Motivation

Quantum technologies is an exciting growing field, using quantum systems as information carriers.

* Quantum computing
  - Quadratic speedup for search
  - Exponential speedup for factoring

* Quantum Cryptography
  - True randomness
  - Provably secure communication

\+ more

Thinking like a quantum researcher

How can I use this special feature of quantum systems

Measurement disturbance

noncommutativity

Superposition

entanglement

nonlocality

no-cloning

interference

to my advantage?

Aims of course:

- Understanding basic mathematical formalism of quantum info/comp
- Explore applications of the special features of quantum systems
- Understand some physical implementations / how can we build these things?

Preliminaries (Brief)

We will only work with finite-dimensional spaces in this course.

Let $\mathbb{C}^d$ be the vector space of d-tuples in $\mathbb{C}$, i.e., $v = (v_1, v_2, \dots, v_d)$ with $v_i \in \mathbb{C}$. We can define an inner-product on $\mathbb{C}^d$ by

Complex Conjugate

Standard Euclidean dot product.

$$\langle v, w \rangle = \sum_{i=1}^{d} \overline{v_i} w_i$$

Example: Take $\mathbb{C}^2$ and $v = \begin{pmatrix} 1 \\ i \end{pmatrix}$ $w = \begin{pmatrix} 1+i \\ -1 \end{pmatrix}$ then $\langle v, w \rangle = 1 + 2i$.

The inner-product also induces a norm $\|\cdot\| : \mathbb{C}^d \to [0, \infty)$

$$\|v\| = \sqrt{\langle v, v \rangle}.$$

Ex: For $v = \begin{pmatrix} 1 \\ i \end{pmatrix}$ $\|v\| = \sqrt{1+1} = \sqrt{2}$

A basis $\{v_i\}_i$ for V is a set of linearly independent vectors that span the vector space V. I.e.,

1) $\sum_i \alpha_i v_i = 0 \iff \alpha_1 = \dots = \alpha_d = 0$ $\qquad \alpha_i \in \mathbb{C}$

2) For any $w \in V$ $\exists\, \alpha_i \in \mathbb{C}$ s.t. $w = \sum_i \alpha_i v_i$

A basis is orthonormal if in addition:

$$\langle v_i, v_j \rangle = \begin{cases} 1 & i = j \\ 0 & \text{otherwise.} \end{cases}$$

A linear operator $M : V \to W$ satisfies

$$M(\alpha v_1 + \beta v_2) = \alpha M v_1 + \beta M v_2 \qquad \forall\, v_1, v_2 \in V,\ \alpha, \beta \in \mathbb{C}$$

Linear operators between vector spaces can be represented by matrices (once bases are fixed).

Ex: Take a basis $\{e_1, \dots, e_n\}$ for V and a basis $\{f_1, \dots, f_m\}$ for W.
A linear operator M is determined by its action on basis elements.

$$Me_j = \sum_i \beta_{ij} f_i \qquad (\beta_{ji} \in \mathbb{C})$$

Writing e_i, f_i as column vectors, this action can be represented by a matrix

$$M = \begin{pmatrix} \beta_{11} & \cdots & \beta_{1n} \\ \vdots & \ddots & \\ \beta_{m1} & & \beta_{mn} \end{pmatrix}$$

f_i, e_i - column vector with 1 in ith component

For example $Me_1 = M\begin{pmatrix} 1 \\ 0 \\ \vdots \end{pmatrix} = \begin{pmatrix} \beta_{11} \\ \beta_{21} \\ \vdots \\ \beta_{m1} \end{pmatrix} = \sum_j \beta_{j1} f_j$

All bases will be orthonormal unless specified!

For a matrix A, $A^\dagger$ denotes adjoint / conjugate transpose.

$$A = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} \qquad A^\dagger = \begin{pmatrix} \overline{a_{00}} & \overline{a_{10}} \\ \overline{a_{01}} & \overline{a_{11}} \end{pmatrix}$$

It represents the unique linear operator satisfying

$$\langle v, Aw \rangle = \langle A^\dagger v, w \rangle \quad \forall\ v, w$$

We say A is:

1) Hermitian / self-adjoint if $A = A^\dagger$

2) Unitary if $AA^\dagger = A^\dagger A = \mathbb{1}$.

3) Positive semidefinite if $A = A^\dagger$ and $\langle v, Av \rangle \geq 0$
Denoted $A \geq 0$

A matrix M has an eigenvalue λ if $\exists\ v \neq 0$ such that

$$Mv = \lambda v$$

λ is called an eigenvector and v is the corresponding eigenvalue

Spectral theorem

Let M be a normal matrix $(M^\dagger M = MM^\dagger)$ acting on $\mathbb{C}^d$ then

$$M = \sum_i \lambda_i v_i v_i^\dagger$$

where λ_i are the distinct eigenvalues of M and v_i are the corresponding eigenvectors. $\{v_i\}$ form an orthonormal basis.

Eigenspaces - Span of eigenvectors associated to an eigenvalue
Eigenvectors for distinct eigenvalues are orthogonal.

Hermitian and unitary operators are both normal.
Effectively says we can find a basis in which these operators are diagonal.

