Quantum Computing Seminar 4

YongHyun "Aeren" An

Samsung Research

November 18, 2024
November 25, 2024

Remark

Remark

- Quantum information is **NOT** probabilistic. It is a fixed sequence of complex numbers stored in qubits.

Remark

- Quantum information is **NOT** probabilistic. It is a fixed sequence of complex numbers stored in qubits.
- Quantum information evolves deterministically when we apply any number of unitary operations.

Remark

- Quantum information is **NOT** probabilistic. It is a fixed sequence of complex numbers stored in qubits.
- Quantum information evolves deterministically when we apply any number of unitary operations.
- What is probabilistic is the way we interact with quantum information, i.e. the measurement.

Remark

- Quantum information is **NOT** probabilistic. It is a fixed sequence of complex numbers stored in qubits.
- Quantum information evolves deterministically when we apply any number of unitary operations.
- What is probabilistic is the way we interact with quantum information, i.e. the measurement.
- If we have information of the initial state and the unitary operations applied, we deterministically know the final state assuming there were no measurement.

Quantum Circuit

Quantum circuit will be the standard description of quantum computation that we'll use.

Quantum Circuit

Quantum circuit will be the standard description of quantum computation that we'll use.
It consists of the following components

Quantum Circuit

Quantum circuit will be the standard description of quantum computation that we'll use. It consists of the following components

- **Qubits** - for storing quantum information, which is hidden

Quantum Circuit

Quantum circuit will be the standard description of quantum computation that we'll use. It consists of the following components

- **Qubits** - for storing quantum information, which is hidden
- **Classical Bits** - for storing classical information, which is visible

Quantum Circuit

Quantum circuit will be the standard description of quantum computation that we'll use. It consists of the following components

- **Qubits** - for storing quantum information, which is hidden
- **Classical Bits** - for storing classical information, which is visible
- **Unitary Operations** - for modifying quantum information

Quantum Circuit

Quantum circuit will be the standard description of quantum computation that we'll use. It consists of the following components

- **Qubits** - for storing quantum information, which is hidden
- **Classical Bits** - for storing classical information, which is visible
- **Unitary Operations** - for modifying quantum information
- **Measurements** - for probabilistically transforming quantum information into classical information, so that we can indirectly observe the quantum information

Quantum Circuit

Quantum circuit will be the standard description of quantum computation that we'll use.
It consists of the following components

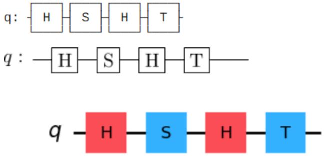
- **Qubits** - for storing quantum information, which is hidden
- **Classical Bits** - for storing classical information, which is visible
- **Unitary Operations** - for modifying quantum information
- **Measurements** - for probabilistically transforming quantum information into classical information, so that we can indirectly observe the quantum information

Unitary operations and measurements are applied sequentially to the qubits and classical bits.

Quantum Circuit

Default name of qubits are $q_0, \cdots, q_{n-1}$
(or q if there's only one qubit)

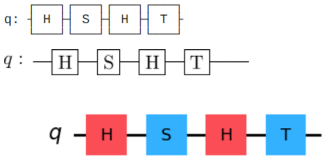
```
from qiskit import QuantumCircuit, QuantumRegister, ClassicalRegister
from qiskit.primitives import Sampler
from qiskit.visualization import plot_histogram

circuit = QuantumCircuit(1)

circuit.h(0)
circuit.s(0)
circuit.h(0)
circuit.t(0)

display(circuit.draw())
display(circuit.draw("latex"))
display(circuit.draw("mpl"))
```



Quantum Circuit

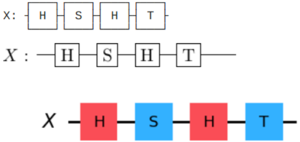
Default name of qubits are $q_0, \cdots, q_{n-1}$
(or q if there's only one qubit)

```
from qiskit import QuantumCircuit, QuantumRegister, ClassicalRegister
from qiskit.primitives import Sampler
from qiskit.visualization import plot_histogram

circuit = QuantumCircuit(1)

circuit.h(0)
circuit.s(0)
circuit.h(0)
circuit.t(0)

display(circuit.draw())
display(circuit.draw("latex"))
display(circuit.draw("mpl"))
```



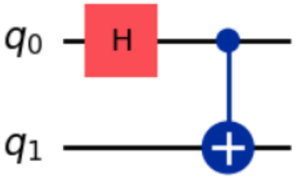
The name of qubits can be set explicitly

```
X = QuantumRegister(1, "X")
circuit = QuantumCircuit(X)

circuit.h(X)
circuit.s(X)
circuit.h(X)
circuit.t(X)

display(circuit.draw())
display(circuit.draw("latex"))
display(circuit.draw("mpl"))
```



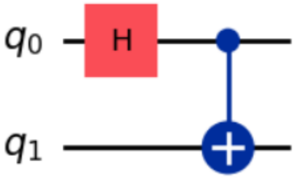
Quantum Circuit

```
circuit = QuantumCircuit(2)

circuit.h(0)
circuit.cx(0, 1)

circuit.draw("mpl")
```



Quantum Circuit

```
circuit = QuantumCircuit(2)

circuit.h(0)
circuit.cx(0, 1)

circuit.draw("mpl")
```

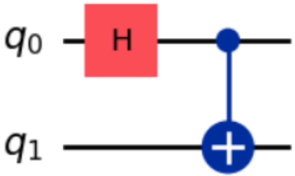


The first layer applies the Hadamard operation on q_0 while leaving q_1 untouched, which is the same as applying the identity operation.

$$I_2 \otimes H = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}$$

Quantum Circuit

```
circuit = QuantumCircuit(2)

circuit.h(0)
circuit.cx(0, 1)

circuit.draw("mpl")
```

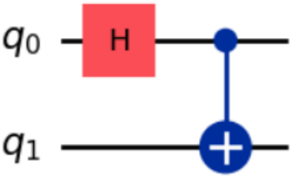


The second layer applies controlled-not operation on q_1 with q_0 as the control bit.

