substack{(b_1,\cdots,b_n) \\ \in\{0,1\}^n}} \frac{1}{\sqrt{2}^n}|b_1 \cdots b_n\rangle$$

All possible bit combinations are stored in $n-$qubits.

The Hadamard Gate and Some Interesting Properties

Hadamard Gate



$$H : \begin{array}{l} |0\rangle \mapsto \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle =: |+\rangle \\ |1\rangle \mapsto \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle =: |-\rangle \end{array}$$

Matrix Representation

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

Property 2

$$|0\rangle \overset{H}{\mapsto} |0\rangle + |1\rangle \quad , \quad |1\rangle \overset{H}{\mapsto} |0\rangle - |1\rangle$$

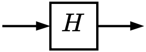
$$|0\rangle \overset{H}{\mapsto} (-1)^{0\cdot 0}|0\rangle + (-1)^{0\cdot 1}|1\rangle,$$

$$|1\rangle \overset{H}{\mapsto} (-1)^{1\cdot 0}|0\rangle + (-1)^{1\cdot 1}|1\rangle,$$

$$|b\rangle \overset{H}{\mapsto} \sum_{z=0}^{1}(-1)^{b\cdot z}|z\rangle,$$

The Hadamard Gate and Some Interesting Properties

Hadamard Gate



$$H : \begin{array}{l} |0\rangle \mapsto \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle =: |+\rangle \\ |1\rangle \mapsto \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle =: |-\rangle \end{array}$$

Matrix Representation

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

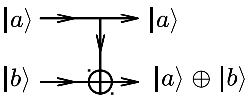
Property 2

$$|b\rangle \overset{H}{\mapsto} \sum_{z=0}^{1} (-1)^{b \cdot z} |z\rangle,$$

$$|b_1 \cdots b_n\rangle \overset{H^{\otimes n}}{\mapsto} \sum_{z^n \in \{0,1\}^n} (-1)^{b_1 \cdot z_1 + \cdots + \cdots b_n z_n} |z_1 \cdots z_n\rangle$$

Our Two Qubit C-NOT Gate

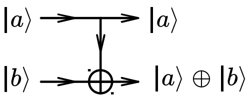
C-NOT Gate



$$\overline{C}: \begin{array}{l} |00\rangle \mapsto |00\rangle \\ |01\rangle \mapsto |01\rangle \\ |10\rangle \mapsto |11\rangle \\ |11\rangle \mapsto |10\rangle \end{array}$$

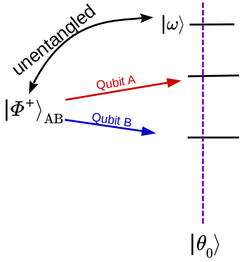
Our Two Qubit C-NOT Gate

C-NOT Gate



$$\overline{C}: \begin{array}{l} |00\rangle \mapsto |00\rangle \\ |01\rangle \mapsto |01\rangle \\ |10\rangle \mapsto |11\rangle \\ |11\rangle \mapsto |10\rangle \end{array}$$

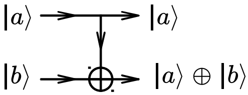
An Application : Entangle two unentangled systems.



Let $|\omega\rangle = a\,|0\rangle + b\,|1\rangle$. $|\theta_0\rangle = |\omega\rangle \otimes |\Phi^+\rangle_{AB}$

Our Two Qubit C-NOT Gate

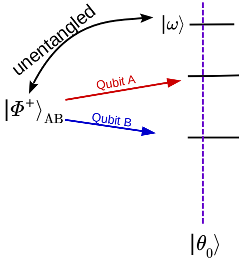
C-NOT Gate



$$\overline{C} : \begin{array}{l} |00\rangle \mapsto |00\rangle \\ |01\rangle \mapsto |01\rangle \\ |10\rangle \mapsto |11\rangle \\ |11\rangle \mapsto |10\rangle \end{array}$$

$$\overline{C} \otimes I : \begin{array}{l} |000\rangle \mapsto |000\rangle \\ |001\rangle \mapsto |001\rangle \\ |010\rangle \mapsto |010\rangle \\ |011\rangle \mapsto |011\rangle \\ |100\rangle \mapsto |110\rangle \\ |111\rangle \mapsto |101\rangle \\ |100\rangle \mapsto |110\rangle \\ |111\rangle \mapsto |101\rangle \end{array}$$

An Application : Entangle two unentangled systems.

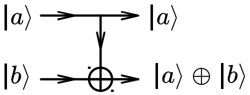


Let $|\omega\rangle = a\,|0\rangle + b\,|1\rangle$. $|\theta_0\rangle = |\omega\rangle \otimes |\Phi^+\rangle_{AB}$

Use gate $\overline{C} \otimes I$

Our Two Qubit C-NOT Gate

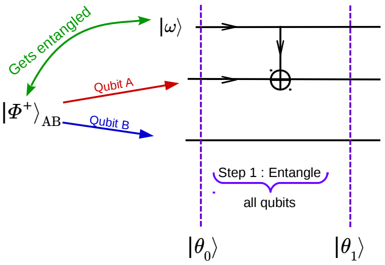
C-NOT Gate



$$\overline{C} : \begin{array}{l} |00\rangle \mapsto |00\rangle \\ |01\rangle \mapsto |01\rangle \\ |10\rangle \mapsto |11\rangle \\ |11\rangle \mapsto |10\rangle \end{array}$$

$$\overline{C} \otimes I : \begin{array}{l} |000\rangle \mapsto |000\rangle \\ |001\rangle \mapsto |001\rangle \\ |010\rangle \mapsto |010\rangle \\ |011\rangle \mapsto |011\rangle \\ |100\rangle \mapsto |110\rangle \\ |111\rangle \mapsto |101\rangle \\ |100\rangle \mapsto |110\rangle \\ |111\rangle \mapsto |101\rangle \end{array}$$

An Application : Entangle two unentangled systems.



Let $|\omega\rangle = a\,|0\rangle + b\,|1\rangle$. $|\theta_0\rangle = |\omega\rangle \otimes |\Phi^+\rangle_{AB}$

Use gate $\overline{C} \otimes I$

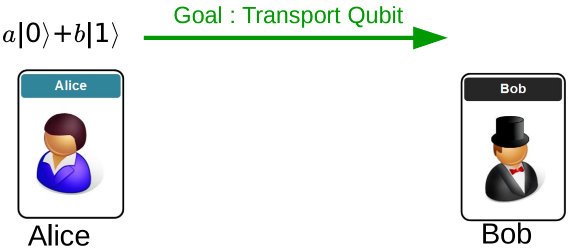
$$|\theta_1\rangle = (\overline{C} \otimes I)\,|\theta_0\rangle = (\overline{C} \otimes I)(|\omega\rangle \otimes |\Phi^+\rangle_{AB})$$

3. Quantum Protocols

Quantum Teleportation

No Cloning Theorem : No Replication of qubits.

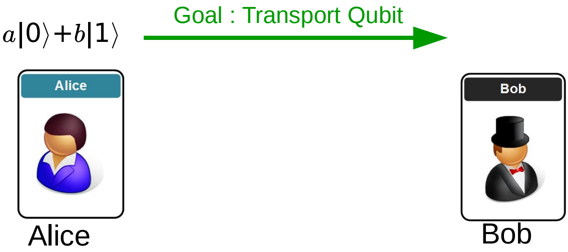
Can we transport them?



Quantum Teleportation

No Cloning Theorem : No Replication of qubits.

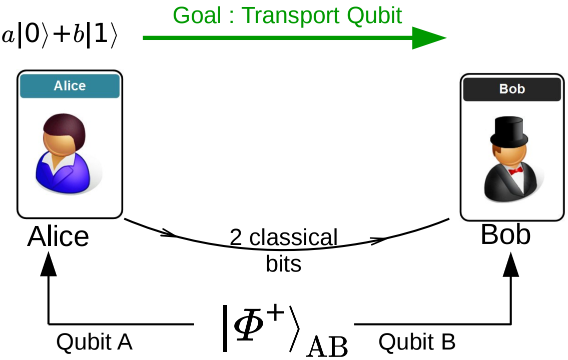
Can we transport them? If YES, what resources do we need?



Quantum Teleportation

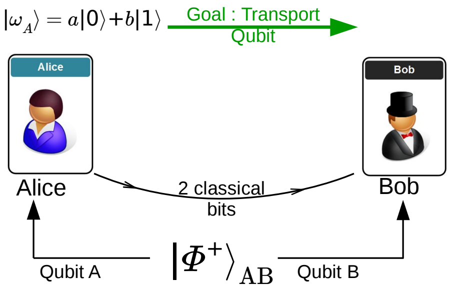
No Cloning Theorem : No Replication of qubits.

Can we transport them? If YES, what resources do we need?

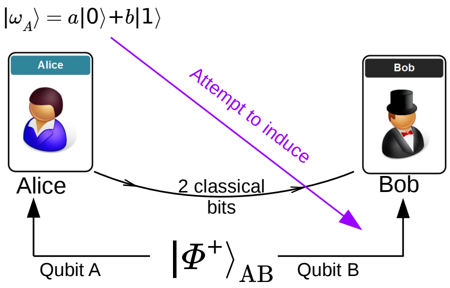


Resource : Shared entangled state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ and 2 classical bits suffice.

The Technique behind Teleportation

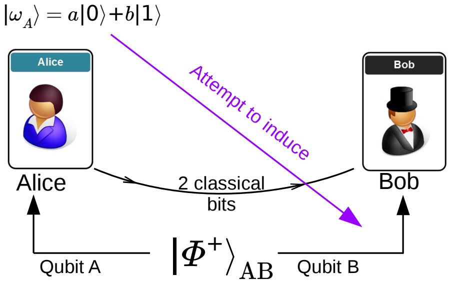


The Technique behind Teleportation



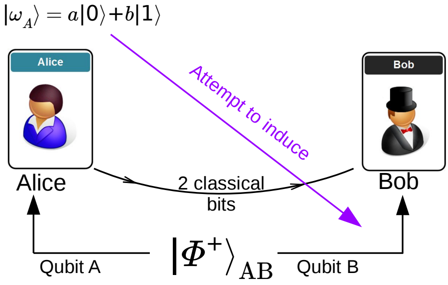
High-Level Technique : 'Induce' $|\omega_A\rangle$ on to Qubit B of $|\Phi^+\rangle_{AB}$.