The postulates of Quantum Theory

To describe a quantum system we want to understand 3 things

1) States: How do we represent the physical system mathematically?

2) Evolution: How can we transform the system? How does it evolve with time?

3) Measurement: How can we probe our system to extract information about its properties?

We'll visit each of these individually. The definitions given here are not completely general but are sufficient for this course.

Quantum States

Postulate (State)

To a quantum system A we associate a Hilbert space $\mathcal{H}_A$. Then the set of possible states of the system A corresponds to the unit vectors of $\mathcal{H}_A$.

That is, to a quantum system we can associate a Hilbert space $\mathbb{C}^d$ for some $d \in \mathbb{N}$, then the state of that system can be represented by a vector $v \in \mathbb{C}^d$ such that $\|v\| = 1$.

Example (Qubits)

A qubit is a 2 dimensional quantum system $-$ $\mathcal{H} = \mathbb{C}^2$.

- Computational basis $\quad e_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \; e_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

- Qubit state $\quad \psi = \underbrace{\alpha e_0 + \beta e_1}_{\text{super position}} \quad \alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$

Remark (Bra-Ket notation)

Quantum theorists often use Dirac notation for states, rather than writing $\psi = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ we instead write $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$. We then write $\langle\psi| = (\bar{\alpha}, \bar{\beta})$ to denote the corresponding row vector conjugated. Formally $|\psi\rangle$ should be thought of as a linear map
$$|\psi\rangle : \mathbb{C} \to \mathbb{C}^d \quad \text{and} \quad \langle\psi| : \mathbb{C}^d \to \mathbb{C}.$$
Using this notation we can write an inner product as $\langle\psi|\phi\rangle$ which previously we denoted by $\langle\psi, \phi\rangle$. Similarly we can form outer-products like $|\psi\rangle\langle\phi| : \mathbb{C}^d \to \mathbb{C}^d$ which are then matrices acting on $\mathbb{C}^d$.

Example (Qubits Continued)

Using Dirac notation we write

$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$ $\quad |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$ $\quad \{|0\rangle, |1\rangle\}$ ← Computational Basis

$|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$ $\quad |-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$ $\quad \{|+\rangle, |-\rangle\}$ ← Hadamard Basis.

Exercise

Which of the following correspond to valid quantum states?

a) $-\frac{1}{2}|0\rangle + \frac{i}{2}|1\rangle$

b) $\frac{1}{\sqrt{2}}|0\rangle + \frac{\sqrt{3}-1}{2}|+\rangle$

c) $\cos(\frac{\theta}{2})|0\rangle + e^{i\phi}\sin(\frac{\theta}{2})|1\rangle$ $\qquad \theta \in (0, 2\pi)$ $\phi \in [0, \pi]$

Remark (Global Phase)

If two states $|\psi\rangle$ $|\phi\rangle$ are such that $|\psi\rangle = e^{it}|\phi\rangle$ for some $t \in \mathbb{R}$. Then we consider these states as the same. This 'global phase' is not observable. (See exercises).

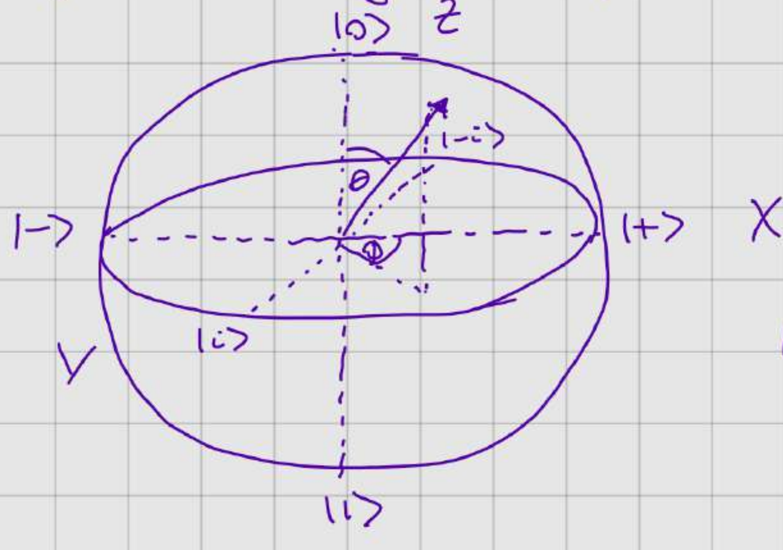
The Bloch Sphere

Because we ignore global phase differences, any single qubit can be represented as

$$\cos(\tfrac{\theta}{2})|0\rangle + \sin(\tfrac{\theta}{2})e^{i\phi}|1\rangle$$

for some $\theta \in [0, \pi]$, $\phi \in [0, 2\pi)$

These two parameters naturally form a sphere (Bloch sphere)



$|i\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}$

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

$|i\rangle$ $|-i\rangle$ are eigenvectors of $Y = \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}$

$(\cos(\phi)\sin(\theta), \sin(\phi)\sin(\theta), \cos(\theta))$.

Nice Geometrical picture to build intuition.