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

Quantum Circuit

```
circuit = QuantumCircuit(2)

circuit.h(0)
circuit.cx(0, 1)

circuit.draw("mpl")
```

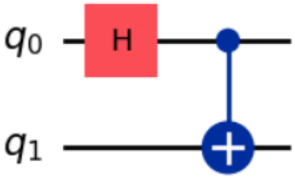


Therefore, the entire circuit represents the following matrix

$$U = CX_{0,1} \cdot (I_2 \otimes H) = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 & 0 \end{bmatrix}$$

Quantum Circuit

```
circuit = QuantumCircuit(2)

circuit.h(0)
circuit.cx(0, 1)

circuit.draw("mpl")
```



And the following relations completely characterizes the circuit

$U|00\rangle = |\phi^+\rangle$
$U|01\rangle = |\phi^-\rangle$
$U|10\rangle = |\psi^+\rangle$
$U|11\rangle = -|\psi^-\rangle$

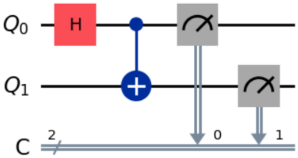
where $|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle$ are bell states

$|\phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$
$|\phi^-\rangle = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$
$|\psi^+\rangle = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$
$|\psi^-\rangle = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$

Quantum Circuit

We can measure by adding classical bits to the circuit; Classical bits are represented with double-lines

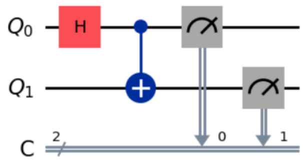
```
Q = QuantumRegister(2, "Q")
C = ClassicalRegister(2, "C")

circuit = QuantumCircuit(Q, C)
circuit.h(Q[0])
circuit.cx(Q[0], Q[1])
circuit.measure(Q[0], C[0])
circuit.measure(Q[1], C[1])

circuit.draw("mpl")
```



Quantum Circuit

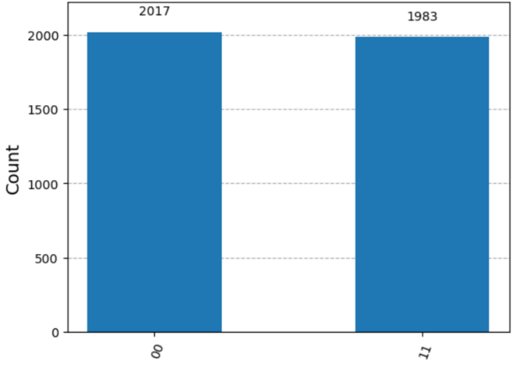
We can measure by adding classical bits to the circuit; Classical bits are represented with double-lines

```
Q = QuantumRegister(2, "Q")
C = ClassicalRegister(2, "C")

circuit = QuantumCircuit(Q, C)
circuit.h(Q[0])
circuit.cx(Q[0], Q[1])
circuit.measure(Q[0], C[0])
circuit.measure(Q[1], C[1])

circuit.draw("mpl")
```



Qubits are initialized with $|0\cdots0\rangle$ by default

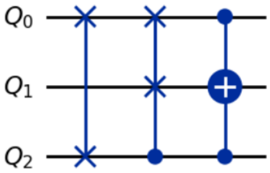
```
result = StatevectorSampler().run([circuit], shots = 4000).result()[0]
plot_histogram(result.data.C.get_counts())
```



Quantum Circuit

Some more examples of gates (SWAP, $C\mathrm{SWAP}$, CCX)

```
Q = QuantumRegister(3, "Q")

circuit = QuantumCircuit(Q)
circuit.swap(Q[0], Q[2])
circuit.cswap(Q[2], Q[0], Q[1])
circuit.ccx(Q[0], Q[2], Q[1])

circuit.draw("mpl")
```



Projective Measurement

Projective Measurement

Definition (Orthogonal Projection)

A complex square matrix P is an **orthogonal projection** if

1. $P^H = P$
2. $P^2 = P$

Projective Measurement

Definition (Orthogonal Projection)

A complex square matrix P is an **orthogonal projection** if

1. $P^H = P$
2. $P^2 = P$

- Let $|u\rangle$ be a unit vector and $P = |u\rangle\langle u|$. Then P is an orthogonal projection.

Projective Measurement

Definition (Orthogonal Projection)

A complex square matrix P is an **orthogonal projection** if

1. $P^H = P$
2. $P^2 = P$

- Let $|u\rangle$ be a unit vector and $P = |u\rangle\langle u|$. Then P is an orthogonal projection.
- More generally, let $\{|u_0\rangle, \cdots, |u_{k-1}\rangle\}$ be an orthonormal set of vectors and let $P = \sum_{i=0}^{k-1} |u_i\rangle\langle u_i|$. Then P is an orthogonal projection.

