Lecture 4: Unitary transformations & the Elitzur-Vaidman Bomb

Recap: d-dim qudit $|\psi\rangle = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_d \end{bmatrix} \in \mathbb{C}^d$,

$\langle\psi|\psi\rangle = |\alpha_1|^2 + \dots + |\alpha_d|^2 = 1.$

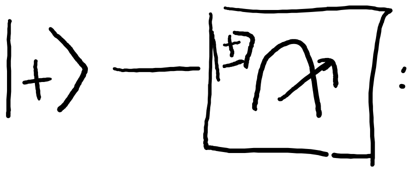
If $\{|u_1\rangle, \dots, |u_d\rangle\}$ is an orthonormal basis, can "measure $|\psi\rangle$ in this basis":

- Write $|\psi\rangle = \beta_1 |u_1\rangle + \dots + \beta_d |u_d\rangle$
  $\beta_1 = \underbrace{\langle u_1|\psi\rangle}$
- Measurement readout is "$|u_i\rangle$" with prob $|\beta_i|^2$
- State "collapses" to $|u_i\rangle$

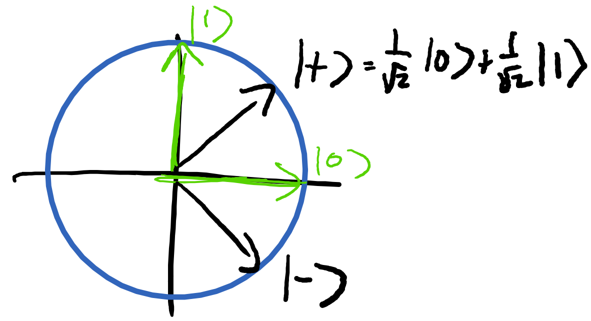
$(\cos\theta)^2$,

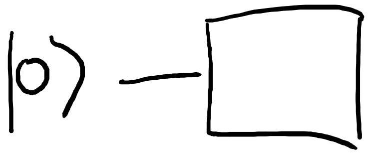
$\theta = \text{angle}(|\psi\rangle, |u_i\rangle)$

E.g.: Measuring a qubit in $\{|+\rangle, |-\rangle\}$ basis:



: 100% chance of "$|+\rangle$"





: ?

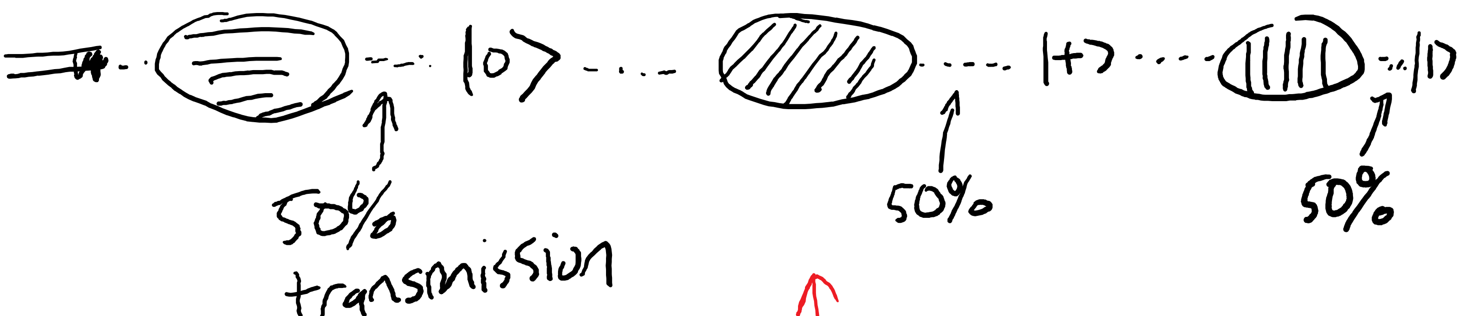
$$|0\rangle = ?\left(\tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|-\rangle\right) + ?\left(\tfrac{1}{\sqrt{2}}|0\rangle - \tfrac{1}{\sqrt{2}}|-\rangle\right)$$

$\frac{1}{\sqrt{2}}$

$\therefore$ 50% chance "$|+\rangle$" $\rightarrow$ state becomes $|+\rangle$

" " "$|-\rangle$" " " $|-\rangle$

((Can do polarizing filter experiment in class.)