Evolution

Def^n (Unitary operator)

A unitary operator is a linear operator $U: \mathcal{H} \to \mathcal{H}$ such that

Hilbert space

$$U^* U = U U^* = \mathbb{1}.$$

Note that such an operator preserves inner products

$$(\langle\psi|U^*)(U|\phi\rangle) = \langle\psi|U^* U|\phi\rangle = \langle\psi|\phi\rangle$$

Postulate (Evolution)

Not interacting with an external system / environment

The evolution of a closed quantum system is described by a unitary transformation. I.e. if the initial state of the system is $|\psi\rangle$ and the system later evolves to $|\phi\rangle$, then $\exists$ a unitary operator U such that $|\phi\rangle = U|\psi\rangle$

Examples (Qubit systems)

Quick exercise: Verify these are unitary matrices.

Pauli Matrices

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Bit flip operator

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

phase flip operator

$$Z(|0\rangle + |1\rangle) = |0\rangle - |1\rangle$$

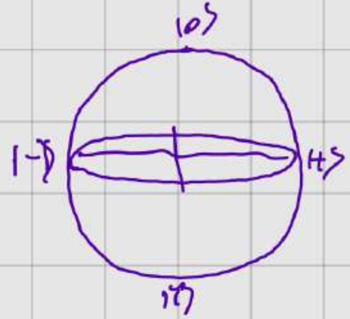
Hadamard Gate

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

Basis change from $\{|0\rangle, |1\rangle\}$ to $\{|+\rangle, |-\rangle\}$

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

Rotations



Remark (Physical Evolution)

From a physics perspective the system evolves according to the Schrödinger equation

$$i\hbar \frac{d}{dt} |\psi(t)\rangle = \tilde{H} |\psi(t)\rangle$$

Plancks constant

Hamiltonian

Hermitian operator

This has a solution $|\psi(t)\rangle = e^{-iHt/\hbar} |\psi(0)\rangle$

Unitary operator...

Measurements

Def^n (Projector)

A projector P is a Hermitian operator satisfying $P^2 = P$.

Idempotent

The term 'projector' is because it is projecting onto some subspace of the Hilbert space.

Exercise: Let P be a projector verify

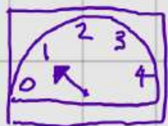
1) Its eigenvalues belong to $\{0,1\}$.
2) It projects onto the subspace
   $\text{span}\{|v_i\rangle : |v_i\rangle \text{ is an eigenvector of } P \text{ with eigenvalue } 1\}$

Examples

The following are all projectors

1) $\mathbb{1}$ ← projects onto entire space
2) $|0\rangle\langle 0|$ ← projects onto $\text{span}\{|0\rangle\}$
3) $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ ← projects onto $\text{span}\{|0\rangle, |1\rangle\}$

To extract information from a quantum system we need to perform a measurement

$|\psi\rangle \longrightarrow$  $\longrightarrow |\phi_x\rangle$

set of possible outcomes

We give our state to the measurement device, we receive so outcome $x \in \mathcal{X}$ probabilistically and our state is transformed depending on the outcome.

Postulate (Measurement)

Let A be a quantum system with associated Hilbert space $\mathcal{H}_A$. A measurement of A corresponds to a set $\{P_x\}_{x\in\mathcal{X}}$ of projection operators acting on $\mathcal{H}_A$ such that $\sum_{x\in\mathcal{X}} P_x = \mathbb{1}$. ($\mathcal{X}$ is the set of possible outcomes of the measurement).

If the system A is in state $|\psi\rangle$, then the probability that the measurement returns the outcome $x \in \mathcal{X}$ is given by

$$\mathbb{P}(x) = \langle\psi|P_x|\psi\rangle$$

and if we receive outcome $x \in \mathcal{X}$ the state of the system becomes

$$|\phi_x\rangle = \frac{P_x|\psi\rangle}{\|P_x|\psi\rangle\|}.$$

Example

Let $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. We'll 'measure in the basis' $\{|0\rangle, |1\rangle\}$. We define projectors

$$P_0 = |0\rangle\langle 0| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$
$$P_1 = |1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Can check $P_0 + P_1 = \mathbb{1}$. Then

$$P(0) = \langle\psi|P_0|\psi\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$
$$= \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \end{pmatrix}$$
$$= \frac{1}{2}.$$

Let $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Now we measure in the Hadamard basis $\{|+\rangle, |-\rangle\}$. (Recall $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$). Let $P_+ = |+\rangle\langle +|$

$$\mathbb{P}(+) = \langle\psi|P_+|\psi\rangle = \underbrace{\langle +|+\rangle}_{1}\underbrace{\langle +|+\rangle}_{1}$$
$$= 1$$

Can measure in any ONB $\{|v_i\rangle\}_i$ by defining projectors
$$P_i = |v_i\rangle\langle v_i|.$$

Exercise: Prove that this defines a valid measurement.

Def^n (Observable)

Suppose the outcomes of a measurement $\{P_{\alpha_i}\}_i$ are real. We can define an expectation operator $M = \sum_i \alpha_i P_{\alpha_i}$ called an observable.