The Technique behind Teleportation



High-Level Technique : 'Induce' $|\omega_A\rangle$ on to Qubit B of $|\Phi^+\rangle_{AB}$. HOW?

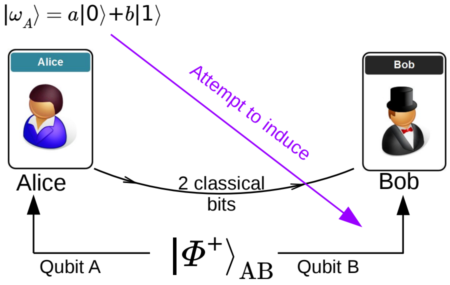
The Technique behind Teleportation



High-Level Technique : 'Induce' $|\omega_A\rangle$ on to Qubit B of $|\Phi^+\rangle_{AB}$. HOW?

Entangled qubits evolve simultaneously.

The Technique behind Teleportation

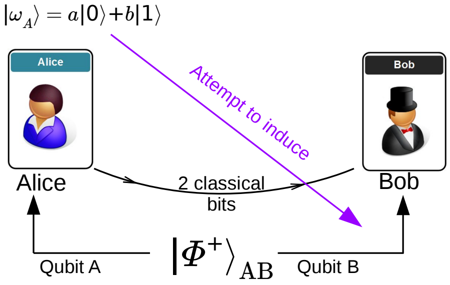


High-Level Technique : 'Induce' $|\omega_A\rangle$ on to Qubit B of $|\Phi^+\rangle_{AB}$. HOW?

Entangled qubits evolve simultaneously.

Alice has $|\omega_A\rangle$ AND first qubit of $|\Phi^+\rangle_{AB}$.

The Technique behind Teleportation



High-Level Technique : 'Induce' $|\omega_A\rangle$ on to Qubit B of $|\Phi^+\rangle_{AB}$. HOW?

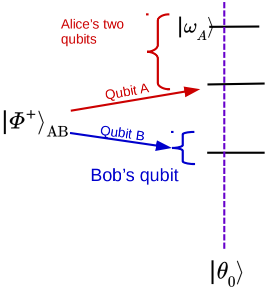
Entangled qubits evolve simultaneously.

Alice has $|\omega_A\rangle$ AND first qubit of $|\Phi^+\rangle_{AB}$.

Step 1 : Entangle $|\Phi^+\rangle_{AB}$ with $|\omega_A\rangle$ by Alice entangling her two qubits.

Step 2 : Alice cleverly evolves her two qubits. Bob's entangled qubit evolves!!!

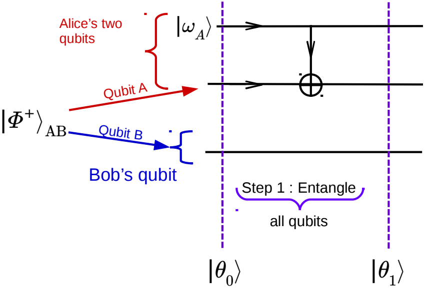
Quantum Teleportation



$$|\theta_0\rangle = |\omega_A\rangle \otimes |\Phi^+\rangle_{AB} = (a\,|0\rangle + b\,|1\rangle) \otimes \frac{1}{\sqrt{2}}\,(|00\rangle + |11\rangle)$$

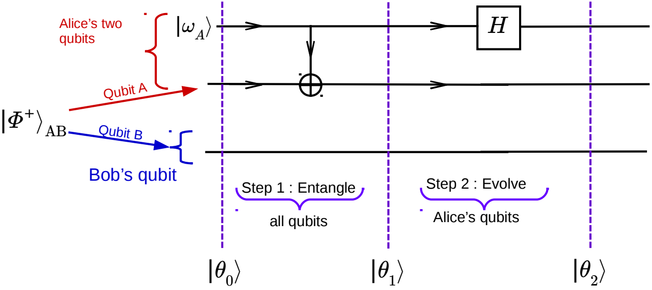
$$|\theta_0\rangle = \frac{1}{\sqrt{2}}\,(a\,|000\rangle + a\,|011\rangle + b\,|100\rangle + b\,|111\rangle)$$

Quantum Teleportation



$$
\begin{aligned}
|\theta_0\rangle &= |\omega_A\rangle \otimes |\Phi^+\rangle_{AB} = (a|0\rangle + b|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
|\theta_0\rangle &= \frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle) \\
|\theta_1\rangle = (\overline{C} \otimes I)(|\theta_0\rangle) &= \frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|110\rangle + b|101\rangle)
\end{aligned}
$$

Quantum Teleportation



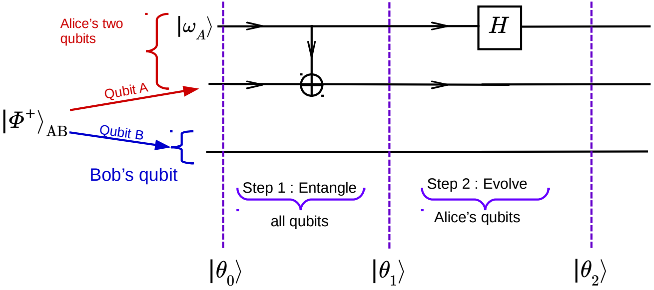
$$|\theta_0\rangle = |\omega_A\rangle \otimes |\Phi^+\rangle_{AB} = (a|0\rangle + b|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|\theta_0\rangle = \frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle)$$

$$|\theta_1\rangle = \frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|110\rangle + b|101\rangle)$$

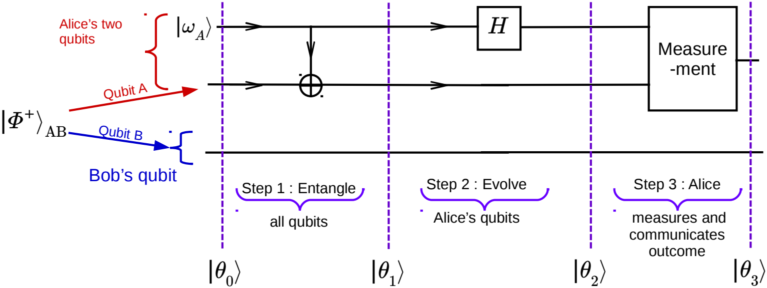
$$|\theta_2\rangle = (H \otimes I \otimes I)(|\theta_1\rangle) =$$

Quantum Teleportation



$$
\begin{aligned}
|\theta_0\rangle &= |\omega_A\rangle \otimes |\Phi^+\rangle_{AB} = (a|0\rangle + b|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
|\theta_0\rangle &= \frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle) \\
|\theta_1\rangle &= \frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|110\rangle + b|101\rangle) \\
|\theta_2\rangle &= |00\rangle \otimes (a|0\rangle + b|1\rangle) + |01\rangle \otimes (a|1\rangle - b|0\rangle) \\
&\quad + |10\rangle \otimes (a|0\rangle - b|1\rangle) + |11\rangle \otimes (a|1\rangle - b|0\rangle)
\end{aligned}
$$

Quantum Teleportation



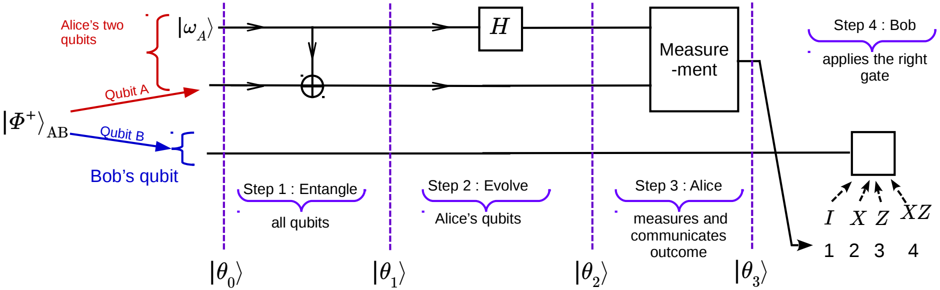
$$|\theta_0\rangle = |\omega_A\rangle \otimes |\Phi^+\rangle_{AB} = (a|0\rangle + b|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|\theta_0\rangle = \frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle)$$

$$|\theta_1\rangle = \frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|110\rangle + b|101\rangle)$$

$$|\theta_2\rangle = |00\rangle \otimes (a|0\rangle + b|1\rangle) + |01\rangle \otimes (a|1\rangle - b|0\rangle) + |10\rangle \otimes (a|0\rangle - b|1\rangle) + |11\rangle \otimes (a|1\rangle - b|0\rangle)$$

Quantum Teleportation



$$|\theta_0\rangle = |\omega_A\rangle \otimes |\Phi^+\rangle_{AB} = (a|0\rangle + b|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|\theta_0\rangle = \frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle)$$

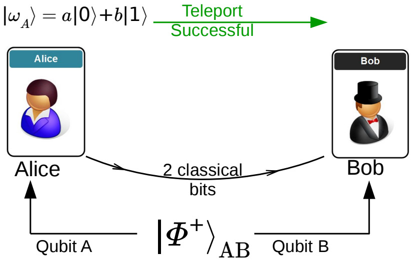
$$|\theta_1\rangle = \frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|110\rangle + b|101\rangle)$$

$$|\theta_2\rangle = |00\rangle \otimes (a|0\rangle + b|1\rangle) + |01\rangle \otimes (a|1\rangle - b|0\rangle)$$
$$+|10\rangle \otimes (a|0\rangle - b|1\rangle) + |11\rangle \otimes (a|1\rangle - b|0\rangle)$$

Super Dense Coding

How many classical bits of information can you pack in one qubit?