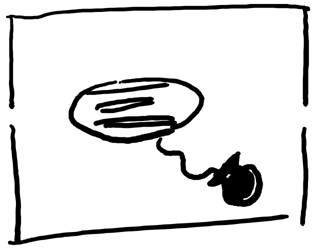


(but if you remove, 0% overall transmission chance)

Elitzur-Vaidman Bomb

(Someone hands you an opaque box with entry and exit slits)

(Inside is either...)



Dud: Nothing (... OR ...) **Bomb**: fuse attached to a horiz. filter

(photon passes thru unchanged)

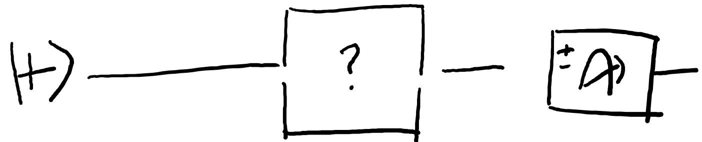
- Measures in std $|0\rangle/|1\rangle$ basis
- If $|0\rangle \to$ passes thru
  If $|1\rangle \to$ heat, bomb explodes

(Goal: Try to determine Dud or Bomb. w/o explosion, of course!)

"Classical" options: Send in $|0\rangle$? $\to$ no info :(

Send in $|1\rangle \to$ KABOOM. (if Bomb)

Quantum idea: Send in $|+\rangle$.
If no explosion, measure in $\{|+\rangle, |-\rangle\}$ basis.



<u>Case Dud</u>: Final readout is "$|+\rangle$" w. prob. 100%.

<u>Case Bomb</u>: • $|+\rangle$ meas'd in std. basis
50% chance $|1\rangle \rightarrow$ <u>explodes</u>
50% ~~~ $|0\rangle \rightarrow$ thru.
Then $|0\rangle$ meas'd in $|\pm\rangle$ basis.
• 50% chance $|+\rangle$ (not helpful, same as Dud case)
• 50% chance $|-\rangle$ (Now you know it's Bomb!)

Summary: If Bomb, 50% chance explosion ☹
But, 25% chance you detect it!!!
& 25 chance inconclusive.

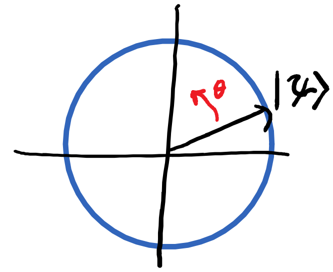
(Today we'll see, you can actually boost this up to a 99.99% chance of explosion-free bomb detection!!)

(Imagine trying not just storing/measuring, but actually computing with qubits. Need to understand how to manip. states.)

Fact: For any θ, can build physical device that "rotates a qubit's state by angle θ"

NOT a measurement ("transformation")

(it has this effect when qubit's amplitudes are real)



(How you do this depends on how logical qubit is physically stored. E.g. photon polarization, in principle doable by passing photon thru some quartz slab whose thickness is a function of θ.
For an "ion trap" qubit, maybe you fire laser at it for some t_θ time.)

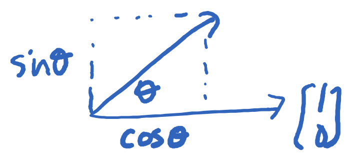
(This is an operation on qubit states, aka 2-dim. vectors. Specifically, can describe it by a 2x2 rotation matrix)

$$R_\theta := \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

(warning: nonstandard notation)

where $\begin{bmatrix}1\\0\end{bmatrix} = |0\rangle$ goes

where $\begin{bmatrix}0\\1\end{bmatrix} = |1\rangle$ goes



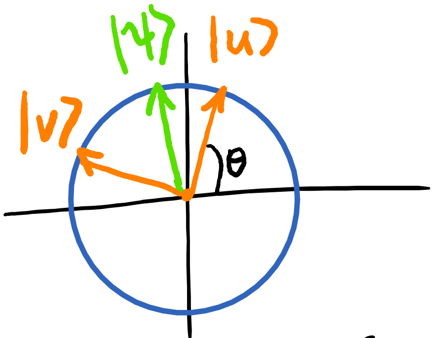
(This is the formal def. of its operation. What it does on states w/ complex ampls. is def'd by this matrix mult.)