Expectation:
$$\langle\psi|M|\psi\rangle = \sum_i \alpha_i \langle\psi|P_{\alpha_i}|\psi\rangle$$
$$= \sum_i \alpha_i \, \mathbb{P}[\alpha_i] = \mathbb{E}[\text{Measurement}]$$

Any Hermitian operator can be seen as an observable. By spectral theorem
$$M = \sum_i \lambda_i P_{\lambda_i} \leftarrow \text{Projector onto eigenspace}$$

Eigenvalues are real

$\{P_{\lambda_i}\}$ form a measurement.

Ex: $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|$

Eigenvalues $\{+1, -1\}$ Eigenvectors $\{|0\rangle, |1\rangle\}$. Projectors $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$

$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = |+\rangle\langle +| - |-\rangle\langle -|$

Eigenvalues $\{+1, -1\}$ Eigenvectors $\{|+\rangle, |-\rangle\}$ Projectors $\{|+\rangle\langle +|, |-\rangle\langle -|\}$

Remark (Distinguishing states)

Suppose we are sent either a state $|\psi_0\rangle$ or a state $|\psi_1\rangle$ Is it possible to determine which state we are sent w/o errors? I.e., can we define a measurement $\{M_0, M_1\}$ such that

$$\mathbb{P}(0 \mid |\psi_0\rangle) = 1 \quad \text{and} \quad ?$$
$$\mathbb{P}(1 \mid |\psi_1\rangle) = 1$$

Case 1: $\langle \psi_0 | \psi_1 \rangle = 0$

Define $M_0 = |\psi_0\rangle\langle \psi_0|$ $\quad M_1 = \mathbb{1} - |\psi_0\rangle\langle\psi_0|$

$$\mathbb{P}(0 \mid |\psi_0\rangle) = \langle \psi_0 | M_0 | \psi_0 \rangle = \underbrace{\langle \psi_0 | \psi_0 \rangle}_{1} \underbrace{\langle \psi_0 | \psi_0 \rangle}_{1} = 1$$

$$\begin{aligned} \mathbb{P}(1 \mid |\psi_0\rangle) = \langle \psi_1 | M_1 | \psi_1 \rangle &= \langle \psi_1 | \mathbb{1} - |\psi_0\rangle\langle\psi_0| \, |\psi_1\rangle \\ &= \langle \psi_1 | \psi_1 \rangle - \underbrace{\langle \psi_1 | \psi_0 \rangle\langle \psi_0 | \psi_1 \rangle}_{0} \\ &= 1 \end{aligned}$$

Case 2: $\langle \psi_0 | \psi_1 \rangle \neq 0$

As $\langle \psi_0 | \psi_1 \rangle \neq 0$ we can write $|\psi_1\rangle = \alpha |\psi_0\rangle + \beta |\psi_0^{\perp}\rangle$ where $|\psi_0\rangle \perp |\psi_0^{\perp}\rangle$.

Now suppose we have a measurement $\{M_0, M_1\}$ that distinguishes perfectly. Then

$$\langle\psi_1|M_1|\psi_1\rangle = 1 \quad \text{and} \quad \langle\psi_0|M_1|\psi_0\rangle = 0$$

The latter implies $M_1|\psi_0\rangle = 0$ (as M_1 is projective) and so

$$\begin{aligned}\langle\psi_1|M_1|\psi_1\rangle &= \left(\bar{\alpha}\langle\psi_0| + \bar{\beta}\langle\psi_0^\perp|\right) M_1 \left(\alpha|\psi_0\rangle + \beta|\psi_0^\perp\rangle\right) \\ &= \underbrace{|\beta|^2}_{\leq 1} \underbrace{\langle\psi_0^\perp|M_1|\psi_0^\perp\rangle}_{\leq 1} \\ &\leq |\beta|^2\end{aligned}$$

But $\Rightarrow$ we must have $|\beta|^2 = 1$ and so $|\alpha|^2 = 0$ and $\langle\psi_0|\psi_1\rangle = 0$ $\boxtimes$

Why doesn't it help if we first transform the states by some unitary i.e., distinguish $U|\psi_0\rangle$ and $U|\psi_1\rangle$?

Exercise

Find the best projective measurement from the Z–X plane of the bloch sphere that distinguishes $|\psi_0\rangle = |0\rangle$ from $|\psi_1\rangle = |+\rangle$.
I.e., find a measurement from the set

$$M_0 = \frac{\mathbb{1} + \cos(\theta) Z + \sin(\theta) X}{2} \qquad M_1 = \mathbb{1} - M_0$$

that maximizes the probability of success, $\frac{1}{2}\left(P(0||\psi_0\rangle) + P(1||\psi_1\rangle)\right)$

Try to interpret this geometrically on the Bloch sphere.

Single system applications:

A QRNG:

Already we have enough to give a basic application 'a random bit generator'.

1) Prepare qubit $|+\rangle = \begin{pmatrix}\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}}\end{pmatrix}$
2) Measure in $\{|0\rangle, |1\rangle\}$ basis.

$$\mathbb{P}(0) = \langle +|0\rangle\langle 0|+\rangle = \frac{1}{2} = \mathbb{P}(1)$$

Quantum Money: Bank notes can be forged...

What if we give them a 'quantum' serial number?