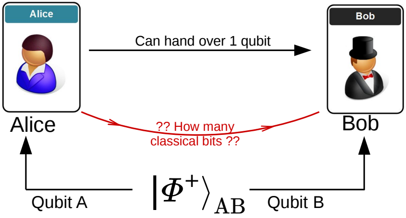
Shared entangled state $|\Phi^+\rangle$ + 2 classical bits = Teleport 1 qubit



Super Dense Coding

How many classical bits of information can you pack in one qubit?

Shared entangled state $|\Phi^+\rangle$ + 2 classical bits $=$ Teleport 1 qubit

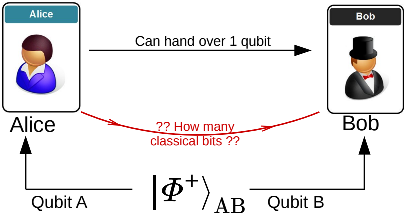


Shared entangled state $|\Phi^+\rangle$ + Hand over 1 qubit $=$?? number of classical bits ??

Super Dense Coding

How many classical bits of information can you pack in one qubit?

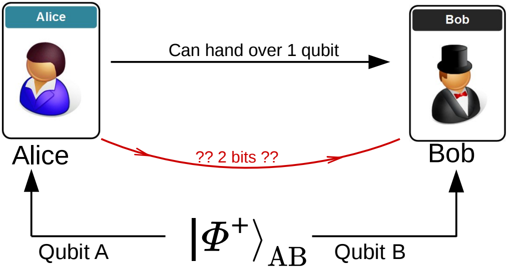
Shared entangled state $|\Phi^+\rangle$ + 2 classical bits $=$ Teleport 1 qubit



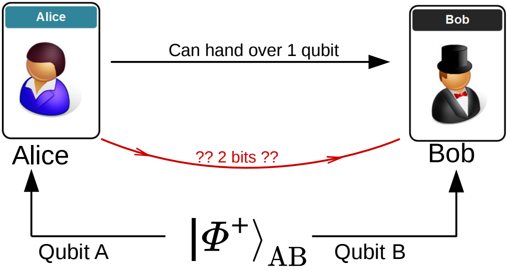
Shared entangled state $|\Phi^+\rangle$ + Hand over 1 qubit $=$!!! Answer is 2 !!!

Super Dense Coding

Super Dense Coding : What is the idea? How do we do it?

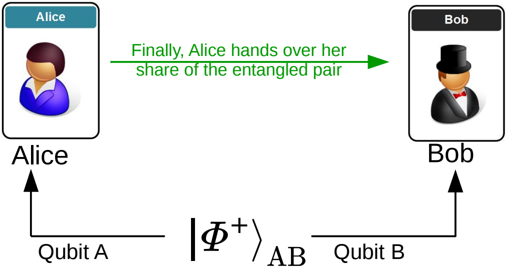


Super Dense Coding : What is the idea? How do we do it?



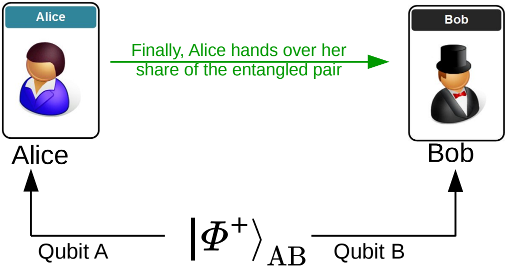
Only qubit Alice has : her share of the entangled pair $|\Phi^+\rangle$.

Super Dense Coding : What is the idea? How do we do it?



Only qubit Alice has : her share of the entangled pair $|\Phi^+\rangle$. She hands it over.

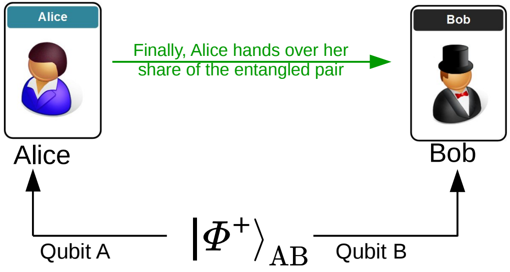
Super Dense Coding : What is the idea? How do we do it?



Only qubit Alice has : her share of the entangled pair $|\Phi^+\rangle$. She hands it over.

At the end, Bob has both qubits.

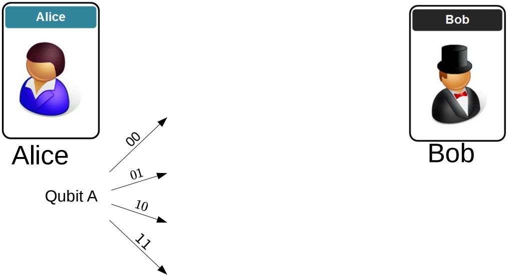
Super Dense Coding : What is the idea? How do we do it?



Only qubit Alice has : her share of the entangled pair $|\Phi^+\rangle$. She hands it over.

At the end, Bob has both qubits. He must read out 2 bits.

Super Dense Coding : What is the idea? How do we do it?

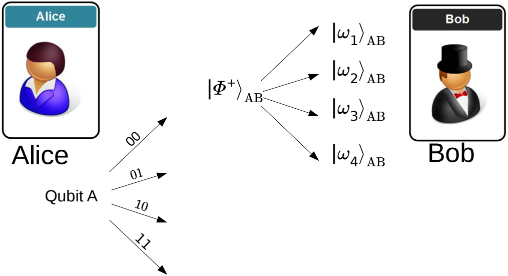


Only qubit Alice has : her share of the entangled pair $|\Phi^+\rangle$. She hands it over.

At the end, Bob has both qubits. He must read out 2 bits.

Based on the two information bits, Alice employs a specific gate on her qubit.

Super Dense Coding : What is the idea? How do we do it?



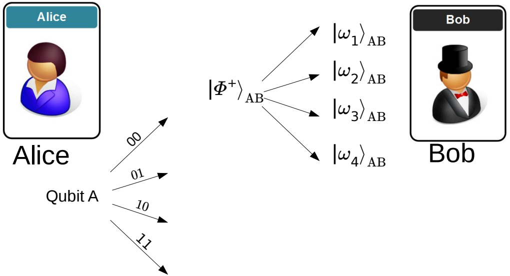
Only qubit Alice has : her share of the entangled pair $|\Phi^+\rangle$. She hands it over.

At the end, Bob has both qubits. He must read out 2 bits.

Based on the two information bits, Alice employs a specific gate on her qubit.

The entangled pair evolves.

Super Dense Coding : What is the idea? How do we do it?



Only qubit Alice has : her share of the entangled pair $|\Phi^+\rangle$. She hands it over.

At the end, Bob has both qubits. He must read out 2 bits.

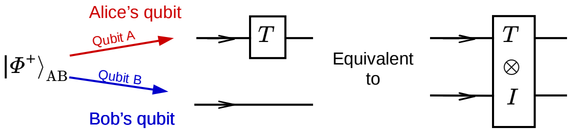
Based on the two information bits, Alice employs a specific gate on her qubit.

The entangled pair evolves.

If $|\omega_1\rangle, |\omega_2\rangle, |\omega_3\rangle, |\omega_4\rangle$ are perfectly distnguishable, Bob can recover the two bits.

Need $|\omega_1\rangle, |\omega_2\rangle, |\omega_3\rangle, |\omega_4\rangle$ mutually orthonormal in $\mathbb{R}^4$.

The Pauli Gates to our rescue



Alice applying gate T is equivalent to transformation $T \otimes I$ on composite system.

Information bits	Gate	Resulting State
00	$I \otimes I$	$\frac{1}{\sqrt{2}}\|00\rangle + \frac{1}{\sqrt{2}}\|11\rangle$
01	$Z \otimes I$	$\frac{1}{\sqrt{2}}\|00\rangle - \frac{1}{\sqrt{2}}\|11\rangle$
10	$X \otimes I$	$\frac{1}{\sqrt{2}}\|01\rangle + \frac{1}{\sqrt{2}}\|10\rangle$
11	$iY \otimes I$	$\frac{1}{\sqrt{2}}\|01\rangle + \frac{1}{\sqrt{2}}\|10\rangle$

On receiving the Qubit A from Alice, Bob performs the measurement

$$\{\Pi_{00} = |00\rangle\langle 00|, \quad \Pi_{01} = |01\rangle\langle 01|, \quad \Pi_{10} = |10\rangle\langle 10|, \quad \Pi_{11} = |11\rangle\langle 11|\}$$

4. Quantum Algorithms

Comparing Classical and Quantum Computational Powers

- Side-Step a formal definition of a Quantum Turing Machine and Quantum complexity clases.
- Single-Qubit Unitary operator $\equiv$ single-input Boolean gate.
- Proxy for run-time $\sim$ No. of quantum gates and No. of unitary operations

BPP : Problem Π is in BPP if $\exists$ a poly-time algo on a probabilistic Classical Turing Machine that returns correct answer with prob. atleast $\frac{3}{4}$.

BQP : Problem Π is in BPP if $\exists$ a poly-time algo on a probabilistic Quantum Turing Machine that returns correct answer with probability atleast $\frac{3}{4}$.

Informal Analysis. Techniques to exploit Superposition.

Power of Quantum Algorithms I : Deutsch Josza algorithm

Is an $n-$bit Boolean function $f : \{0,1\}^n \to \{0,1\}$ constant or balanced ?

Power of Quantum Algorithms I : Deutsch Josza algorithm

Is an $n-$bit Boolean function $f:\{0,1\}^n \to \{0,1\}$ constant or balanced ?

Category 1	
$f(x^n)$ is constant i.e., either $f = 0$ or $f = 1$.	

Power of Quantum Algorithms I : Deutsch Josza algorithm

Is an $n-$bit Boolean function $f : \{0,1\}^n \to \{0,1\}$ constant or balanced ?