e.g.: $\theta = 45°$. $R_{45°} = \begin{bmatrix} 1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{bmatrix}$. Transforms $|0\rangle$ to... $\underline{|+\rangle}$

(If you want to transform $|+\rangle$ to $|0\rangle$, just put it thru an $R_{-45°}$ "gate".)

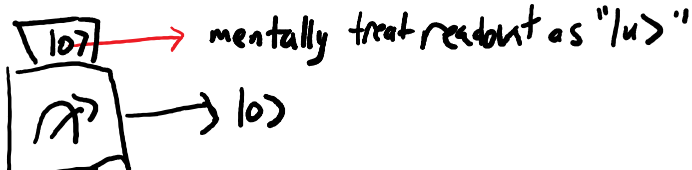
Simulating measuring in $\{|u\rangle, |v\rangle\}$ basis

(I "gave" you ability to measure in any orthonormal basis. Now that you have R_θ ops, WLOG you only "need" the standard $\{|0\rangle, |1\rangle\}$ measurer.)

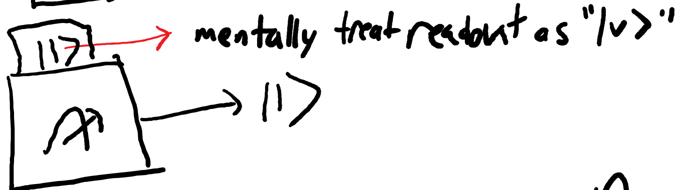


- Pass $|\psi\rangle$ thru $R_{-\theta}$ op.
  ($|u\rangle \to |0\rangle$, $|v\rangle \to |1\rangle$)
- Do std. measurement

Case 1:



Case 2:

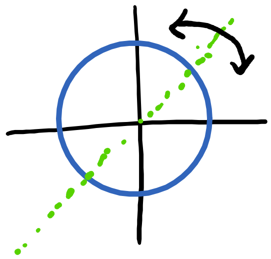


- Pass outcome thru R_θ.

(OK, I told you you can do any rotation R_θ.
Anything else? Yes, you can also do <u>reflections</u>.)

Fact: Can also build <u>reflector</u> thru any line.

E.g 1:



$$\begin{bmatrix}\alpha\\ \beta\end{bmatrix} \longmapsto \begin{bmatrix}\beta\\ \alpha\end{bmatrix}$$

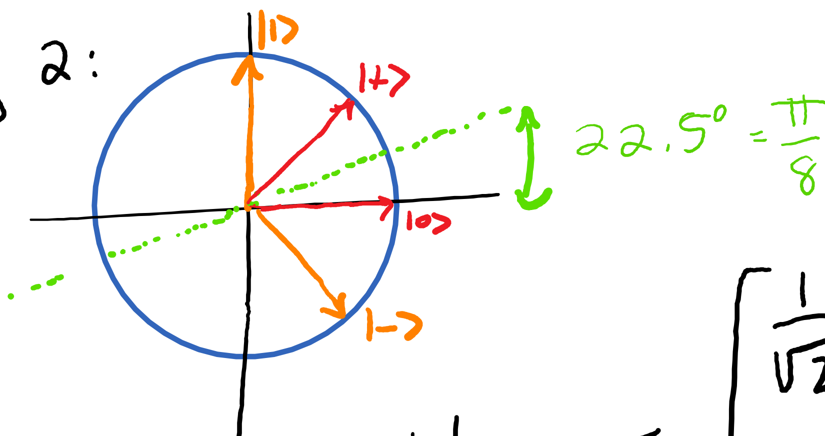
Op. defined by matrix $\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$

where $|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}$ goes

Swaps $|0\rangle$ & $|1\rangle$, and therefore called ....