Projective Measurement

Theorem

A complex square matrix P is an orthogonal projection if and only if there exists an orthonormal set of vectors $\{|u_0\rangle, \cdots, |u_{k-1}\rangle\}$ such that $P = \sum_{i=0}^{k-1} |u_i\rangle\langle u_i|$.

Projective Measurement

Theorem

A complex square matrix P is an orthogonal projection if and only if there exists an orthonormal set of vectors $\{|u_0\rangle, \cdots, |u_{k-1}\rangle\}$ such that $P = \sum_{i=0}^{k-1} |u_i\rangle \langle u_i|$.

Proof

- Since $P = P^2$, its eigenvalues are either 0 or 1.
- Since P is Hermitian, it has an orthonormal basis consisting of eigenvectors. Hence,

$$P = QDQ^{-1} = \sum_{i=0}^{n-1} \lambda_i Q |i\rangle \langle i| Q^{-1} = \sum_{i=0}^{n-1} \lambda_i (Q|i\rangle)(Q|i\rangle)^H$$

- Let $|u_i\rangle = Q|j\rangle$ for each j with $\lambda_j = 1$ and we're done.

Projective Measurement

Definition (Standard basis measurement and projective measurement)

The measurements we've discussed so far is called the **standard basis measurement**.
A **projective measurement** is a set $\{P_0, \cdots, P_{m-1}\}$ of orthogonal projection matrices such that $P_0 + \cdots + P_{m-1} = I_{2^n}$.

Projective Measurement

Definition (Standard basis measurement and projective measurement)

The measurements we've discussed so far is called the **standard basis measurement**.
A **projective measurement** is a set $\{P_0, \cdots, P_{m-1}\}$ of orthogonal projection matrices such that $P_0 + \cdots + P_{m-1} = I_{2^n}$.
Let X be a system with state $|u\rangle$.

- The projective measurement on X has probability $|P_i |u\rangle|^2$ of having outcome i.
- In such case, the state of X collapses to $\frac{1}{|P_i|u\rangle|} P_i |u\rangle$.

Projective Measurement

Definition (Standard basis measurement and projective measurement)

The measurements we've discussed so far is called the **standard basis measurement**.
A **projective measurement** is a set $\{P_0, \cdots, P_{m-1}\}$ of orthogonal projection matrices such that $P_0 + \cdots + P_{m-1} = I_{2^n}$.
Let X be a system with state $|u\rangle$.

- The projective measurement on X has probability $|P_i |u\rangle|^2$ of having outcome i.
- In such case, the state of X collapses to $\frac{1}{|P_i|u\rangle|} P_i |u\rangle$.

- Verify that the probabilities sums up to 1.

Projective Measurement

Definition (Standard basis measurement and projective measurement)

The measurements we've discussed so far is called the **standard basis measurement**.
A **projective measurement** is a set $\{P_0, \cdots, P_{m-1}\}$ of orthogonal projection matrices such that $P_0 + \cdots + P_{m-1} = I_{2^n}$.
Let X be a system with state $|u\rangle$.

- The projective measurement on X has probability $|P_i\,|u\rangle|^2$ of having outcome i.
- In such case, the state of X collapses to $\frac{1}{|P_i|u\rangle|} P_i\,|u\rangle$.

- Verify that the probabilities sums up to 1.
- What happens when $m = 2^n$ and $P_i = |\mathrm{binary}_n(i)\rangle\,\langle\mathrm{binary}_n(i)|$?

Projective Measurement

Theorem

A set of 2^n by 2^n complex matrices $\{P_0, \cdots, P_{m-1}\}$ is a projective measurement if and only if there exists an orthonormal basis B and a partition

$$C_0 = \{|c_{0,0}\rangle, \cdots, |c_{0,n_0-1}\rangle\}, \cdots, C_{m-1} = \{|c_{m-1,0}\rangle, \cdots, |c_{m-1,n_{m-1}-1}\rangle\}$$

of B such that $P_i = \sum_{j=0}^{n_i-1} |c_{i,j}\rangle \langle c_{i,j}|$ for all $0 \leq i < m$.

Projective Measurement

Theorem

A set of 2^n by 2^n complex matrices $\{P_0, \cdots, P_{m-1}\}$ is a projective measurement if and only if there exists an orthonormal basis B and a partition

$$C_0 = \{|c_{0,0}\rangle, \cdots, |c_{0,n_0-1}\rangle\}, \cdots, C_{m-1} = \{|c_{m-1,0}\rangle, \cdots, |c_{m-1,n_{m-1}-1}\rangle\}$$

of B such that $P_i = \sum_{j=0}^{n_i-1} |c_{i,j}\rangle \langle c_{i,j}|$ for all $0 \leq i < m$.