Category 1	Category 2
$f(x^n)$ is constant i.e., either $f = 0$ or $f = 1$.	$f(x^n) = 0$ for half the inputs and $f(x^n) = 1$ for the rest half of the inputs. $\lvert\{x^n : f(x^n) = 1\}\rvert = \lvert\{x^n : f(x^n) = 1\}\rvert = 2^{n-1}$

Power of Quantum Algorithms I : Deutsch Josza algorithm

Is an $n-$bit Boolean function $f : \{0,1\}^n \to \{0,1\}$ constant or balanced ?

Category 1	Category 2
$f(x^n)$ is constant i.e., either $f = 0$ or $f = 1$.	$f(x^n) = 0$ for half the inputs and $f(x^n) = 1$ for the rest half of the inputs. $\lvert\{x^n : f(x^n) = 1\}\rvert = \lvert\{x^n : f(x^n) = 1\}\rvert = 2^{n-1}$

Task : Given f, determine whether it is in Category 1 or Category 2.

Power of Quantum Algorithms I : Deutsch Josza algorithm

Is an $n-$bit Boolean function $f : \{0,1\}^n \to \{0,1\}$ constant or balanced ?

Category 1	Category 2
$f(x^n)$ is constant i.e., either $f = 0$ or $f = 1$.	$f(x^n) = 0$ for half the inputs and $f(x^n) = 1$ for the rest half of the inputs. $\lvert\{x^n : f(x^n) = 1\}\rvert = \lvert\{x^n : f(x^n) = 1\}\rvert = 2^{n-1}$

Task : Given f, determine whether it is in Category 1 or Category 2.

We have an oracle who, given x^n, will compute $f(x^n)$.

One usage : Binary oracle will provide us $f(x^n)$.

One usage : Quantum oracle will provide us $|f(x^n)\rangle$.

How many times should we poll our oracles?

Known algorithms on Classical Computers

Worst Case Analysis with guaranteed correctness

Must poll $\geq 2^{n-1} + 1$ sequences in $\{0, 1\}^n$

Known algorithms on Classical Computers

Worst Case Analysis with guaranteed correctness

Must poll $\geq 2^{n-1} + 1$ sequences in $\{0, 1\}^n$

Performance of Probabilistic (Randomized) Algorithms

Algorithm : Pick k boolean inputs uniformly and randomly.

Poll $f-$values for chosen random inputs.

If all $f-$values for chosen random inputs are same, declare f is constant, (Category 1).

Otherwise, declare f is balanced, i.e., Category 2.

Performance : If you declare f is balanced, f is definitely balanced.

$\Rightarrow P(f \text{ is constant} \mid \text{you declare balanced}) = 0.$

$$P(f \text{ is balanced} \mid \text{you declare constant}) = \frac{2^{-k} P(f \text{ is balanced })}{1 - P(f \text{ is balanced })} \overset{k \to \infty}{\to} 0.$$

Problem in BPP.

$2^{n-1} + 1$ computations for certain answer.

Deustch Jozsa discovered an efficient quantum algorithm

What is the idea?

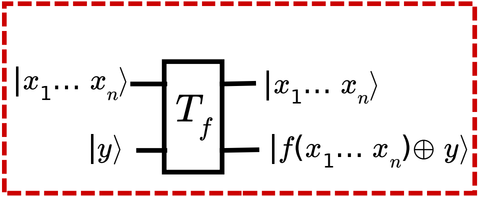
Prepare a $(n+1)-$ qubit state $|\phi\rangle$ based on the function f such that is

(a) if f is constant state $|\phi\rangle$ lies in subspace W and

(b) if f is balanced, then $|\phi\rangle$ lies in subspace $W^{\perp}$.

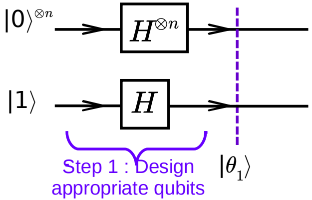
(c) Preparation of $|\phi\rangle$ has low quantum complexity.

Our Quantum Oracle



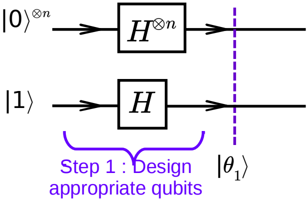
How many times will we need poll this quantum oracle?

Deutsch Jozsa Algorithm



$$|\theta_1\rangle = H^{\otimes(n+1)}|0\rangle^{\otimes n}|1\rangle = H^{\otimes n}(|0\rangle^{\otimes n}) \otimes H(|1\rangle)$$

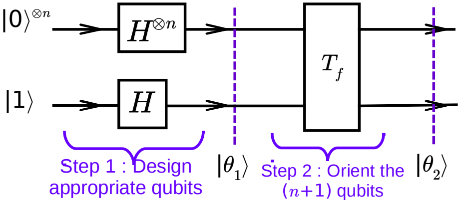
Deutsch Jozsa Algorithm

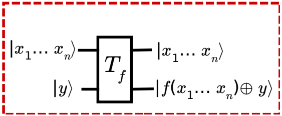


$$|\theta_1\rangle = H^{\otimes(n+1)}\,|0\rangle^{\otimes n}\,|1\rangle = H^{\otimes n}(|0\rangle^{\otimes n}) \otimes H(|1\rangle)$$ Ignoring $\frac{1}{\sqrt{2}}$ factors

$$= \sum_{b^n \in \{0,1\}^n} |b_1 \cdots b_n\ 0\rangle \quad - \sum_{b^n \in \{0,1\}^n} |b_1 \cdots b_n\ 1\rangle$$

Deutsch Jozsa Algorithm





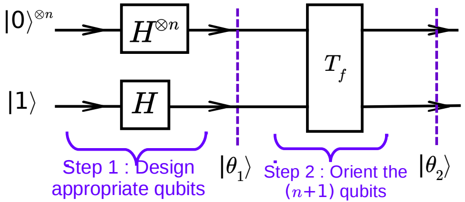
$$|\theta_1\rangle = H^{\otimes(n+1)}|0\rangle^{\otimes n}|1\rangle = H^{\otimes n}(|0\rangle^{\otimes n}) \otimes H(|1\rangle) \quad \text{Ignoring } \frac{1}{\sqrt{2}} \text{ factors}$$

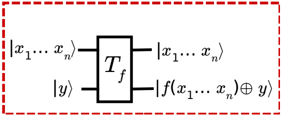
$$= \sum_{b^n \in \{0,1\}^n} |b_1 \cdots b_n\ 0\rangle - \sum_{b^n \in \{0,1\}^n} |b_1 \cdots b_n\ 1\rangle$$

$$|\theta_2\rangle = \sum_{b^n \in \{0,1\}^n} |b_1 \cdots b_n\ f(b_1 \cdots b_n)\rangle - \sum_{b^n \in \{0,1\}^n} |b_1 \cdots b_n\ 1 \oplus f(b_1 \cdots b_n)\rangle$$

Suppose f were a constant $f(b^n) = 0$ for all b^n

Deutsch Jozsa Algorithm





$$|\theta_1\rangle = H^{\otimes(n+1)}|0\rangle^{\otimes n}|1\rangle = H^{\otimes n}(|0\rangle^{\otimes n}) \otimes H(|1\rangle) \quad \text{Ignoring } \tfrac{1}{\sqrt{2}} \text{ factors}$$

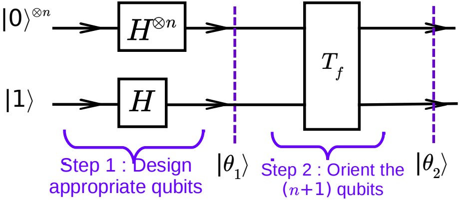
$$= \sum_{b^n \in \{0,1\}^n} |b_1 \cdots b_n \; 0\rangle \; - \sum_{b^n \in \{0,1\}^n} |b_1 \cdots b_n \; 1\rangle$$

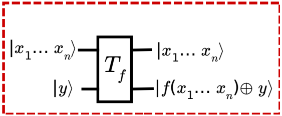
$$|\theta_2\rangle = \sum_{b^n \in \{0,1\}^n} |b_1 \cdots b_n \; f(b_1 \cdots b_n)\rangle - \sum_{b^n \in \{0,1\}^n} |b_1 \cdots b_n \; 1 \oplus f(b_1 \cdots b_n)\rangle$$

Suppose f were a constant $f(b^n) = 0$ for all b^n

$$|\theta_2\rangle = \sum_{b^n \in \{0,1\}^n} |b_1 \cdots b_n \; 0\rangle - \sum_{b^n \in \{0,1\}^n} |b_1 \cdots b_n \; 1\rangle$$

Deutsch Jozsa Algorithm





$$|\theta_1\rangle = H^{\otimes(n+1)}\,|0\rangle^{\otimes n}\,|1\rangle = H^{\otimes n}(|0\rangle^{\otimes n}) \otimes H(|1\rangle) \quad \text{Ignoring } \tfrac{1}{\sqrt{2}} \text{ factors}$$

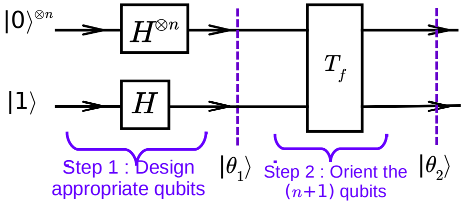
$$= \sum_{b^n \in \{0,1\}^n} |b_1 \cdots b_n\ 0\rangle - \sum_{b^n \in \{0,1\}^n} |b_1 \cdots b_n\ 1\rangle$$

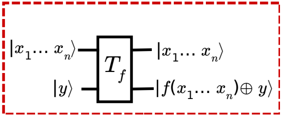
$$|\theta_2\rangle = \sum_{b^n \in \{0,1\}^n} |b_1 \cdots b_n\ f(b_1 \cdots b_n)\rangle - \sum_{b^n \in \{0,1\}^n} |b_1 \cdots b_n\ 1 \oplus f(b_1 \cdots b_n)\rangle$$