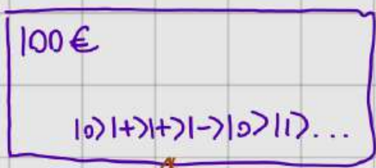
Suppose you receive state $|0\rangle$, $|1\rangle$, $|+\rangle$ or $|-\rangle$

If you receive state $|0\rangle$ or $|+\rangle$ answer 0

$|1\rangle$ or $|-\rangle$ answer 1.

If you know the basis information $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$.
Then easy (distinguishable).

If you don't know then you may measure in the wrong basis and return the wrong answer! ← Measuring destroys information!



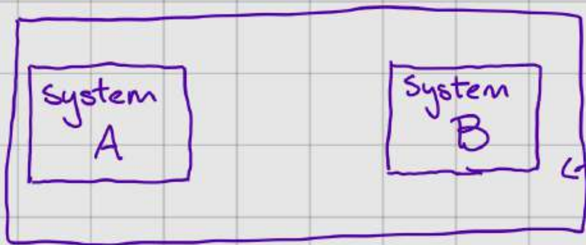
Bank knows basis information but you don't...

Bank can verify by measuring in correct basis

You cannot!

Multiple Systems

What if we want to describe 2 qubits or n-qubits?



← System AB ?

Def^n (Joint Systems)

Let system A (resp. B) be associated with the Hilbert space $\mathcal{H}_A$ (resp. $\mathcal{H}_B$) then the joint system (denoted AB) is associated with the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$

Remark (Tensor Product)

Given two Hilbert spaces V, W (over $\mathbb{C}$) we can form a new Hilbert space $V \otimes W$ in the following way. Take a basis $\{|v_i\rangle\}_i$ for V and a basis $\{|w_i\rangle\}_i$ for W. Then

$$V \otimes W = \mathrm{Span}\{ |v_i\rangle \otimes |w_j\rangle : \forall\, i,j \}$$

where $\otimes : V \times W \to V \otimes W$ is <u>bilinear</u> i.e.

$$(\alpha v_1 + \beta v_2) \otimes (\gamma w_1 + \delta w_2) = \alpha\gamma\, v_1 \otimes w_1 + \alpha\delta\, v_1 \otimes w_2 + \beta\gamma\, v_2 \otimes w_1 + \beta\delta\, v_2 \otimes w_2$$

The inner product on $V \otimes W$ is defined via

$$\left(\langle v_1| \otimes \langle w_1|\right)\left(|v_2\rangle \otimes |w_2\rangle\right) = \langle v_1|v_2\rangle\langle w_1|w_2\rangle$$

Note $\mathbb{C}^n \otimes \mathbb{C}^m \cong \mathbb{C}^{nm}$. We can use the Kronecker product when working with explicit vectors and matrices.

Let $v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in \mathbb{C}^n \quad w = \begin{pmatrix} w_1 \\ \vdots \\ w_m \end{pmatrix} \in \mathbb{C}^m$ then

$$v \otimes w = \begin{pmatrix} v_1 w \\ v_2 w \\ \vdots \\ v_n w \end{pmatrix} = \begin{pmatrix} v_1 w_1 \\ v_1 w_2 \\ \vdots \\ v_1 w_m \\ v_2 w_1 \\ v_2 w_2 \\ \vdots \\ v_n w_n \end{pmatrix} \updownarrow \text{size } nm \text{ vector}$$

We can also take the tensor product of matrices.
Let

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$$ be an $m \times n$ matrix

and $B = \begin{pmatrix} b_{11} & \cdots & b_{1q} \\ \vdots & \ddots & \vdots \\ b_{p1} & \cdots & b_{pq} \end{pmatrix}$ be a $p \times q$ matrix.

Then

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix}$$

$$= \begin{pmatrix} \begin{matrix} a_{11}b_{11} & \cdots & a_{11}b_{1q} \\ \vdots & \ddots & \vdots \\ a_{11}b_{p1} & \cdots & a_{11}b_{pq} \end{matrix} & \cdots & \begin{matrix} a_{1n}b_{11} & \cdots & a_{1n}b_{1q} \\ \vdots & \ddots & \vdots \\ a_{1n}b_{p1} & \cdots & a_{1n}b_{pq} \end{matrix} \\ \vdots & \ddots & \vdots \\ & \cdots & \begin{matrix} a_{mn}b_{11} & \cdots & a_{mn}b_{1q} \\ \vdots & \ddots & \\ & & a_{mn}b_{pq} \end{matrix} \end{pmatrix}$$

which is a $mp \times nq$ matrix.

Example

1) $|0\rangle \otimes |+\rangle = |0\rangle \otimes \left(\frac{1}{\sqrt{2}}|0\rangle + |1\rangle\right) = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ 0 \\ 0 \end{pmatrix}$

2) $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$$Z \otimes X = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{pmatrix}$$

Properties

1) (Bilinear) $(\alpha A_1 + \beta A_2) \otimes B = \alpha A_1 \otimes B + \beta A_2 \otimes B$

$$A \otimes (\alpha B_1 + \beta B_2) = \alpha A \otimes B_1 + \beta A \otimes B_2$$

2) (Products) $(A \otimes B)(C \otimes D) = AC \otimes BD$

3) (Adjoint) $(A \otimes B)^{\dagger} = A^{\dagger} \otimes B^{\dagger}$ (conjugate transpose)

Notation

We will use shorthand notation for a bitstring

$$|x_1 x_2 \dots x_n\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \dots \otimes |x_n\rangle$$
$$= |x_1\rangle |x_2\rangle \dots |x_n\rangle$$

Eg. $\underline{x} = x_1 \dots x_n$ could be a bit string then $|x_1 \dots x_n\rangle$ is a state where qubit i is in the state x_i.