Proof of sufficiency

- $P_i^H = \sum_{j=0}^{n_i-1} (|c_{i,j}\rangle \langle c_{i,j}|)^H = \sum_{j=0}^{n_i-1} |c_{i,j}\rangle \langle c_{i,j}| = P_i$
- $P_i^2 = \sum_{j=0}^{n_i-1} \sum_{k=0}^{n_i-1} |c_{i,j}\rangle \langle c_{i,j}|c_{i,k}\rangle \langle c_{i,k}| = \sum_{j=0}^{n_i-1} |c_{i,j}\rangle \langle c_{i,j}| = P_i$
- For all vector $|u\rangle$, $\sum_{i=0}^{n-1} P_i |u\rangle = \sum_{i=0}^{n-1} \sum_{j=0}^{n_i-1} |c_{i,j}\rangle \langle c_{i,j}|u\rangle = |u\rangle$, hence $\sum_{i=0}^{n-1} P_i = I_{2^n}$

Projective Measurement

Theorem

A set of 2^n by 2^n complex matrices $\{P_0, \cdots, P_{m-1}\}$ is a projective measurement if and only if there exists an orthonormal basis B and a partition

$$C_0 = \{|c_{0,0}\rangle, \cdots, |c_{0,n_0-1}\rangle\}, \cdots, C_{m-1} = \{|c_{m-1,0}\rangle, \cdots, |c_{m-1,n_{m-1}-1}\rangle\}$$

of B such that $P_i = \sum_{j=0}^{n_i-1} |c_{i,j}\rangle\langle c_{i,j}|$ for all $0 \leq i < m$.

Proof of necessity

- We know that $P_i = \sum_{j=0}^{n_i-1} |c_{i,j}\rangle$ where $C_i = \{c_{i,0}, \cdots, c_{i,n_i-1}\}$ is an orthonormal basis of the eigenspace of P_i corresponding to the eigenvalue 1.
- Fix an i, then for each $|u\rangle \in C_i$,

$$1 = \langle u|u\rangle = \langle u| \sum_{j=0}^{m-1} P_j |u\rangle = 1 + \sum_{j=0, j\neq i}^{m-1} \sum_{k=0}^{n_j-1} |\langle c_{j,k}|u\rangle|^2$$

Projective Measurement

Theorem

A set of 2^n by 2^n complex matrices $\{P_0, \cdots, P_{m-1}\}$ is a projective measurement if and only if there exists an orthonormal basis B and a partition

$$C_0 = \{|c_{0,0}\rangle, \cdots, |c_{0,n_0-1}\rangle\}, \cdots, C_{m-1} = \{|c_{m-1,0}\rangle, \cdots, |c_{m-1,n_{m-1}-1}\rangle\}$$

of B such that $P_i = \sum_{j=0}^{n_i-1} |c_{i,j}\rangle \langle c_{i,j}|$ for all $0 \leq i < m$.

Proof of necessity

- Hence, $\langle c_{j,k}|u\rangle = 0$ for all $j \neq i$ and $0 \leq k < n_j$, and every eigenspaces corresponding to 1 of P_i are orthogonal to each other.
- Since the sum of ranks of P_i must sum up to 2^n, the union of C_i must form an orthonormal basis.

Projective Measurement

Excercise

Consider a system consisting of 4 qubits $q_0, \cdots, q_3$.

Projective Measurement

Excercise

Consider a system consisting of 4 qubits $q_0, \cdots, q_3$.

1. Show that the partial measurement of qubits q_0 and q_3 is a projective measurement.

Projective Measurement

Excercise

Consider a system consisting of 4 qubits $q_0, \cdots, q_3$.

1. Show that the partial measurement of qubits q_0 and q_3 is a projective measurement.
2. Find the corresponding partition of an orthonormal basis given by the previous theorem.

Projective Measurement

Implementation of projective measurement

Projective Measurement

Implementation of projective measurement

- It turns out we can implement projective measurement with unitary operations, standard basis measurement, and an extra workspace system.

Projective Measurement

Implementation of projective measurement

- It turns out we can implement projective measurement with unitary operations, standard basis measurement, and an extra workspace system.
- Let $\{P_0, \cdots, P_{m-1}\}$ be a projective measurement on a system X with n qubits $q_0, \cdots, q_{n-1}$. We introduce a new system Y with a single special qubit which can have value of $|0\rangle, \cdots, |m-1\rangle$ upon measurement, which is initially on the state $|0\rangle$.

Projective Measurement

Implementation of projective measurement

- It turns out we can implement projective measurement with unitary operations, standard basis measurement, and an extra workspace system.
- Let $\{P_0, \cdots, P_{m-1}\}$ be a projective measurement on a system X with n qubits $q_0, \cdots, q_{n-1}$. We introduce a new system Y with a single special qubit which can have value of $|0\rangle, \cdots, |m-1\rangle$ upon measurement, which is initially on the state $|0\rangle$.
- Let

$$U = \begin{bmatrix} P_0 & 0 & \cdots & 0 \\ P_1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ P_{m-1} & 0 & \cdots & 0 \end{bmatrix}$$

  be a matrix acting on the combined system (Y, X)
- U is not unitary since it has zero determinant due to having zero column. However,

Projective Measurement

Lemma

First 2^n columns of U forms an orthonormal set of size n.

Projective Measurement

Lemma

First 2^n columns of U forms an orthonormal set of size n.

Proof

Projective Measurement

Lemma

First 2^n columns of U forms an orthonormal set of size n.

Proof

- The i-th column of U, where $0 \leq i < 2^n$, is $|C_i\rangle = \sum_{k=0}^{m-1} |k\rangle \otimes P_k \, |\mathrm{binary}_n(i)\rangle$

Projective Measurement

Lemma

First 2^n columns of U forms an orthonormal set of size n.

