LECTURE 2

Quantum state : A state of being in superposition of N classical states, $|0\rangle, \ldots, |N-1\rangle$

$$|\phi\rangle = \alpha_0 |0\rangle + \ldots + \alpha_{N-1} |N-1\rangle = \begin{bmatrix} \alpha_0 \\ \vdots \\ \alpha_{N-1} \end{bmatrix}$$

Superposition: Being in all N states at the same time

$|0\rangle, \ldots, |N-1\rangle$: names given to the N states.
(the numbers $0, \ldots, N-1$ are not important)

$\alpha_i \in \mathbb{C}$: amplitude on state "i", measure of how much the superposition looks like $|i\rangle$

The quantum state is represented as an N dimensional vector and the corresponding N classical states form an orthonormal basis

$$|i\rangle = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \leftarrow \text{i-th position}$$

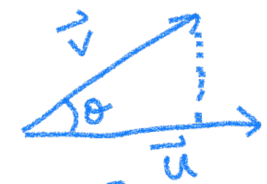
NOTE : $\begin{bmatrix} \alpha_0 \\ \vdots \\ \vdots \\ \alpha_{N-1} \end{bmatrix} = \sum_{i=0}^{N-1} \alpha_i |i\rangle$

INNER PRODUCT (Real Vectors)

Unit vector : $\vec{v}$ s.t. $\|\vec{v}\|^2 = \langle \vec{v}, \vec{v} \rangle = 1.$

$\langle \vec{u}, \vec{v} \rangle$ means (length of $\vec{u}$) $\times$ (length of $\vec{v}$'s projection on $\vec{u}$)

$= (\|\vec{u}\|) \cdot (\|\vec{v}\| \cos\theta)$



$= u_1 v_1 + \cdots + u_d v_d = [u_1 \ldots u_d] \begin{bmatrix} v_1 \\ \vdots \\ v_d \end{bmatrix} = \vec{u}^T \vec{v}$

INNER PRODUCT (COMPLEX VECTORS)

We still want $\langle \vec{v}, \vec{v} \rangle = \|\vec{v}\|^2 = \sum_i |v_i|^2$

Define $\langle \vec{u}, \vec{v} \rangle := u_1^* v_1 + \dots + u_d^* v_d$

$$= \begin{bmatrix} u_1^* & u_2^* & \dots & u_d^* \end{bmatrix} \begin{bmatrix} v_1 \\ \vdots \\ v_d \end{bmatrix}$$

Conjugate

$\vec{u}^\dagger$: conjugate transpose of $\vec{u} = [u_1^* \dots u_d^*]$

Let u be $3+4i$

u^* is $3-4i$

$u.u^* = |u|^2 = 3^2+4^2$

Dirac's Bra Ket Notation

In high school $\hat{i} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$ $\hat{j} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$ $\hat{k} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$

Linear Algebra $e_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \end{bmatrix}$ $e_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \end{bmatrix}$, $e_3 = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ \vdots \end{bmatrix}$

Quantum Computing $|0\rangle = \begin{bmatrix} 1 \\ 0 \\ \vdots \end{bmatrix}$ $|1\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \end{bmatrix}$, $|2\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ \vdots \end{bmatrix}$

DIRAC'S BRA KET NOTATION

$|\vec{v}\rangle$ is a column vector $\begin{bmatrix} v_1 \\ \vdots \\ v_d \end{bmatrix} \in \mathbb{C}^d$

$\langle\vec{v}| :=$ Conjugate transpose of $\vec{v}$

ie. row vector $[v_1^* \ v_2^* \ \cdots \ v_d^*]$

read as bra $\vec{v}$.

$\langle\vec{u}|.|\vec{v}\rangle = \vec{u}^\dagger \vec{v} = \langle u|v\rangle$ ← notational shorthand

Example

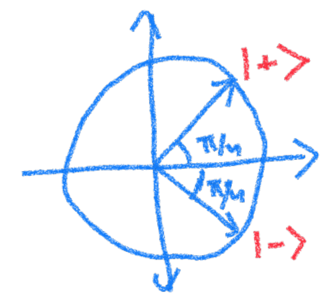
$$|\vec{v}\rangle = \frac{1}{13}\begin{bmatrix} (3+4i) \\ 12i \end{bmatrix}$$

$$\langle\vec{v}| = \frac{1}{13}\begin{bmatrix} 3-4i & -12i \end{bmatrix}$$

$|+\rangle$ and $|-\rangle$

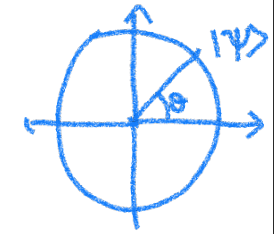
$$|+\rangle = \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$|-\rangle = \begin{bmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{bmatrix} = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$