Suppose f were a constant $f(b^n) = 1$ for all b^n

$$|\theta_2\rangle = \sum_{b^n \in \{0,1\}^n} |b_1 \cdots b_n\ 1\rangle - \sum_{b^n \in \{0,1\}^n} |b_1 \cdots b_n\ 0\rangle$$

Deutsch Jozsa Algorithm





$$|\theta_1\rangle = H^{\otimes(n+1)}\,|0\rangle^{\otimes n}\,|1\rangle = H^{\otimes n}(|0\rangle^{\otimes n}) \otimes H(|1\rangle)$$ Ignoring $\frac{1}{\sqrt{2}}$ factors

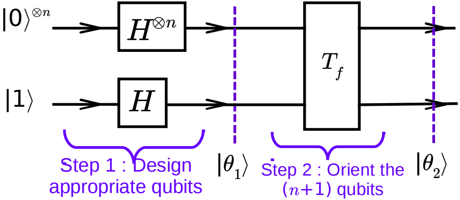
$$= \sum_{b^n \in \{0,1\}^n} |b_1 \cdots b_n\ 0\rangle \quad - \sum_{b^n \in \{0,1\}^n} |b_1 \cdots b_n\ 1\rangle$$

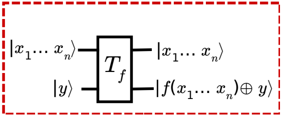
$$|\theta_2\rangle = \sum_{b^n \in \{0,1\}^n} |b_1 \cdots b_n\ f(b_1 \cdots b_n)\rangle - \sum_{b^n \in \{0,1\}^n} |b_1 \cdots b_n\ 1 \oplus f(b_1 \cdots b_n)\rangle$$

Suppose f were a constant

$$|\theta_2\rangle_{\text{cnst}} \quad = \quad \pm \sum_{b^n \in \{0,1\}^n} |b_1 \cdots b_n\rangle \otimes (|0\rangle - |1\rangle)$$

Deutsch Jozsa Algorithm





$$|\theta_1\rangle = H^{\otimes(n+1)}|0\rangle^{\otimes n}|1\rangle = H^{\otimes n}(|0\rangle^{\otimes n}) \otimes H(|1\rangle) \quad \text{Ignoring } \tfrac{1}{\sqrt{2}} \text{ factors}$$

$$= \sum_{b^n \in \{0,1\}^n} |b_1 \cdots b_n \; 0\rangle \quad - \sum_{b^n \in \{0,1\}^n} |b_1 \cdots b_n \; 1\rangle$$

$$|\theta_2\rangle = \sum_{b^n \in \{0,1\}^n} |b_1 \cdots b_n \; f(b_1 \cdots b_n)\rangle - \sum_{b^n \in \{0,1\}^n} |b_1 \cdots b_n \; 1 \oplus f(b_1 \cdots b_n)\rangle$$

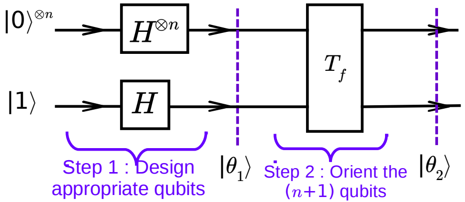
Suppose f were a constant

$$|\theta_2\rangle_{\text{cnst}} = \pm \sum_{b^n \in \{0,1\}^n} |b_1 \cdots b_n\rangle \otimes (|0\rangle - |1\rangle)$$

Suppose f were a balanced

$$|\theta_2\rangle_{\text{blncd}} = \sum_{b^n : f(b^n)=0} |b_1 \cdots b_n\rangle \otimes (|0\rangle - |1\rangle) \quad - \sum_{b^n : f(b^n)=1} |b_1 \cdots b_n\rangle \otimes (|0\rangle - |1\rangle)$$

Deutsch Jozsa Algorithm



$|\theta_2\rangle_{\text{cnst}}$ and $|\theta_2\rangle_{\text{blncd}}$ are orthogonal!!!

$$|\theta_1\rangle = H^{\otimes(n+1)}\,|0\rangle^{\otimes n}\,|1\rangle = H^{\otimes n}(|0\rangle^{\otimes n}) \otimes H(|1\rangle)$$ Ignoring $\frac{1}{\sqrt{2}}$ factors

$$= \sum_{b^n\in\{0,1\}^n} |b_1 \cdots b_n\ 0\rangle \quad - \sum_{b^n\in\{0,1\}^n} |b_1 \cdots b_n\ 1\rangle$$

$$|\theta_2\rangle = \sum_{b^n\in\{0,1\}^n} |b_1 \cdots b_n\ f(b_1 \cdots b_n)\rangle - \sum_{b^n\in\{0,1\}^n} |b_1 \cdots b_n\ 1 \oplus f(b_1 \cdots b_n)\rangle$$

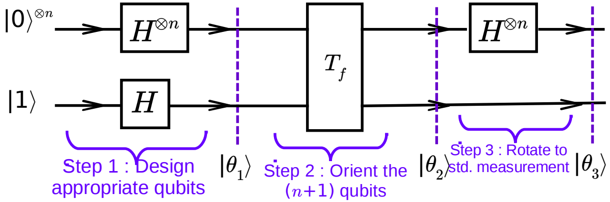
Suppose f were a constant

$$|\theta_2\rangle_{\text{cnst}} \quad = \quad \pm \sum_{b^n\in\{0,1\}^n} |b_1 \cdots b_n\rangle \otimes (|0\rangle - |1\rangle)$$

Suppose f were a balanced

$$|\theta_2\rangle_{\text{blncd}} \quad = \sum_{b^n:f(b^n)=0} |b_1 \cdots b_n\rangle \otimes (|0\rangle - |1\rangle) \quad - \sum_{b^n:f(b^n)=1} |b_1 \cdots b_n\rangle \otimes (|0\rangle - |1\rangle)$$

Deutsch Jozsa Algorithm



$$|\theta_1\rangle = H^{\otimes(n+1)}\,|0\rangle^{\otimes n}\,|1\rangle = H^{\otimes n}(|0\rangle^{\otimes n}) \otimes H(|1\rangle)$$ Ignoring $\frac{1}{\sqrt{2}}$ factors

$$= \sum_{b^n\in\{0,1\}^n} |b_1\cdots b_n\ 0\rangle \quad - \sum_{b^n\in\{0,1\}^n} |b_1\cdots b_n\ 1\rangle$$

$$|\theta_2\rangle = \sum_{b^n\in\{0,1\}^n} |b_1\cdots b_n\ f(b_1\cdots b_n)\rangle - \sum_{b^n\in\{0,1\}^n} |b_1\cdots b_n\ 1\oplus f(b_1\cdots b_n)\rangle$$

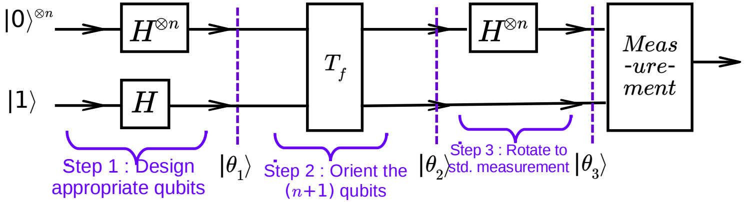
Suppose f were a constant

$$|\theta_2\rangle_{\text{cnst}} \quad = \quad \pm \sum_{b^n\in\{0,1\}^n} |b_1\cdots b_n\rangle \otimes (|0\rangle - |1\rangle)$$

Suppose f were a balanced

$$|\theta_2\rangle_{\text{blncd}} \quad = \sum_{b^n:f(b^n)=0} |b_1\cdots b_n\rangle \otimes (|0\rangle - |1\rangle) \quad - \sum_{b^n:f(b^n)=1} |b_1\cdots b_n\rangle \otimes (|0\rangle - |1\rangle)$$

Deutsch Jozsa Algorithm



$$|\theta_1\rangle = H^{\otimes(n+1)}\,|0\rangle^{\otimes n}\,|1\rangle = H^{\otimes n}(|0\rangle^{\otimes n}) \otimes H(|1\rangle)$$ Ignoring $\frac{1}{\sqrt{2}}$ factors

$$= \sum_{b^n \in \{0,1\}^n} |b_1 \cdots b_n\ 0\rangle \quad - \sum_{b^n \in \{0,1\}^n} |b_1 \cdots b_n\ 1\rangle$$

$$|\theta_2\rangle = \sum_{b^n \in \{0,1\}^n} |b_1 \cdots b_n\ f(b_1 \cdots b_n)\rangle - \sum_{b^n \in \{0,1\}^n} |b_1 \cdots b_n\ 1 \oplus f(b_1 \cdots b_n)\rangle$$

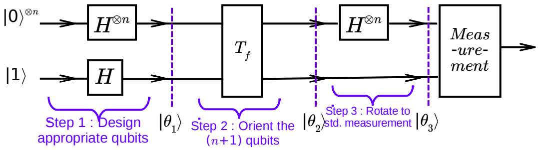
Suppose f were a constant

$$|\theta_2\rangle_{\text{cnst}} \quad = \quad \pm \sum_{b^n \in \{0,1\}^n} |b_1 \cdots b_n\rangle \otimes (|0\rangle - |1\rangle)$$

Suppose f were a balanced

$$|\theta_2\rangle_{\text{blncd}} \quad = \sum_{b^n : f(b^n)=0} |b_1 \cdots b_n\rangle \otimes (|0\rangle - |1\rangle) \quad - \sum_{b^n : f(b^n)=1} |b_1 \cdots b_n\rangle \otimes (|0\rangle - |1\rangle)$$

Analyzing Quantum Complexity

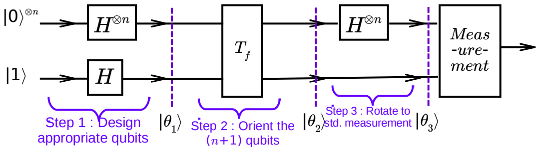


Quantum Algorithm

Computes Correct Answer with CERTAINTY.