Proof

- The i-th column of U, where $0 \leq i < 2^n$, is $|C_i\rangle = \sum_{k=0}^{m-1} |k\rangle \otimes P_k \, |\mathrm{binary}_n(i)\rangle$
-

$$
\begin{aligned}
\langle C_i | C_j \rangle &= \left(\sum_{k=0}^{m-1} |k\rangle \otimes P_k \, |\mathrm{binary}_n(i)\rangle \right)^H \left(\sum_{l=0}^{m-1} |l\rangle \otimes P_k \, |\mathrm{binary}_n(j)\rangle \right) \\
&= \sum_{k=0}^{m-1} \sum_{l=0}^{m-1} \langle k | l \rangle \, \langle \mathrm{binary}_n(i) | P_k P_l | \mathrm{binary}_n(j) \rangle = \sum_{k=0}^{m-1} \langle \mathrm{binary}_n(i) | P_k | \mathrm{binary}_n(j) \rangle \\
&= \langle \mathrm{binary}_n(i) | \mathrm{binary}_n(j) \rangle = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}
\end{aligned}
$$

Projective Measurement

Implementation of projective measurement

- Therefore, we can fill the zero columns of U so that U becomes unitary, for example, using Gram-Schmidt process.

Projective Measurement

Implementation of projective measurement

- Therefore, we can fill the zero columns of U so that U becomes unitary, for example, using Gram-Schmidt process.
- Suppose X is initially in the state $|u\rangle$, hence (Y, X) is on the state $|0, u\rangle$. Applying U changes the state of (Y, X) into

$$U|0, u\rangle = \sum_{k=0}^{m-1} |k\rangle \otimes P_k |u\rangle$$

Projective Measurement

Implementation of projective measurement

- Therefore, we can fill the zero columns of U so that U becomes unitary, for example, using Gram-Schmidt process.
- Suppose X is initially in the state $|u\rangle$, hence (Y, X) is on the state $|0, u\rangle$. Applying U changes the state of (Y, X) into

$$U|0, u\rangle = \sum_{k=0}^{m-1} |k\rangle \otimes P_k |u\rangle$$

- Performing the standard basis measurement on Y has probability $|P_i |u\rangle|^2$ of having outcome i, in which case the state of (Y, X) collapses to

$$|i\rangle \otimes \frac{1}{|P_i |u\rangle|} P_i |u\rangle$$

Projective Measurement

Implementation of projective measurement

- Therefore, we can fill the zero columns of U so that U becomes unitary, for example, using Gram-Schmidt process.
- Suppose X is initially in the state $|u\rangle$, hence (Y, X) is on the state $|0, u\rangle$. Applying U changes the state of (Y, X) into

$$U|0, u\rangle = \sum_{k=0}^{m-1} |k\rangle \otimes P_k |u\rangle$$

- Performing the standard basis measurement on Y has probability $|P_i |u\rangle|^2$ of having outcome i, in which case the state of (Y, X) collapses to

$$|i\rangle \otimes \frac{1}{|P_i |u\rangle|} P_i |u\rangle$$

- We now discard Y and has obtained the projective measurement on X.

Remark

Remark

- An isolated quantum system can only go through unitary evolution.

Remark

- An isolated quantum system can only go through unitary evolution.
- The implementation of projective measurement hints at what a measurement is: if we perform a specific unitary process to a combined system, we obtain what we've known as a measurement on one of the subsystem.

Limitation on Quantum Information

Limitation on Quantum Information

Limitation #1: Global phases are irrelevant

Let $|u\rangle$ and $|v\rangle$ be quantum states with $|v\rangle = e^{i\theta} |u\rangle$ for some real number θ. These states are said to **differ by a global phase**.

Then $|u\rangle$ and $|v\rangle$ have identical probability distribution of measurement results in any sequence of (projective) measurements and unitary operations.

Limitation on Quantum Information

Limitation #1: Global phases are irrelevant

Let $|u\rangle$ and $|v\rangle$ be quantum states with $|v\rangle = e^{i\theta}|u\rangle$ for some real number θ. These states are said to **differ by a global phase**.

Then $|u\rangle$ and $|v\rangle$ have identical probability distribution of measurement results in any sequence of (projective) measurements and unitary operations.

Proof

Limitation on Quantum Information

Limitation #1: Global phases are irrelevant

Let $|u\rangle$ and $|v\rangle$ be quantum states with $|v\rangle = e^{\mathrm{i}\theta} |u\rangle$ for some real number θ. These states are said to **differ by a global phase**.

Then $|u\rangle$ and $|v\rangle$ have identical probability distribution of measurement results in any sequence of (projective) measurements and unitary operations.

Proof

- If the first operation is an unitary operation U, the state after it is $U|u\rangle$ and $e^{\mathrm{i}\theta} U |u\rangle$, which differs by a global phase.

Limitation on Quantum Information

Limitation #1: Global phases are irrelevant

Let $|u\rangle$ and $|v\rangle$ be quantum states with $|v\rangle = e^{i\theta}|u\rangle$ for some real number θ. These states are said to **differ by a global phase**.
Then $|u\rangle$ and $|v\rangle$ have identical probability distribution of measurement results in any sequence of (projective) measurements and unitary operations.