These quantum states will be used a lot

$$|\psi\rangle = \begin{bmatrix} \cos\theta \\ \sin\theta \end{bmatrix} = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle$$



$$P_r\left[\text{measuring } |0\rangle\right] = (\cos\theta)^2$$
$$= |\langle 0|\psi\rangle|^2 \leftarrow$$

Also true for complex amplitudes

$$P_r\left[\text{measuring } |1\rangle\right] = (\sin\theta)^2$$
$$= |\langle 1|\psi\rangle|^2$$

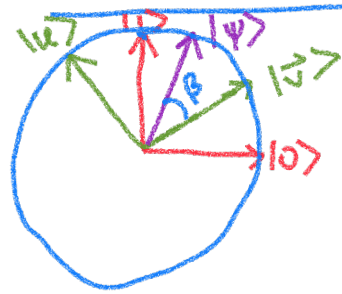
Basis of a quantum system

For a quantum system in d dimensions, any set of d states $|u_1\rangle, \ldots, |u_d\rangle$ is called a basis if the states are orthonormal i.e.

$$\langle u_i | u_i \rangle = 1 \quad \text{and} \quad \langle u_i | u_j \rangle = 0$$

by default for any valid quantum state.

Measuring in a different "basis"



$$|\psi\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$$

If we measure $|\psi\rangle$ in the basis $\{|\vec{u}\rangle, |\vec{v}\rangle\}$ we get

$|\vec{u}\rangle$ with probability $|\langle u|\psi\rangle|^2$
$= \sin^2\beta$

$|\vec{v}\rangle$ with probability $|\langle v|\psi\rangle|^2$
$= \cos^2\beta$

Example

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \qquad \times \tfrac{1}{\sqrt{2}}$$

$$|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \qquad \times \tfrac{1}{\sqrt{2}}$$

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

If we measure in $|+\rangle$, $|-\rangle$ basis, we get $|+\rangle$ w.p. $1/2$ and $|-\rangle$ w.p. $1/2$

In general

$$|\psi\rangle = \begin{bmatrix} \alpha_0 \\ \vdots \\ \vdots \\ \alpha_{d-1} \end{bmatrix} = \alpha_0|0\rangle + \ldots\ldots + \alpha_{d-1}|d-1\rangle$$

For any orthonormal basis $\{|u_0\rangle, \ldots\ldots, |u_{d-1}\rangle\}$

$$|\psi\rangle = \beta_0|u_0\rangle + \ldots\ldots + \beta_{d-1}|u_{d-1}\rangle$$

$$\beta_0 = \langle\psi|u_0\rangle, \quad \beta_1 = \langle\psi|u_1\rangle, \ldots\ldots$$

$|\psi\rangle$ —— $\boxed{\text{Measure in the basis } \{|u_0\rangle, \dots, |u_{d-1}\rangle\}}$

$|u_i\rangle$ w.p. $|\beta_i|^2 = |\langle u_i|\psi\rangle|^2$

Example:

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$$

we want to express $|\psi\rangle$ in the basis $|u\rangle, |v\rangle$

where $|u\rangle = \begin{bmatrix} 3/5 \\ 4/5 \end{bmatrix}$, $|v\rangle = \begin{bmatrix} 4/5 \\ -3/5 \end{bmatrix}$ Is this a basis?

$$|\psi\rangle = \beta_0 |u\rangle + \beta_1 |v\rangle \quad \Bigg| \quad \begin{aligned} \beta_0 &= \frac{3}{5}\alpha_0 + \frac{4}{5}\alpha_1 \\ \beta_1 &= 4/5\, \alpha_0 - \frac{3}{5}\alpha_1 \end{aligned}$$

APPLICATION: ELITZUR-VAIDMAN BOMB

Suppose you are given a box that does one of the following

Measure in $\{|0\rangle, |1\rangle\}$

If $|0\rangle$ then output $|0\rangle$

If $|1\rangle$ then BOMB EXPLODES.

Figure out which box we are given without explosion!

Classical ideas:

Send $|\psi\rangle = |0\rangle$

$= |1\rangle$

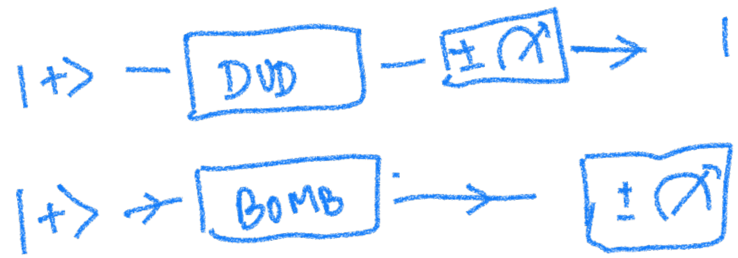
Ideas: Send $|+\rangle$

Send $i|0\rangle$

Quantum idea.