No. of Unitary Operations $= O(n)$!!!

Analyzing Quantum Complexity



Quantum Algorithm

Computes Correct Answer with CERTAINTY.

No. of Unitary Operations $= O(n)$!!!

Classical Computer

$2^{n-1} + 1$ computations for certain answer.

Problem in BPP.

Problem in BPP $\cap$ BQP. No insights on BQP $\setminus$ BPP.

Finding the Unknown Period in $(\mathbb{Z}_2)^n$

$f : \{0,1\}^n \to \{0,1\}^n$ is $2-to-1$ and periodic with unknown period $(a_1, \cdots, a_n)$.

Exactly two n–bit sequences yield same output and $f(x_1, \cdots, x_n) = f(x_1 \oplus a_1, \cdots, x_n \oplus a_n)$.

On how many n–bit inputs must you poll $f(\cdot)$–values to figure out period $(a_1, \cdots, a_n)$?

Classically, if you poll for $2^{\alpha n}$ n–bit sequences, you have $f(\cdot)$–values for at most $\binom{2^{\alpha n}}{2} \leq 2^{2\alpha n}$ input pairs.

$$P(\text{Finding } a^n) = \frac{2^{2\alpha n}}{2^n} = 2^{-n(1-2\alpha)} \overset{n\to\infty}{\to} 0 \quad \text{if } \alpha < \frac{1}{2}$$

Need to poll $f(\cdot)$–values for $2^{\frac{n}{2}}$ inputs to obtain reasonable success.

Recall Property 2 of the Hadamard Gate

For $x \in \{0,1\}$ or $x^n \in \{0,1\}^n$

$$|x\rangle \overset{H}{\mapsto} \sum_{z=0}^{1} (-1)^{x \cdot z} |z\rangle$$

$$|x_1 \cdots x_n\rangle \overset{H^{\otimes n}}{\mapsto} \sum_{z^n \in \{0,1\}^n} (-1)^{x_1 \cdot z_1 + \cdots + \cdots x_n z_n} |z_1 \cdots z_n\rangle = \sum_{z^n \in \{0,1\}^n} (-1)^{\underline{x} \cdot \underline{z}} |z_1 \cdots z_n\rangle$$

Exploring the Versatility of the The Hadamard Gate

Problem : Prepared State :

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|x_1 \cdots x_n \; b_1 \cdots b_n\rangle + |(x_1 \oplus a_1) \cdots (x_n \oplus a_n) \; b_1 \cdots b_n\rangle)$$

$x_1, \cdots, x_n, a_1, \cdots, a_n$ unknown. Find $a_1, \cdots, a_n$. !!! Cannot eye-ball A State!!!

Exploring the Versatility of the The Hadamard Gate

Problem : Prepared State : $x_1 \oplus a_1 = y_1, \cdots, x_n \oplus a_n = y_n$

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|x_1 \ \cdots \ x_n \ b_1 \ \cdots \ b_n\rangle + |y_1 \ \cdots \ y_n \ b_1 \ \cdots \ b_n\rangle$$

$x_1, \cdots, x_n, a_1, \cdots, a_n$ unknown. Find $a_1, \cdots, a_n$. !!! Cannot eye-ball A State!!!

Exploring the Versatility of the The Hadamard Gate

Problem : Prepared State : $x_1 \oplus a_1 = y_1, \cdots, x_n \oplus a_n = y_n$

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|x_1 \cdots x_n \; b_1 \cdots b_n\rangle + |y_1 \cdots y_n \; b_1 \cdots b_n\rangle$$

$x_1, \cdots, x_n, a_1, \cdots, a_n$ unknown. Find $a_1, \cdots, a_n$.

Step 1: Apply $H^{\otimes n} \otimes I_2^{\otimes n}$

$$\begin{aligned} |\phi\rangle \mapsto & \sum_{z_1, \cdots, z_n \in \{0,1\}^n} \left[\; (-1)^{\underline{x} \cdot \underline{z}} + (-1)^{\underline{x} \cdot \underline{z} \oplus \underline{a} \cdot \underline{z}} \; \right] |z_1 \cdots z_n \; b_1 \cdots b_n\rangle \\ = & \sum_{\substack{z_1, \cdots, z_n : \\ a_1 z_1 \oplus \cdots \oplus a_n z_n = 0}} |z_1 \cdots z_n \; b_1 \cdots b_n\rangle \end{aligned}$$

Exploring the Versatility of the The Hadamard Gate

Problem : Prepared State : $x_1 \oplus a_1 = y_1, \cdots, x_n \oplus a_n = y_n$

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|x_1 \cdots x_n \; b_1 \cdots b_n\rangle + |y_1 \cdots y_n \; b_1 \cdots b_n\rangle$$

$x_1, \cdots, x_n, a_1, \cdots, a_n$ unknown. Find $a_1, \cdots, a_n$.

Step 1: Apply $H^{\otimes n} \otimes I_2^{\otimes n}$

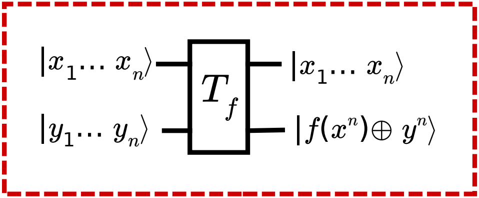
$$\begin{aligned} |\phi\rangle &\mapsto \sum_{z_1,\cdots,z_n \in \{0,1\}^n} \left[\; (-1)^{\underline{x}\cdot\underline{z}} + (-1)^{\underline{x}\cdot\underline{z} \oplus \underline{a}\cdot\underline{z}} \; \right] |z_1 \cdots z_n \; b_1 \cdots b_n\rangle \\ &= \sum_{\substack{z_1,\cdots,z_n: \\ a_1 z_1 \oplus \cdots \oplus a_n z_n = 0}} |z_1 \cdots z_n \; b_1 \cdots b_n\rangle \end{aligned}$$

For any $(a_1, \cdots, a_n)$ there are 2^{n-1} terms in above sum.

Step 2: Apply Measurement : $\{|0\cdots 0\rangle\langle 0\cdots 0| \otimes I, \cdots, |1\cdots 1\rangle\langle 1\cdots 1| \otimes I\}$.

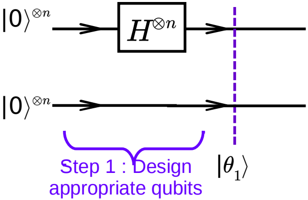
Outcome provides one choice of $z_1, z_2, \cdots, z_n$ for which $a_1 z_1 \oplus \cdots \oplus a_n z_n = 0$.

Quantum Oracle for our period finding function



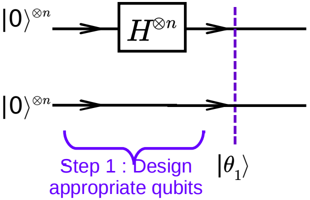
$$|x_1 \cdots x_n \; y_1 \cdots y_n\rangle \overset{T_f}{\mapsto} |x_1 \cdots x_n \; f(x^n) \oplus (y_1 \cdots y_n)\rangle$$

Simon's circuit for period finding



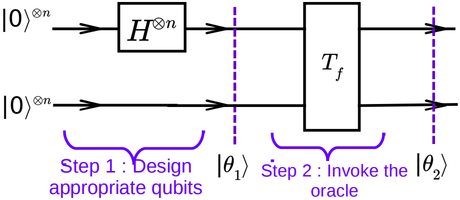
$$|\theta_1\rangle = H^{\otimes(n)}\,|0\rangle^{\otimes n} \otimes I\,|0\rangle^{\otimes n}$$

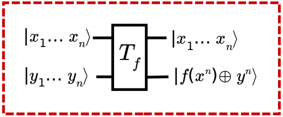
Simon's circuit for period finding



$$
\begin{aligned}
|\theta_1\rangle &= H^{\otimes(n)} |0\rangle^{\otimes n} \otimes I\, |0\rangle^{\otimes n} \quad \text{Ignoring } \tfrac{1}{\sqrt{2}} \text{ factors} \\
&= \sum_{x^n \in \{0,1\}^n} |x_1 \cdots x_n \; 0 \cdots 0\rangle
\end{aligned}
$$

Simon's circuit for period finding



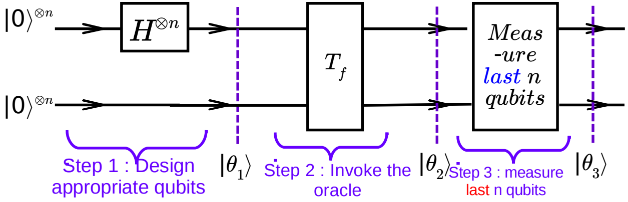


$$|\theta_1\rangle = H^{\otimes(n)} |0\rangle^{\otimes n} \otimes I |0\rangle^{\otimes n}$$ Ignoring $\frac{1}{\sqrt{2}}$ factors

$$= \sum_{x^n \in \{0,1\}^n} |x_1 \cdots x_n \; 0 \cdots 0\rangle$$

$$|\theta_2\rangle = \sum_{x^n \in \{0,1\}^n} |x_1 \cdots x_n \; f(x_1 \cdots x_n)\rangle$$

Simon's circuit for period finding



$$|\theta_1\rangle = H^{\otimes(n)}\,|0\rangle^{\otimes n} \otimes I\,|0\rangle^{\otimes n} \quad \text{Ignoring } \frac{1}{\sqrt{2}} \text{ factors}$$