Proof

- If the first operation is an unitary operation U, the state after it is $U|u\rangle$ and $e^{i\theta}U|u\rangle$, which differs by a global phase.
- If the first operation is a projective measurement $\{P_0, \cdots, P_{m-1}\}$, the probability of the outcome being i is $|P_i|u\rangle|$ and $\left|e^{i\theta}\right| \cdot |P_i|u\rangle| = |P_i|u\rangle|$, which are identical. The state after the outcome i is $\frac{1}{|P|u\rangle|}P|u\rangle$ and $\frac{e^{i\theta}}{|P|u\rangle|}P|u\rangle$ which differs by a global phase.

Limitation on Quantum Information

Limitation #1: Global phases are irrelevant

Let $|u\rangle$ and $|v\rangle$ be quantum states with $|v\rangle = e^{i\theta} |u\rangle$ for some real number θ. These states are said to **differ by a global phase**.
Then $|u\rangle$ and $|v\rangle$ have identical probability distribution of measurement results in any sequence of (projective) measurements and unitary operations.

Proof

- If the first operation is an unitary operation U, the state after it is $U|u\rangle$ and $e^{i\theta} U |u\rangle$, which differs by a global phase.
- If the first operation is a projective measurement $\{P_0, \cdots, P_{m-1}\}$, the probability of the outcome being i is $|P_i |u\rangle|$ and $\left|e^{i\theta}\right| \cdot |P_i |u\rangle| = |P_i |u\rangle|$, which are identical. The state after the outcome i is $\frac{1}{|P|u\rangle|} P |u\rangle$ and $\frac{e^{i\theta}}{|P|u\rangle|} P |u\rangle$ which differs by a global phase.
- Use induction on the length of the sequence and we're done.

Limitation on Quantum Information

Note
global phase vs local phase

Note

global phase vs local phase

- Let $|u\rangle$ be either $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ or $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$, which differs by a local phase. They can be distinguished by measuring $H|u\rangle$ as mentioned before.

Limitation on Quantum Information

Note

global phase vs local phase

- Let $|u\rangle$ be either $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ or $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$, which differs by a local phase. They can be distinguished by measuring $H|u\rangle$ as mentioned before.
- On the other hand, if $|u\rangle$ is either $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$ or $-|-\rangle = -\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ which differs by a global phase, they cannot be distinguished no matter what.

Limitation on Quantum Information

Limitation #2: States cannot be copied (no cloning theorem)

Let X and Y be states with n qubits each, where Y is on $|v\rangle$. There is no unitary operation U on (X, Y) such that for all state $|u\rangle$ of X, $U(|u\rangle \otimes |v\rangle) = |u\rangle \otimes |u\rangle$.

Limitation on Quantum Information

Limitation #2: States cannot be copied (no cloning theorem)

Let X and Y be states with n qubits each, where Y is on $|v\rangle$. There is no unitary operation U on (X, Y) such that for all state $|u\rangle$ of X, $U(|u\rangle \otimes |v\rangle) = |u\rangle \otimes |u\rangle$.

Proof

Limitation on Quantum Information

Limitation $\#2$: States cannot be copied (no cloning theorem)

Let X and Y be states with n qubits each, where Y is on $|v\rangle$. There is no unitary operation U on (X, Y) such that for all state $|u\rangle$ of X, $U(|u\rangle \otimes |v\rangle) = |u\rangle \otimes |u\rangle$.

Proof

We have $U(|0\rangle \otimes |v\rangle) = |0\rangle \otimes |0\rangle$ and $U(|1\rangle \otimes |v\rangle) = |1\rangle \otimes |1\rangle$.

Limitation on Quantum Information

Limitation #2: States cannot be copied (no cloning theorem)

Let X and Y be states with n qubits each, where Y is on $|v\rangle$. There is no unitary operation U on (X, Y) such that for all state $|u\rangle$ of X, $U(|u\rangle \otimes |v\rangle) = |u\rangle \otimes |u\rangle$.

Proof

We have $U(|0\rangle \otimes |v\rangle) = |0\rangle \otimes |0\rangle$ and $U(|1\rangle \otimes |v\rangle) = |1\rangle \otimes |1\rangle$.
Adding each side and multiplying them by $\frac{1}{\sqrt{2}}$ yields

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

Limitation on Quantum Information

Limitation #2: States cannot be copied (no cloning theorem)

Let X and Y be states with n qubits each, where Y is on $|v\rangle$. There is no unitary operation U on (X, Y) such that for all state $|u\rangle$ of X, $U(|u\rangle \otimes |v\rangle) = |u\rangle \otimes |u\rangle$.

Proof

We have $U(|0\rangle \otimes |v\rangle) = |0\rangle \otimes |0\rangle$ and $U(|1\rangle \otimes |v\rangle) = |1\rangle \otimes |1\rangle$.
Adding each side and multiplying them by $\frac{1}{\sqrt{2}}$ yields

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

However,

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

Which is a contradiction.

Limitation on Quantum Information

Note

There are unitary operations which can clone some subset of states.

Note

There are unitary operations which can clone some subset of states.
For example, let $U = CX_{1,0}$ and Y is on $|0\rangle$. Then $U|00\rangle = |00\rangle$ and $U|10\rangle = |11\rangle$.