Send $|\psi\rangle = |+\rangle$

Measure in $\{|+\rangle, |-\rangle\}$



$|+\rangle$ w.p. 1

$\Pr[\text{Explosion}] = 1/2$

$\Pr[\text{Output } |+\rangle] = 1/4$

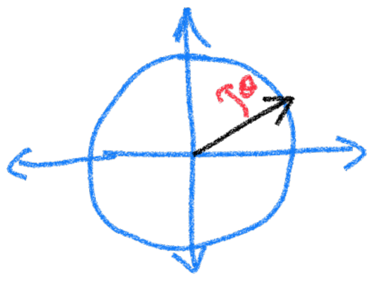
$\Pr[\quad " \quad |-\rangle] = 1/4$

Can we improve this?

- We will take a detour and talk about operations we can perform on quantum states

ROTATION:

FACT: For any θ, we can build a physical device that "rotates a qubit by angle θ".



$$|0\rangle \longrightarrow \begin{bmatrix} \cos\theta \\ \sin\theta \end{bmatrix}$$

$$|1\rangle \longrightarrow \begin{bmatrix} \cos(\pi/2+\theta) \\ \sin(\pi/2+\theta) \end{bmatrix} = \begin{bmatrix} -\sin\theta \\ \cos\theta \end{bmatrix}$$

$\alpha|0\rangle + \beta|1\rangle$ gets transformed to $\alpha\begin{bmatrix}\cos\theta\\ \sin\theta\end{bmatrix} + \beta\begin{bmatrix}-\sin\theta\\ \cos\theta\end{bmatrix}$

$$= \begin{bmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{bmatrix}\begin{bmatrix}\alpha\\ \beta\end{bmatrix}$$

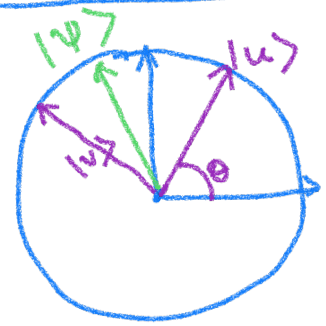
$\begin{bmatrix}1\\ 0\end{bmatrix}$ goes to this vector

$\begin{bmatrix}0\\ 1\end{bmatrix}$ goes to this vector

$|\psi\rangle$ gets transformed to $R_\theta|\psi\rangle$, $R_\theta = \begin{bmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{bmatrix}$

- α and β may be complex numbers.
- Viewing R_θ as a rotation might only be intuitive for real amplitudes.

Measuring in $|u\rangle, |v\rangle$ basis via rotation



$$|u\rangle = R_\theta |0\rangle$$
$$|v\rangle = R_\theta |1\rangle$$

$$|\psi\rangle = \alpha |u\rangle + \beta |v\rangle$$
$$= \alpha . R_\theta |0\rangle + \beta . R_\theta |1\rangle$$

How to measure in $|u\rangle, |v\rangle$ while actually measuring in standard basis?

$R_{-\theta} |\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

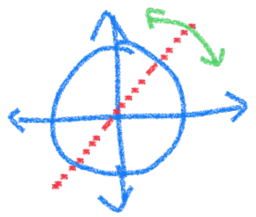
Measure in $\{|0\rangle, |1\rangle\}$

$|0\rangle$ w.p. $|\alpha|^2$, output $|u\rangle$

$|1\rangle$ w.p. $|\beta|^2$, output $|v\rangle$

FACT: Can also build reflector along any axis.

Example 1:



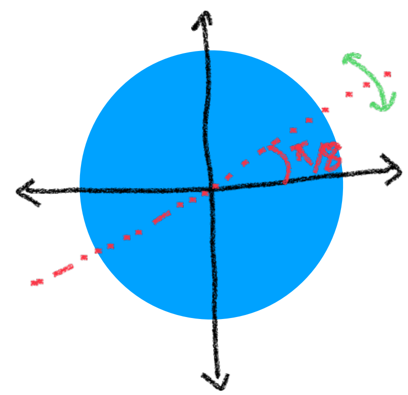
$\begin{bmatrix}1\\0\end{bmatrix} \rightarrow \begin{bmatrix}0\\1\end{bmatrix}$, $\begin{bmatrix}0\\1\end{bmatrix} \rightarrow \begin{bmatrix}1\\0\end{bmatrix}$

$|0\rangle \rightarrow |1\rangle \qquad |1\rangle \rightarrow |0\rangle$

$\begin{bmatrix}\alpha\\\beta\end{bmatrix}$ gets transformed to $\begin{bmatrix}\beta\\\alpha\end{bmatrix}$