NOT operator. (aka "X" in quantum lingo)

Eg 2:



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

Hadamard "gate"

(Arguably, most important transformation in quantum computing. It's the 2×2 D.F.T. matrix!)

(Anything else you can do? If you assume only real ampls: No. But because of complex amplitudes, yes; e.g....)

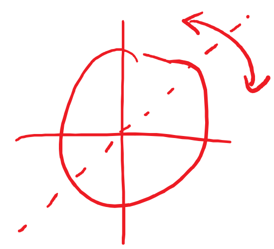
$$\text{"}S\text{"} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \; : \; \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \longmapsto \begin{bmatrix} \alpha \\ i\beta \end{bmatrix} \qquad \left(\text{Check: } |\alpha|^2 + |i\beta|^2 = |\alpha|^2 + |\beta|^2 = 1 \checkmark\right)$$

("phase Shift")

(Really, this is a rotation, too)

(In fact, even reflections can be considered "rotations", if you allow yourself extra dimensions — which actually you have, due to complex #'s.

E.g, take the NOT gate:



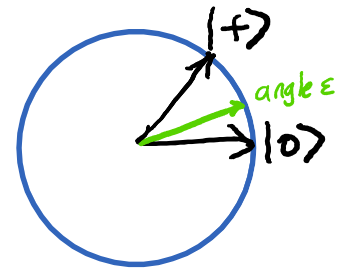
You can imagine a 3rd dim. coming out of the page. Then the reflection is a rotation around axis thru the 3rd dim.

BTW, what would result if you stopped that rotation halfway thru... Half a NOT? We'll see...)

(Anyway, if you're a bit liberal with the meaning of "rotation", there's a sense in which all possible quantum ops are "rotations". Hence Simon's quote, "Rotate, Compute, Rotate".)

(Before we get to formal math of all allowed quantum transformations, let's have some fun with the E-V Bomb.)

(Recall our first strat fired in $|+\rangle$. Risky start: 50% chance of explosion. OTOH, doing $|0\rangle$ is pointless. Why not fire in something at a tiny angle, ε?)



- Start with $|0\rangle$
- Apply R_ε
- Send into box. $\longrightarrow$ <u>If Dud</u>: Qubit exits at angle ε,

<u>If Bomb</u>: $\Pr[\text{measure "}|0\rangle\text{"}] = (\cos\varepsilon)^2$, and $|0\rangle$ exits.

$$\Pr[\text{explode}] = \Pr[\text{measure "}|1\rangle\text{"}] = (\sin\varepsilon)^2 \leq \varepsilon^2$$

$$\left[\text{Taylor: } \sin\varepsilon = \varepsilon - \frac{\varepsilon^3}{6} + \frac{\varepsilon^5}{120} - \cdots \approx \varepsilon\right]$$

Repeat $n := \frac{90^\circ}{\varepsilon} = \frac{\pi}{2\varepsilon}$ times. (Actually, choose integer n first, then set...) $\varepsilon = \pi/2n$.

<u>If Dud</u>: n rotations $\rightsquigarrow$ final state is $|1\rangle$,

<u>If Bomb</u>: final state $|0\rangle$ assuming no explosion.

$$\Pr[\text{explosion}] \leq \varepsilon^2 \cdot n = \frac{\pi^2}{4n} \leq 2.5/n. \quad !$$

(e.g.: Set $n = 1000$; $\Pr[\text{kaboom}] \leq \frac{1}{4}\%$)

And at end, measure: $|0\rangle \Rightarrow$ bomb for sure

$|1\rangle \Rightarrow$ dud for sure. $\square$

(Back to allowable quantum transformations. For generality, consider qudits)

Q.M. Law 3: A qudit's state can* be changed by any linear transformation that preserves lengths.

*in principle (Physically making a device that effects your fave such transform could be challenging. Indeed Q.C. is to some extent about complexity of doing this. NB: these days, we're very good at truly doing any qubit transform.)

(The preserving lengths part is obviously nec.: qudit states must have length 1, so transforms must preserve this. The essence of QM Law3, then, is that all transformations are linear: matrix mults.)