Limitation on Quantum Information

Note

There are unitary operations which can clone some subset of states.
For example, let $U = CX_{1,0}$ and Y is on $|0\rangle$. Then $U|00\rangle = |00\rangle$ and $U|10\rangle = |11\rangle$.
However, it cannot clone $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ as seen before.

Limitation on Quantum Information

Limitation #3: Non-orthogonal states cannot be perfectly distinguished

Two states $|u\rangle$ and $|v\rangle$ over the system X with qubits $q_0, \cdots, q_{n-1}$ are orthogonal if and only if there exists a system Y which is on the all-zero state, a unitary operation U on (Y, X), and a projective measurement $M = \{M_0, M_1\}$ such that

$$\mathcal{P}_{M=0}\left(U\left|0\cdots0, u\right\rangle\right) = \mathcal{P}_{M=1}\left(U\left|0\cdots0, v\right\rangle\right) = 1$$

Limitation #3: Non-orthogonal states cannot be perfectly distinguished

Two states $|u\rangle$ and $|v\rangle$ over the system X with qubits $q_0, \cdots, q_{n-1}$ are orthogonal if and only if there exists a system Y which is on the all-zero state, a unitary operation U on (Y, X), and a projective measurement $M = \{M_0, M_1\}$ such that

$$\mathcal{P}_{M=0}\left(U\left|0\cdots 0, u\right\rangle\right) = \mathcal{P}_{M=1}\left(U\left|0\cdots 0, v\right\rangle\right) = 1$$

Proof of sufficiency

Limitation on Quantum Information

Limitation #3: Non-orthogonal states cannot be perfectly distinguished

Two states $|u\rangle$ and $|v\rangle$ over the system X with qubits $q_0, \cdots, q_{n-1}$ are orthogonal if and only if there exists a system Y which is on the all-zero state, a unitary operation U on (Y, X), and a projective measurement $M = \{M_0, M_1\}$ such that

$$\mathcal{P}_{M=0}(U|0\cdots0, u\rangle) = \mathcal{P}_{M=1}(U|0\cdots0, v\rangle) = 1$$

Proof of sufficiency

- Let $A = \{|a_0\rangle, \cdots, |a_{n_a-1}\rangle\}$ and $B = \{|b_0\rangle, \cdots, |b_{n_b-1}\rangle\}$ the corresponding orthonormal sets for M_0 and M_1.

Limitation on Quantum Information

Limitation #3: Non-orthogonal states cannot be perfectly distinguished

Two states $|u\rangle$ and $|v\rangle$ over the system X with qubits $q_0, \cdots, q_{n-1}$ are orthogonal if and only if there exists a system Y which is on the all-zero state, a unitary operation U on (Y, X), and a projective measurement $M = \{M_0, M_1\}$ such that

$$\mathcal{P}_{M=0}\left(U\left|0\cdots 0, u\right\rangle\right) = \mathcal{P}_{M=1}\left(U\left|0\cdots 0, v\right\rangle\right) = 1$$

Proof of sufficiency

- Let $A = \{|a_0\rangle, \cdots, |a_{n_a-1}\rangle\}$ and $B = \{|b_0\rangle, \cdots, |b_{n_b-1}\rangle\}$ the corresponding orthonormal sets for M_0 and M_1.
- The condition implies that $U\left|0\cdots 0, u\right\rangle = \sum_{i=0}^{n_a-1} c_i \left|a_i\right\rangle$ and $U\left|0\cdots 0, v\right\rangle = \sum_{j=0}^{n_b-1} d_j \left|b_j\right\rangle$ for some scalars c_i and d_j.

Limitation #3: Non-orthogonal states cannot be perfectly distinguished

Two states $|u\rangle$ and $|v\rangle$ over the system X with qubits $q_0, \cdots, q_{n-1}$ are orthogonal if and only if there exists a system Y which is on the all-zero state, a unitary operation U on (Y, X), and a projective measurement $M = \{M_0, M_1\}$ such that

$$\mathcal{P}_{M=0}\left(U\left|0\cdots0, u\right\rangle\right) = \mathcal{P}_{M=1}\left(U\left|0\cdots0, v\right\rangle\right) = 1$$

Proof of sufficiency

- Let $A = \{|a_0\rangle, \cdots, |a_{n_a-1}\rangle\}$ and $B = \{|b_0\rangle, \cdots, |b_{n_b-1}\rangle\}$ the corresponding orthonormal sets for M_0 and M_1.
- The condition implies that $U\left|0\cdots0, u\right\rangle = \sum_{i=0}^{n_a-1} c_i\left|a_i\right\rangle$ and $U\left|0\cdots0, v\right\rangle = \sum_{j=0}^{n_b-1} d_j\left|b_j\right\rangle$ for some scalars c_i and d_j.
- These are equivalent to $\left|0\cdots0, u\right\rangle = \sum_{i=0}^{n_a-1} c_i U^H\left|a_i\right\rangle$ and $\left|0\cdots0, v\right\rangle = \sum_{j=0}^{n_b-1} d_j U^H\left|b_j\right\rangle$.