NOT operation. $|\psi\rangle = \begin{bmatrix}\alpha\\\beta\end{bmatrix}$ maps to $\underline{\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}}\begin{bmatrix}\alpha\\\beta\end{bmatrix}$

EXAMPLE :



$|0\rangle$ maps to $|+\rangle$

$|1\rangle$ maps to $|-\rangle$

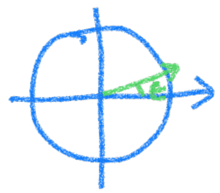
$$\psi = \begin{bmatrix}\alpha \\ \beta\end{bmatrix} \text{ is mapped to } \overset{\displaystyle H}{\overset{\shortparallel}{\begin{bmatrix}1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2}\end{bmatrix}}} \begin{bmatrix}\alpha \\ \beta\end{bmatrix}$$

Hadamard gate

Hadamard is <u>the</u> most important transformation.

Back to Elitzur Vaidman Bomb

- Start with $|0\rangle$
- Apply R_ϵ
- Send to unknown box.

If Dud, then  $\cos\epsilon\,|0\rangle + \sin\epsilon\,|1\rangle$

If Bomb, then $\Pr[\text{Measure } |0\rangle] = \cos^2\epsilon$

$\Pr[\text{Measure } |1\rangle \text{ and explode}] = \sin^2\epsilon$ $< \epsilon^2$

- Repeat $n = \frac{\pi}{2\epsilon}$ times

(Choose ϵ so that $\frac{\pi}{2\epsilon}$ is a large integer)

- Measure in standard basis.

If Dud, then $\Pr[\text{output } |1\rangle] = 1$

If Bomb, then $\Pr[\text{explosion}] \leq n \cdot \epsilon^2 = \frac{\pi}{2}\epsilon$

$\Pr[\text{output } |0\rangle] \geq 1 - \frac{\pi}{2}\epsilon$

WHAT QUANTUM TRANSFORMATIONS ARE POSSIBLE

Quantum Mechanics Law 3 : A qudit can be changed by any linear transformation that preserves lengths.

Such transformations are called unitary transformations.

UNITARY TRANSFORMATION :

U s.t. $\| U|\psi\rangle \|^2 = \| |\psi\rangle \|^2$

$$\Leftrightarrow \quad (U|\psi\rangle)^\dagger U|\psi\rangle = \langle\psi|\psi\rangle$$

$$\Leftrightarrow \quad \langle\psi|U^\dagger U|\psi\rangle = \langle\psi|\psi\rangle$$

Thm: U is unitary $\Leftrightarrow U^\dagger U = \mathrm{Id}.$

Proof : exercise.

LEMMA: Unitary transformations preserve angles

Proof $\left(U|\phi\rangle\right)^{\dagger} U|\psi\rangle =$

LEMMA: Every unitary is invertible/reversible.

Reverse of U is $U^{\dagger}$

FACT (Stated without proof)

Every unitary U has a square root W, which is a unitary s.t. $W^2 = U$.

Example $\sqrt{NOT}$

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

Can check

$$\frac{1}{4}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$$

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

CLASSICAL ANALOGUE OF UNITARY TRANSFORMATION

- Roll a fair dice
- If ODD then toss a fair coin
  - If heads, add 1

$$
\begin{array}{c}
1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6
\end{array}
\begin{bmatrix}
1/6 \\ 1/6 \\ 1/6 \\ 1/6 \\ 1/6 \\ 1/6
\end{bmatrix}
\xrightarrow{\text{Transformation}}
\begin{bmatrix}
1/2 & 0 & 0 & 0 & 0 & 0 \\
1/2 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1/2 & 0 & 0 & 0 \\
0 & 0 & 1/2 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1/2 & 0 \\
0 & 0 & 0 & 0 & 1/2 & 1
\end{bmatrix}
\begin{bmatrix}
1/6 \\ 1/6 \\ 1/6 \\ 1/6 \\ 1/6 \\ 1/6
\end{bmatrix}
$$

MORE GENERALLY

$$\begin{bmatrix} p_1 \\ \vdots \\ p_d \end{bmatrix} \rightarrow \begin{bmatrix} M_{11} & \cdots & M_{1d} \\ M_{21} & & M_{2d} \\ \vdots & & \vdots \\ M_{d1} & & M_{dd} \end{bmatrix} \begin{bmatrix} p_1 \\ \vdots \\ p_d \end{bmatrix}$$

$$M_{11} + M_{21} + \cdots + M_{d1} = 1$$

$$M_{12} + M_{22} + \cdots + M_{d2} = 1$$

$$\vdots$$

$M_{ij} \geq 0$ for all i, j

QUESTION

Can such transformations be used to solve the ELITZUR VAIDMAN problem?