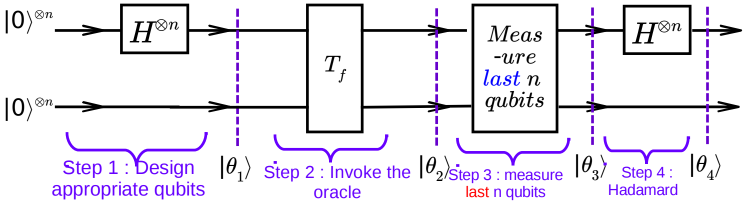
$$= \sum_{x^n \in \{0,1\}^n} |x_1 \cdots x_n\ 0 \cdots 0\rangle$$

$$|\theta_2\rangle = \sum_{x^n \in \{0,1\}^n} |x_1 \cdots x_n\ f(x_1 \cdots x_n)\rangle$$

Suppose outcome of the measurement were $b_1, \cdots, b_n$

$$|\theta_3\rangle = \frac{1}{\sqrt{2}}\left(|x_1\ \cdots\ x_n\ b_1\ \cdots\ b_n\rangle + |(x_1 \oplus a_1)\ \cdots\ (x_n \oplus a_n)\ b_1\ \cdots\ b_n\rangle\right)$$

Simon's circuit for period finding



$$|\theta_1\rangle = H^{\otimes(n)}\,|0\rangle^{\otimes n} \otimes I\,|0\rangle^{\otimes n}$$ Ignoring $\frac{1}{\sqrt{2}}$ factors

$$= \sum_{x^n \in \{0,1\}^n} |x_1 \cdots x_n \; 0 \cdots 0\rangle$$

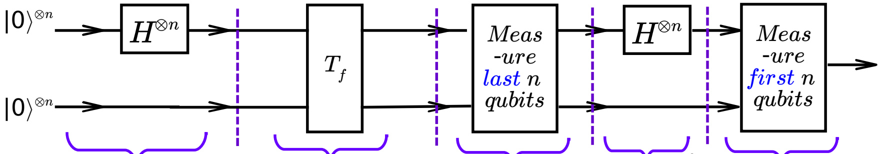
$$|\theta_2\rangle = \sum_{x^n \in \{0,1\}^n} |x_1 \cdots x_n \; f(x_1 \cdots x_n)\rangle$$

Suppose outcome of the measurement were $b_1, \cdots, b_n$

$$|\theta_3\rangle = \frac{1}{\sqrt{2}}(|x_1 \cdots x_n \; b_1 \cdots b_n\rangle + |(x_1 \oplus a_1) \cdots (x_n \oplus a_n) \; b_1 \cdots b_n\rangle)$$

$$|\theta_4\rangle = \sum_{\substack{z_1, \cdots, z_n: \\ a_1 z_1 \oplus \cdots \oplus a_n z_n = 0}} |z_1 \cdots z_n \; b_1 \cdots b_n\rangle$$

Simon's circuit for period finding



$$|\theta_1\rangle = H^{\otimes(n)}\,|0\rangle^{\otimes n} \otimes I\,|0\rangle^{\otimes n} \quad \text{Ignoring } \tfrac{1}{\sqrt{2}} \text{ factors}$$

$$= \sum_{x^n \in \{0,1\}^n} |x_1 \cdots x_n\ 0 \cdots 0\rangle$$

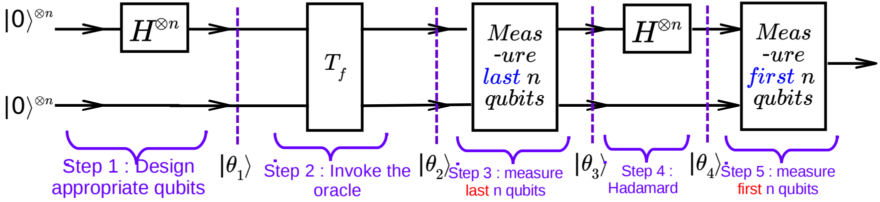
$$|\theta_2\rangle = \sum_{x^n \in \{0,1\}^n} |x_1 \cdots x_n\ f(x_1 \cdots x_n)\rangle$$

Suppose outcome of the measurement were $b_1, \cdots, b_n$

$$|\theta_3\rangle = \frac{1}{\sqrt{2}}\left(|x_1 \cdots x_n\ b_1 \cdots b_n\rangle + |(x_1 \oplus a_1) \cdots (x_n \oplus a_n)\ b_1 \cdots b_n\rangle\right)$$

$$|\theta_4\rangle = \sum_{\substack{z_1,\cdots,z_n:\\ a_1 z_1 \oplus \cdots \oplus a_n z_n = 0}} |z_1 \cdots z_n\ b_1 \cdots b_n\rangle$$

Simon's circuit for period finding



Suppose outcome of the measurement were $b_1, \cdots, b_n$

$$|\theta_4\rangle = \sum_{\substack{z_1,\cdots,z_n: \\ a_1 z_1 \oplus \cdots \oplus a_n z_n = 0}} |z_1 \,\cdots\, z_n \; b_1 \,\cdots\, b_n\rangle$$

Measure the first n registers with measurement operators $\{|0\cdots00\rangle\langle 0\cdots00| \otimes I_2^{\otimes n}, |0\cdots01\rangle\langle 0\cdots01| \otimes I_2^{\otimes n}, |1\cdots11\rangle\langle 1\cdots11| \otimes I_2^{\otimes n}\}$

Every outcome gives you one linear equation $o_1 a_1 \oplus \cdots \oplus o_n a_n = 0$ where $(o_1, \cdots, o_n)$ is your outcome.

Need n linear independent eqns to solve for $a_1, \cdots, a_n$. Repeat whole apparatus k times.

Analysis of Simon's period finding algorithm

Factoring a composite integer

Every composite integer is a product of powers of primes.

Example
$66 = 2 \cdot 3 \cdot 11$

Example
$275 = 5 \cdot 5 \cdot 11$

Example
$277 = ??$

Given $n-$bit integer N, find primes $p_1, \cdots, p_m$ and integers $q_1, \cdots, q_m$ s.t

$$N = p_1^{q_1} \cdots p_m^{q_m}.$$

Given $n-$bit integer N, need a quantum algorithm that identifies prime factors in run-time n^k for some k.

Towards Shor's Algorithm for Prime Factorization

Goal : Design a polynomial-time quantum algorithm that can identify the prime factors of a $n-$bit composite number N.

Break the task down.

Efficiently identify non-trivial factor of N.

Find α such that $\alpha | N$ and $\alpha \neq 1$ and $\alpha \neq N$.

		No. Factors	No. Computations
$N =$	$\alpha_1 \cdot \alpha_2$		

Towards Shor's Algorithm for Prime Factorization

Goal : Design a polynomial-time quantum algorithm that can identify the prime factors of a $n-$bit composite number N.

Break the task down.

Efficiently identify non-trivial factor of N.

Find α such that $\alpha|N$ and $\alpha \neq 1$ and $\alpha \neq N$.

No. Factors No. Computations

$$
\begin{aligned}
N &= \alpha_1 \cdot \alpha_2 \\
&= \alpha_{11} \cdot \alpha_{12} \cdot \alpha_{21} \cdot \alpha_{22} \\
&= \alpha_{111}\alpha_{112}\alpha_{121}\alpha_{122}\cdots\alpha_{211}\alpha_{212}\alpha_{221}\alpha_{222}
\end{aligned}
$$

Towards Shor's Algorithm for Prime Factorization

Goal : Design a polynomial-time quantum algorithm that can identify the prime factors of a $n-$bit composite number N.

Break the task down.

Efficiently identify non-trivial factor of N.

Find α such that $\alpha|N$ and $\alpha \neq 1$ and $\alpha \neq N$.

No. Factors   No. Computations

$$\begin{aligned}
N &= \alpha_1 \cdot \alpha_2 \\
&= \alpha_{11} \cdot \alpha_{12} \cdot \alpha_{21} \cdot \alpha_{22} \\
&= \alpha_{111}\alpha_{112}\alpha_{121}\alpha_{122} \cdots \alpha_{211}\alpha_{212}\alpha_{221}\alpha_{222} \\
&= \vdots
\end{aligned}$$

Towards Shor's Algorithm for Prime Factorization

Goal : Design a polynomial-time quantum algorithm that can identify the prime factors of a $n-$bit composite number N.

Break the task down.

Efficiently identify non-trivial factor of N.

Find α such that $\alpha|N$ and $\alpha \neq 1$ and $\alpha \neq N$.

No. Factors   No. Computations

$$
\begin{aligned}
N &= \alpha_1 \cdot \alpha_2 \\
&= \alpha_{11} \cdot \alpha_{12} \cdot \alpha_{21} \cdot \alpha_{22} \\
&= \alpha_{111}\alpha_{112}\alpha_{121}\alpha_{122} \cdots \alpha_{211}\alpha_{212}\alpha_{221}\alpha_{222} \\
&= \vdots \\
&= p_1^{q_1} \cdot p_2^{q_2} \cdot \cdot p_{m-1}^{q_{m-1}} \cdot p_m^{q_m}
\end{aligned}
$$

Towards Shor's Algorithm for Prime Factorization

Goal : Design a polynomial-time quantum algorithm that can identify the prime factors of a $n-$bit composite number N.

Break the task down.

Efficiently identify non-trivial factor of N.

Find α such that $\alpha | N$ and $\alpha \neq 1$ and $\alpha \neq N$.

			No. Factors	No. Computations
N	$=$	$\alpha_1 \cdot \alpha_2$	2	n^k
	$=$	$\alpha_{11} \cdot \alpha_{12} \cdot \alpha_{21} \cdot \alpha_{22}$	4	$2(n-1)^k$
	$=$	$\alpha_{111}\alpha_{112}\alpha_{121}\alpha_{122} \cdots \alpha_{211}\alpha_{212}\alpha_{221}\alpha_{222}$	8	$4(n-2)^k$
	$=$	$\vdots$	$\cdots$	$\vdots$
	$=$	$p_1^{q_1} \cdot p_2^{q_2} \cdot \cdot p_{m-1}^{q_{m-1}} \cdot p_m^{q_m}$	2^l	$2^{l-1}(n-l)^k$

Towards Shor's Algorithm for Prime Factorization

Goal : Design a polynomial-time quantum algorithm that can identify the prime factors of a $n-$bit composite number N.