Limitation on Quantum Information

Limitation #3: Non-orthogonal states cannot be perfectly distinguished

Two states $|u\rangle$ and $|v\rangle$ over the system X with qubits $q_0, \cdots, q_{n-1}$ are orthogonal if and only if there exists a system Y which is on the all-zero state, a unitary operation U on (Y, X), and a projective measurement $M = \{M_0, M_1\}$ such that

$$\mathcal{P}_{M=0}\left(U\left|0\cdots 0, u\right\rangle\right) = \mathcal{P}_{M=1}\left(U\left|0\cdots 0, v\right\rangle\right) = 1$$

Proof of sufficiency

- We take their inner product to obtain the orthogonality.

$$\text{LHS} = \langle 0\cdots 0, u | 0\cdots 0, v\rangle = \langle 0\cdots 0 | 0\cdots 0\rangle \langle u|v\rangle = \langle u|v\rangle$$

$$\text{RHS} = \sum_{i=0}^{n_a-1}\sum_{j=0}^{n_b-1} c_i d_j \langle a_i|UU^H|b_j\rangle = \sum_{i=0}^{n_a-1}\sum_{j=0}^{n_b-1} c_i d_j \langle a_i|b_j\rangle = 0$$

Limitation on Quantum Information

Limitation #3: Non-orthogonal states cannot be perfectly distinguished

Two states $|u\rangle$ and $|v\rangle$ over the system X with qubits $q_0, \cdots, q_{n-1}$ are orthogonal if and only if there exists a system Y which is on the all-zero state, a unitary operation U on (Y, X), and a projective measurement $M = \{M_0, M_1\}$ such that

$$\mathcal{P}_{M=0}\left(U\left|0\cdots0, u\right\rangle\right) = \mathcal{P}_{M=1}\left(U\left|0\cdots0, v\right\rangle\right) = 1$$

Proof of necessity

Limitation on Quantum Information

Limitation #3: Non-orthogonal states cannot be perfectly distinguished

Two states $|u\rangle$ and $|v\rangle$ over the system X with qubits $q_0, \cdots, q_{n-1}$ are orthogonal if and only if there exists a system Y which is on the all-zero state, a unitary operation U on (Y, X), and a projective measurement $M = \{M_0, M_1\}$ such that

$$\mathcal{P}_{M=0}\left(U\left|0\cdots0, u\right\rangle\right) = \mathcal{P}_{M=1}\left(U\left|0\cdots0, v\right\rangle\right) = 1$$

Proof of necessity

- Set $Y = \emptyset$, $U = I_{2^n}$, and $M = \{|u\rangle\langle u|, I_{2^n} - |u\rangle\langle u|\}$.

Limitation on Quantum Information

Limitation #3: Non-orthogonal states cannot be perfectly distinguished

Two states $|u\rangle$ and $|v\rangle$ over the system X with qubits $q_0, \cdots, q_{n-1}$ are orthogonal if and only if there exists a system Y which is on the all-zero state, a unitary operation U on (Y, X), and a projective measurement $M = \{M_0, M_1\}$ such that

$$\mathcal{P}_{M=0}(U|0\cdots 0, u\rangle) = \mathcal{P}_{M=1}(U|0\cdots 0, v\rangle) = 1$$

Proof of necessity

- Set $Y = \emptyset$, $U = I_{2^n}$, and $M = \{|u\rangle\langle u|, I_{2^n} - |u\rangle\langle u|\}$.
- $\mathcal{P}_{M=0}(|u\rangle) = ||u\rangle\langle u|u\rangle|^2 = ||u\rangle|^2 = 1$

Limitation on Quantum Information

Limitation #3: Non-orthogonal states cannot be perfectly distinguished

Two states $|u\rangle$ and $|v\rangle$ over the system X with qubits $q_0, \cdots, q_{n-1}$ are orthogonal if and only if there exists a system Y which is on the all-zero state, a unitary operation U on (Y, X), and a projective measurement $M = \{M_0, M_1\}$ such that

$$\mathcal{P}_{M=0}\left(U\left|0\cdots0, u\right\rangle\right) = \mathcal{P}_{M=1}\left(U\left|0\cdots0, v\right\rangle\right) = 1$$

Proof of necessity

- Set $Y = \emptyset$, $U = I_{2^n}$, and $M = \{\left|u\right\rangle\left\langle u\right|, I_{2^n} - \left|u\right\rangle\left\langle u\right|\}$.
- $\mathcal{P}_{M=0}\left(\left|u\right\rangle\right) = \left|\left|u\right\rangle\left\langle u|u\right\rangle\right|^2 = \left|\left|u\right\rangle\right|^2 = 1$
- $\mathcal{P}_{M=1}\left(\left|v\right\rangle\right) = \left|\left|v\right\rangle - \left|u\right\rangle\left\langle u|v\right\rangle\right|^2 = \left|\left|v\right\rangle\right|^2 = 1$

Limitation on Quantum Information

Note

Limitation on Quantum Information

Note

- When two states differs by a global phase, they cannot be distinguished

Limitation on Quantum Information

Note

- When two states differs by a global phase, they cannot be distinguished
- When two states are orthogonal, they can be perfectly distinguished

Limitation on Quantum Information

Note

- When two states differs by a global phase, they cannot be distinguished
- When two states are orthogonal, they can be perfectly distinguished
- For every pair of states in-between them, you cannot perfectly distinguish them, but you can perform some unitary operation so that the probability distribution of some measurement differs. The probability can be maximized by the **Helstrom measurement**. Please refer to the **Wikipedia** for more detail.

The End