(Which are the lin. transfs. that preserve all lengths? They're like "rigid motions"; basically/slangily, they're rotations (/reflections).

The linear algebra nerds have a name for such transformations on $\mathbb{C}^d$ ...)

Unitary Transformations (In $\mathbb{R}^d$, called "Orthogonal Transformations")

↳ U such that $\| U|\psi\rangle \|^2 = \| |\psi\rangle \|^2 \quad \forall |\psi\rangle \in \mathbb{C}^d$

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

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

(certainly implied by) $\Leftarrow$ $U^\dagger U = I$ (in fact, it's iff — homework)

↑ (identity matrix, $\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$)

thm: U is unitary $\Leftrightarrow$ $U^\dagger U = I \Leftrightarrow UU^\dagger = I \Leftrightarrow U^{-1} = U^\dagger$

$$\begin{pmatrix} - u_1^* - \\ \vdots \\ - u_d^* - \end{pmatrix} \begin{pmatrix} | & & | \\ u_1 & \cdots & u_d \\ | & & | \end{pmatrix} = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$

$\Leftrightarrow$ U's cols (/rows) are orthonormal

(think of U as an orthonormal change-of-basis operation.)

<u>fact</u>: Unitaries U also preserve <u>angles</u>.

Equivalently, preserve inner products.

<u>proof</u>: $(U|\phi\rangle)^\dagger U|\psi\rangle = \langle\phi|U^\dagger U|\psi\rangle$

$$= \langle\phi| I |\psi\rangle = \langle\phi|\psi\rangle. \checkmark$$

<u>fact</u>: Every unitary U is invertible/<u>reversible</u>.

pf: $U^{-1} = U^\dagger$ (← also unitary)

Examples:

On qubits, $\mathbb{C}^2$: $R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$

$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ $\quad NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$ $\quad$ "Z" $= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

In, say, 3 dimensions: $\begin{pmatrix} 0 & 0 & \pm 1 \\ \pm 1 & 0 & 0 \\ 0 & \pm 1 & 0 \end{pmatrix}$

(Any permutation matrix clearly preserves length: $|\beta|^2 + |\gamma|^2 + |\alpha|^2 = |\alpha|^2 + |\beta|^2 + |\gamma|^2$.)

In 4-d: $\begin{array}{c|c} & \begin{matrix} 00 & 01 & 10 & 11 \end{matrix} \\ \begin{matrix} 00 \\ 01 \\ 10 \\ 11 \end{matrix} & \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{array}$: "SWAP"

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

((Check: cols orthonormal.))

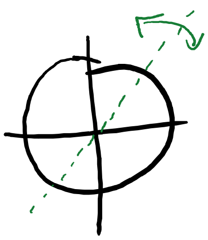
= Boolean Fourier Transform matrix on 2 bits...

Fun Fact: Every unitary U has a square-root: a (unitary) $W = \text{"}\sqrt{U}\text{"}$ such that $W^2 = U$.

e.g. $\sqrt{R_\theta} = \underline{R_{\theta/2}}$ (Physically, for photons, make that slab of quartz half as thick. For ion trap, fire that laser for half as long.)

(In fact, unitaries are, like, "infinitely divisible"— they have cube roots, fourth roots, etc. (Kinda makes sense, from a continuous physics point of view.)

· $\sqrt{\text{NOT}} = ???!$ (An op. such that if you do it <u>twice</u> you effect a logical NOT? Impossible classically! But



(A reflection doesn't seem to have a square root. It doesn't if you stick to $\mathbb{R}^2$. But if you think of it as a 3-d rotation, with complex #'s allowing that 3^{rd} dim., you can indeed stop halfway.)

$$\sqrt{\text{NOT}} = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$$

(Can check unitary — cols. orthonormal.)

Check: squares to
$$\frac{1}{4}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix} = \frac{1}{4}\begin{pmatrix} 0 & 4 \\ 4 & 0 \end{pmatrix}$$
$$= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \text{NOT}. \checkmark$$

(Kinda justifies "why" quantum states have to go to complex numbers.)