Example

Consider an n-qubit system $\left(\overbrace{\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \dots \otimes \mathbb{C}^2}^{n\text{-times}} \cong \mathbb{C}^{2^n} \right) = \left(\mathbb{C}^2\right)^{\otimes n}$

1) $|0 \dots 0\rangle$ valid state

2) $2^{-n/2} \sum_{\underline{x} \in \{0,1\}^n} |\underline{x}\rangle = |+\rangle \otimes |+\rangle \otimes \dots \otimes |+\rangle \equiv |+\rangle^{\otimes n}$

Because $\mathbb{C}^n \otimes \mathbb{C}^m \cong \mathbb{C}^{nm}$ we can treat it as a composition of two smaller systems or one large system.

Qubit A

Qubit B

If we describe joint system by $\mathbb{C}^2 \otimes \mathbb{C}^2$. Suppose it is in a state

$|\psi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$. If A and B are isolated from each other then applying a unitary U_A to system A corresponds to

$$(U_A \otimes \mathbb{1})|\psi\rangle \qquad \text{(Similarly for B)}$$

If we apply U_B to system B also, then we end up with

$$(U_A \otimes U_B)|\psi\rangle.$$

If we bring the systems together however (allow them to interact) then we can get more interesting transformations. Mathematically, $\mathcal{U}(\mathcal{H}_A \otimes \mathcal{H}_B) \supset \mathcal{U}(\mathcal{H}_A) \otimes \mathcal{U}(\mathcal{H}_B)$.

local operations.

$\mathcal{U}(\mathcal{H})$ - set of unitary operators acting on $\mathcal{H}$.

Example (CNOT)

$$C_{NOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

cannot be written as $U \otimes V$ for some $U, V \in \mathcal{U}(\mathbb{C}^2)$.

Proof

Let $U = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix}$ $V = \begin{pmatrix} v_{11} & v_{12} \\ v_{21} & v_{22} \end{pmatrix}$

Then $$U \otimes V = \begin{pmatrix} u_{11}v_{11} & u_{11}v_{12} & u_{12}v_{11} & u_{12}v_{12} \\ u_{11}v_{21} & u_{11}v_{22} & u_{12}v_{21} & u_{12}v_{22} \\ u_{21}v_{11} & u_{21}v_{12} & u_{22}v_{11} & u_{22}v_{12} \\ u_{21}v_{21} & u_{21}v_{22} & u_{22}v_{21} & u_{22}v_{22} \end{pmatrix}$$

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

$\Rightarrow$ Either $V = 0$ (trivial)

Or $u_{12} = 0$

$\Rightarrow u_{21} = 0$

$$\Rightarrow U = \begin{pmatrix} u_{11} & 0 \\ 0 & u_{22} \end{pmatrix} \Rightarrow U \otimes V = \begin{pmatrix} u_{11}v_{11} & u_{11}v_{12} & & \\ u_{11}v_{21} & u_{11}v_{22} & & \\ & & u_{22}v_{11} & u_{22}v_{12} \\ & & u_{22}v_{21} & u_{22}v_{22} \end{pmatrix}$$

By 1st block we need $V_{12} = V_{21} = 0$

But $\Rightarrow$ 2nd block of form $\begin{pmatrix} U_{22}V_{11} & 0 \\ 0 & U_{22}V_{22} \end{pmatrix}$

which does not work...

<u>Exercise</u> For U, V unitary matrices show
1) UV is unitary
2) $U \otimes V$ is unitary.

<u>No cloning principle</u>
You cannot build a universal cloner for quantum information.
I.e., there does not exist a unitary U that maps

$$|\psi\rangle \otimes |0\rangle \longmapsto |\psi\rangle \otimes |\psi\rangle \quad \text{for all } |\psi\rangle.$$

<u>Proof</u>
Suppose such a U exists. Let $|\psi\rangle$ and $|\phi\rangle$ be two quantum states such that $\langle\psi|\phi\rangle \neq 0$. Then

$$U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle \quad \text{and}$$
$$U|\phi\rangle|0\rangle = |\phi\rangle|\phi\rangle$$

But

$$\begin{aligned}\langle\phi|\psi\rangle\langle\phi|\psi\rangle &= (\langle\phi|\langle\phi|)(|\psi\rangle|\psi\rangle) \\ &= (\langle\phi|\langle 0|U^{\dagger})(U|\psi\rangle|0\rangle) \\ &= (\langle\phi|\langle 0|)(|\psi\rangle|0\rangle) \\ &= \langle\phi|\psi\rangle\end{aligned}$$

only valid if $\langle\phi|\psi\rangle^2 = \langle\phi|\psi\rangle$

i.e. $\in \{0, 1\}$ $\leftarrow$ $|\phi\rangle = |\psi\rangle$

orthogonal

$\boxtimes$

$\therefore$ Only sets of orthogonal states can be cloned.