Break the task down.

Efficiently identify non-trivial factor of N.

Find α such that $\alpha|N$ and $\alpha \neq 1$ and $\alpha \neq N$.

			No. Factors	No. Computations
N	$=$	$\alpha_1 \cdot \alpha_2$	2	n^k
	$=$	$\alpha_{11} \cdot \alpha_{12} \cdot \alpha_{21} \cdot \alpha_{22}$	4	$2(n-1)^k$
	$=$	$\alpha_{111}\alpha_{112}\alpha_{121}\alpha_{122}\cdots\alpha_{211}\alpha_{212}\alpha_{221}\alpha_{222}$	8	$4(n-2)^k$
	$=$	$\vdots$	$\cdots$	$\vdots$
	$=$	$p_1^{q_1} \cdot p_2^{q_2} \cdot \cdot p_{m-1}^{q_{m-1}} \cdot p_m^{q_m}$	2^l	$2^{l-1}(n-l)^k$

l steps $\Rightarrow$ No. Computations $\leq n^k + 2n^k + 4n^k + \cdots 2^{l-1}n^k \leq 2^l n^k$

Towards Shor's Algorithm for Prime Factorization

Goal : Design a polynomial-time quantum algorithm that can identify the prime factors of a $n-$bit composite number N.

Break the task down.

Efficiently identify non-trivial factor of N.

Find α such that $\alpha|N$ and $\alpha \neq 1$ and $\alpha \neq N$.

			No. Factors	No. Computations
N	$=$	$\alpha_1 \cdot \alpha_2$	2	n^k
	$=$	$\alpha_{11} \cdot \alpha_{12} \cdot \alpha_{21} \cdot \alpha_{22}$	4	$2(n-1)^k$
	$=$	$\alpha_{111}\alpha_{112}\alpha_{121}\alpha_{122}\cdots\alpha_{211}\alpha_{212}\alpha_{221}\alpha_{222}$	8	$4(n-2)^k$
	$=$	$\vdots$	$\cdots$	$\vdots$
	$=$	$p_1^{q_1} \cdot p_2^{q_2} \cdot \cdot p_{m-1}^{q_{m-1}} \cdot p_m^{q_m}$	2^l	$2^{l-1}(n-l)^k$

$$l \text{ steps } \Rightarrow \text{No. Computations } \leq n^k + 2n^k + 4n^k + \cdots 2^{l-1}n^k \leq 2^l n^k$$

$$\text{Since } p_i \geq 2, \quad \text{No. of factors } 2^l \leq \log_2 N \Rightarrow \text{No. Computations } \leq n^k \log_2 N \leq n^{k+1}.$$

The factorization Problem

Suffices to efficiently identify non-trivial factor of $n-$bit integer N.

Goal : Given N, find $1 < x < N$ s.t, GCD$(x, N) > 1$.

Some Number Theoretic Preliminaries

Goal : Given N, find $1 < x < N$ s.t, GCD$(x, N) > 1$.

co-pr$(N) = \{a : 1 < a < N-1,$ s.t GCD$(a, N) = 1,$ i.e., a, N are co-prime$\}$

1. co-pr(N) is a finite group under $\mod N$ multiplication.

   Need b s.t : $ab = 1$ mod N. As you sweep b, ab's are distinct.

2. Being a finite group, each element of co-pr(N) has a finite order.

   $$\text{ord}(a) = \min\{k : a^k = 1 \mod N\} = \text{ period of the fn. } f_{a,N}(k) = a^k \mod N.$$

3. Suppose $r = \text{ord}(a)$ for $a \in \{1, \cdots, N-1\}$. Then

   $$a^r = \theta N + 1 \Rightarrow N \mid (a^r - 1) \text{ and } N \nmid (a^{\frac{r}{2}} - 1)$$

   Case 1: r is even.

   $$N \mid (a^r - 1) = (a^{\frac{r}{2}} - 1)(a^{\frac{r}{2}} + 1)$$

   If $N \nmid (a^{\frac{r}{2}} - 1)$, then we are done. Indeed, $a^{\frac{r}{2}} + 1$ and $a^{\frac{r}{2}} + 1$ have non-trivial common factors with N, i.e., GCD$(a^{\frac{r}{1}} - 1, N) > 1$ and GCD$(a^{\frac{r}{1}} + 1, N) > 1$.

Chances of this happening are HIGH

Theorem

Suppose $N = p_1^{q_1} \cdots p_m^{q_m}$ is the prime factorization. Let $X \in$ co-pr(N) be chosen uniformly at random, Let $R =$ ord(X). Then

$$P(R \text{ is even and } N \nmid (X^{\frac{R}{2}} - 1)) \geq 1 - \frac{1}{2^m}.$$

Suppose we can efficiently compute

$$\text{ord}(a) = \min\{k : a^k = 1 \mod N\} = \text{period of the fn. } f_{a,N}(k) = a^k \mod N.$$

Pick $X_1, \cdots, X_l$ unformly at random, compute $R_1 = \text{ord}(X_1), \cdots, R_l = \text{ord}(X_l)$ and obtain a non-trivial factor of N with high probability.

Algorithm for Identifying Prime Factors

Efficiently identify non-trivial factor of $n-$bit integer N.

Algorithm

Inputs: Composite $n-$bit number N

Algorithm for Identifying Prime Factors

Efficiently identify non-trivial factor of $n-$bit integer N.

Algorithm

Inputs: Composite $n-$bit number N

Step 1 : If N is even, return 2.

Algorithm for Identifying Prime Factors

Efficiently identify non-trivial factor of $n-$bit integer N.

Algorithm

Inputs: Composite $n-$bit number N

Step 1 : If N is even, return 2.

Step 2 : Check if $N = a^b$ for $a \geq 1$, $b \geq 2$. If YES, return a.

Algorithm for Identifying Prime Factors

Efficiently identify non-trivial factor of $n-$bit integer N.

Algorithm

Inputs: Composite $n-$bit number N

Step 1 : If N is even, return 2.

Step 2 : Check if $N = a^b$ for $a \geq 1$, $b \geq 2$. If YES, return a. $b \geq 2$ guarantees $a \neq N$.

Efficiently identify non-trivial factor of $n-$bit integer N.

Algorithm

Inputs: Composite $n-$bit number N

Step 1 : If N is even, return 2.

Step 2 : Check if $N = a^b$ for $a \geq 1$, $b \geq 2$. If YES, return a. $\exists$ efficient classical algorithm.

Algorithm for Identifying Prime Factors

Efficiently identify non-trivial factor of $n-$bit integer N.

Algorithm

Inputs: Composite $n-$bit number N

Step 1 : If N is even, return 2.

Step 2 : Check if $N = a^b$ for $a \geq 1$, $b \geq 2$. If YES, return a. $\exists$ efficient classical algorithm.

Steps 1,2 are quick. Progression to Step 3 implies N is odd, non-prime power.

Algorithm for Identifying Prime Factors

Efficiently identify non-trivial factor of $n-$bit integer N.

Algorithm

Inputs: Composite $n-$bit number N

Step 1 : If N is even, return 2.

Step 2 : Check if $N = a^b$ for $a \geq 1$, $b \geq 2$. If YES, return a. $\exists$ efficient classical algorithm.

Steps 1,2 are quick. Progression to Step 3 implies N is odd, non-prime power.

Step 3 : Randomly choose $x \in \{1, \cdots, N-1\}$. If $\mathrm{GCD}(x, N) > 1$, return $\mathrm{GCD}(x, N)$

Algorithm for Identifying Prime Factors

Efficiently identify non-trivial factor of $n-$bit integer N.

Algorithm

Inputs: Composite $n-$bit number N

Step 1 : If N is even, return 2.

Step 2 : Check if $N = a^b$ for $a \geq 1$, $b \geq 2$. If YES, return a. $\exists$ efficient classical algorithm.

Steps 1,2 are quick. Progression to Step 3 implies N is odd, non-prime power.

Step 3 : Randomly choose $x \in \{1, \cdots, N-1\}$. If GCD$(x, N) > 1$, return GCD(x, N)

Step 4 : Use quantum order finding sub-routine to find ord$(x) \mod N$.

Algorithm for Identifying Prime Factors

Efficiently identify non-trivial factor of $n-$bit integer N.

Algorithm

Inputs: Composite $n-$bit number N

Step 1 : If N is even, return 2.

Step 2 : Check if $N = a^b$ for $a \geq 1$, $b \geq 2$. If YES, return a. $\exists$ efficient classical algorithm.

Steps 1,2 are quick. Progression to Step 3 implies N is odd, non-prime power.

Step 3 : Randomly choose $x \in \{1, \cdots, N-1\}$. If GCD$(x, N) > 1$, return GCD(x, N)

Step 4 : Use quantum order finding sub-routine to find ord$(x) \mod N$.

Step 5 : If r is even and $N \nmid (x^{\frac{r}{2}} + 1)$, then compute GCD$(x^{\frac{r}{2}} + 1, N)$, GCD$(x^{\frac{r}{2}} - 1, N)$. Return if either is non-trivial factor. If none is non-trivial factor return FAILURE

Period Finding is $\mathbb{Z}_{2^n}$ is fundamental to Factorization

Simon's algorithm utilized the Hadamard transform to provide us period in $(\mathbb{Z}_2)^n$.

Suppose $f : \{0, 1, \cdots, 2^n - 1\} \to \{0, 1, \cdots, 2^m - 1\}$ is a periodic function in $\mathbb{Z}_{2^n}$, i.e,

$$f(x) = f(x + r) \text{ for some } 0 < r < 2^n - 1 \text{ and } \forall x \text{ valid.}$$

$\exists$ efficient algo. to compute r with high prob. $\Rightarrow$ $\exists$ efficient algo. to FACTOR composite integer N with high. prob.

Quantum Fourier Transform in place of Hadamard transform yield period in $\mathbb{Z}_{2^n}$.