Analogous happenings for measurements.

Suppose we have an n-qubit system, we can measure the k^{th} qubit (with a measurement $\{P_i\}$) by using the global measurement

$$\{\mathbb{1} \otimes \mathbb{1} \otimes \ldots \otimes \mathbb{1} \otimes \underset{\swarrow k^{th}\text{ qubit}}{P_i} \otimes \mathbb{1} \otimes \ldots \otimes \mathbb{1}\}_i$$

Like in the case of transformations there are measurements not in tensor product form.

Example

Let

$$|\psi\rangle = \frac{1}{\sqrt{3}}(|00\rangle + |01\rangle + |10\rangle)$$

We measure the 1st qubit in the computational basis.

Output	Probability	Post-measurement state
0	$2/3$	$\frac{1}{\sqrt{2}}(\lvert 00\rangle + \lvert 01\rangle)$
1	$1/3$	$\lvert 10\rangle$

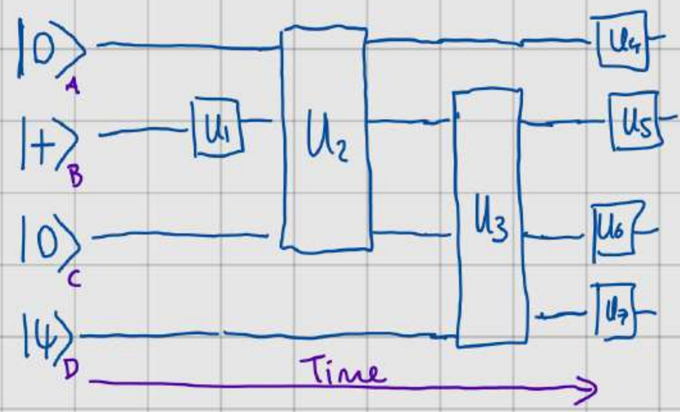
Summary

* States - Unit vectors in Hilbert space
* Evolution - Unitary operators
* Measurement - Projection operators resolving the identity.
  State collapses to

$$\frac{P_i|\psi\rangle}{\|P_i|\psi\rangle\|}$$

Quantum Circuits

Quantum circuits consist of wires (states), gates (unitaries) and measurements



This circuit translates to

$$(\underset{A}{U_4}\otimes\underset{B}{U_5}\otimes\underset{C}{U_6}\otimes\underset{D}{U_7})(\underset{A}{\mathbb{1}}\otimes\underset{BCD}{U_3})(\underset{ABC}{U_2}\otimes\underset{D}{\mathbb{1}})(\underset{A}{\mathbb{1}}\otimes\underset{B}{U_1}\otimes\underset{C}{\mathbb{1}}\otimes\underset{D}{\mathbb{1}})(\underset{A}{|0\rangle}\otimes\underset{B}{|+\rangle}\otimes\underset{C}{|0\rangle}\otimes\underset{D}{|\psi\rangle})$$

We can also measure various systems in this circuit to read out information about our computation

Common gates (single qubit)

$$X=\begin{pmatrix}0&1\\1&0\end{pmatrix}\qquad Y=\begin{pmatrix}0&-i\\i&0\end{pmatrix}\qquad Z=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$$

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad R_\phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$$

Controlled operations

Suppose we want to implement a gate on qubit 2 that depends on the value of qubit 1. Example CNOT

$$\text{CNOT}: \; |0\rangle|b\rangle \mapsto |0\rangle|b\rangle \qquad b \in \{0,1\}.$$
$$|1\rangle|b\rangle \mapsto |1\rangle|b \oplus 1\rangle$$

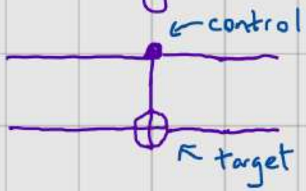
This is given by the unitary

$$\text{CNOT} = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes X$$

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

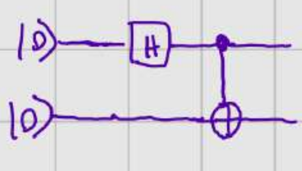
Relate back to no-cloning

In circuit diagrams we represent this gate as

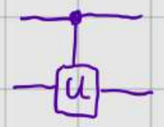


Exercise: Verify that CNOT is unitary. (Using bra-ket form)

Exercise: Compute the output of



More generally we can control any gate



$$= |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes U$$

You can also control on multiple wires

CCNOT (Toffoli) →

$$= \left(|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10|\right) \otimes \mathbb{1} + |11\rangle\langle 11| \otimes X$$

↑ Apply X only when both control qubits are 1

<u>Exercise</u>

Construct the quantum gate that swaps 2 qubits. I.e. for qubit states $|\psi\rangle$ and $|\phi\rangle$ we have

$$U|\psi\rangle|\phi\rangle = |\phi\rangle|\psi\rangle$$

Universal Gate sets

We want to decompose arbitrary unitaries into products of simpler unitaries.

We say a set $G = \{U_1, U_2, \ldots\}$ is universal if any unitary operation can be approximated (to arbitrary accuracy) by a circuit involving only those gates. More formally let

$$\mathrm{Error}(\underset{\substack{\uparrow \\ \text{target unitary}}}{U}, V) := \max_{|\psi\rangle} \| (U - V)|\psi\rangle \| \qquad \leftarrow \text{implemented unitary.}$$

Then G is universal if for every unitary U and $\varepsilon > 0$ $\exists$ a circuit V built from G such that

$$\mathrm{Error}(U, V) \leq \varepsilon.$$

Lemma (Small Error $\Rightarrow$ accurate statistics)

Let $|\psi\rangle$ be a state, M be a projector and U, V be unitaries. Let $P_U = \langle\psi|U^\dagger M U|\psi\rangle$ and $P_V = \langle\psi|V^\dagger M V|\psi\rangle$. Then

$$|P_U - P_V| \leq 2\,\mathrm{Error}(U,V).$$

Proof

$$\begin{aligned}
|P_U - P_V| &= |\langle\psi| U^\dagger M U - V^\dagger M V |\psi\rangle| \\
&= |\langle\psi| U^\dagger M U - U^\dagger M V + U^\dagger M V - V^\dagger M V |\psi\rangle \\
&= |\langle\psi| U^\dagger M (U-V)|\psi\rangle + \langle\psi|(U^\dagger - V^\dagger) M V|\psi\rangle| \\
\text{triangle inequality} \quad &\leq |\langle\psi| U^\dagger M (U-V)|\psi\rangle| + |\langle\psi|(U^\dagger - V^\dagger) M V|\psi\rangle| \\
\text{Cauchy-Schwarz} \quad &\leq \underbrace{\| M U|\psi\rangle\|}_{\leq 1} \, \|(U-V)|\psi\rangle\| + \|(U-V)|\psi\rangle\| \, \underbrace{\| M V|\psi\rangle\|}_{\leq 1} \\
&\leq 2\,\mathrm{Error}(U,V)
\end{aligned}$$

$\boxtimes$

Thus a low error $\Rightarrow$ accurate measurement results!

Th^m (A universal set)

Quite surprising 2 qubits & finite!

The set $G = \{H, C_{NOT}, T\}$ is universal for quantum computation, where

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad C_{NOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

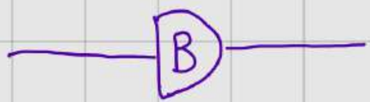
Proof (See Nielsen & Chuang)

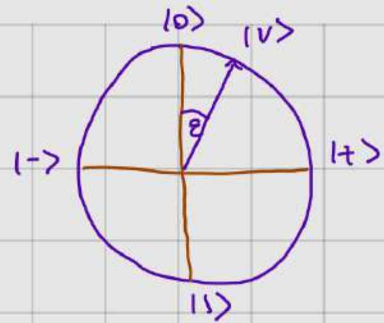
1) Induction - Unitaries acting nontrivially on 2 dimensional subspaces are universal

2) Single qubit unitaries + C_{NOT} can construct all 2-level unitaries

3) $\{T, H\}$ can approximate all single qubit unitaries.

The Elitzur-Vaidman Bomb



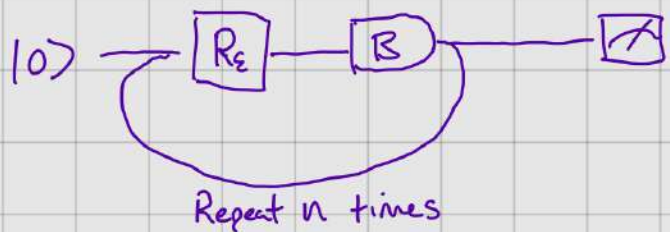


↑ Bomb will measure in $\{|0\rangle, |1\rangle\}$ basis.

Outcome $|0\rangle$ it outputs $|0\rangle$

Outcome $|1\rangle$ it explodes.

Question: Can you detect the presence of a bomb w/o it exploding? Yes!



$$R_\varepsilon = \begin{pmatrix} \cos(\varepsilon) & \sin(\varepsilon) \\ -\sin(\varepsilon) & \cos(\varepsilon) \end{pmatrix}$$

$$\varepsilon = \frac{\pi}{2n}$$

Case 1: (No bomb)

Qubit evolves to
$$R_\varepsilon^n |0\rangle = \cos(n\varepsilon)|0\rangle + \sin(n\varepsilon)|1\rangle$$
$$= \underbrace{\cos\left(\frac{\pi}{2}\right)}_{0}|0\rangle + \underbrace{\sin\left(\frac{\pi}{2}\right)}_{1}|1\rangle$$

Outcome 1 with certainty.

Case 2: (Bomb)

Each round qubit $|0\rangle \longmapsto \cos(\varepsilon)|0\rangle + \sin(\varepsilon)|1\rangle$

Probability of exploding is $\sin^2(\varepsilon) \approx \varepsilon^2$

Probability of not exploding after n rounds
$$\cos^{2n}(\varepsilon) \approx 1 - 2n\varepsilon^2$$
$$= 1 - \frac{\pi^2}{2n}$$

Can be made arbitrarily close to 1!

State measured at end is $|0\rangle$.