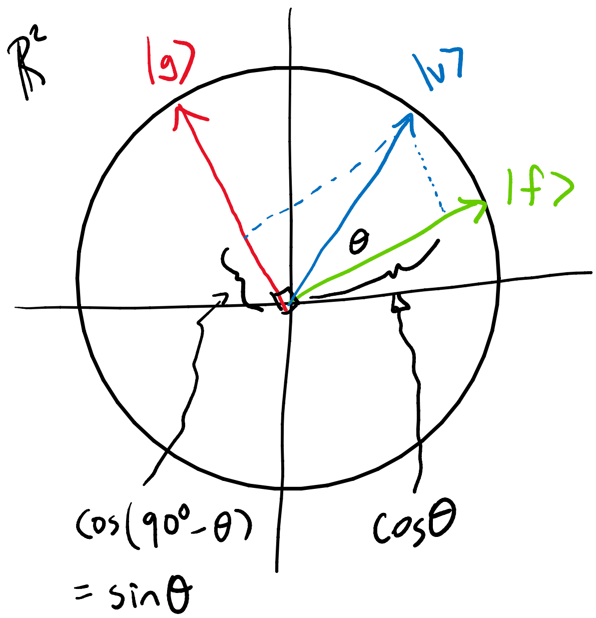
Lecture 12 – Learning a Mystery Rotation

Recall measuring $|v\rangle$ in $|f\rangle, |g\rangle$ basis:



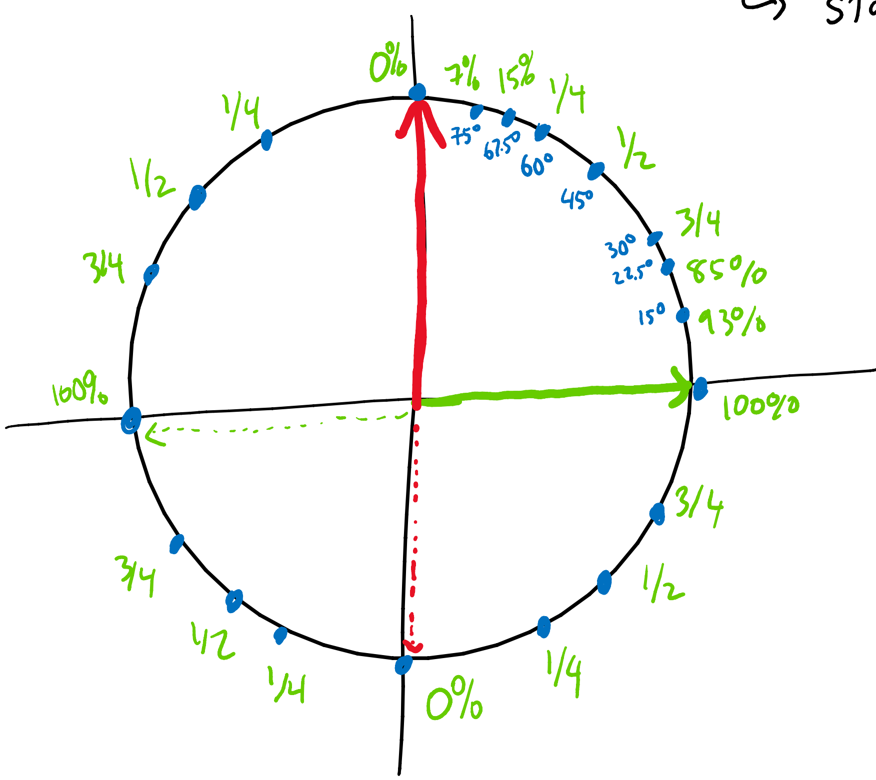
- $\Pr[\text{readout "f"}] = \langle f|v\rangle^2 = (\cos\theta)^2$

  ⤳ state remade ("collapses") to $|f\rangle$

- $\Pr[\text{readout "g"}] = \langle g|v\rangle^2$

  $= \cos(90^\circ - \theta)^2 = (\sin\theta)^2$

  ⤳ state remade ("collapses") to $|g\rangle$



Prob of measuring & getting "0"

[Your Mom comes to you and says "Darling, I have a test for you. I prepared this beautiful photon, and I...]

<u>Promise</u>: Photon's qubit state $|test\rangle$ is either $|0\rangle$ or $|1\rangle$.

<u>Question</u>: Yes or no: $|test\rangle = |1\rangle$?

[Well, it's obvious what to do.]

~~Print All~~ Measure.

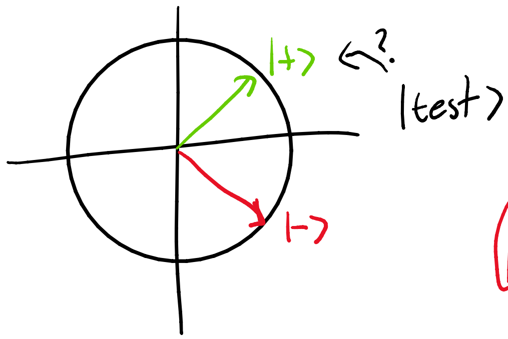
If readout = "1", say "yes".

If readout = "0", say "no".

Pr[you're correct] = 100%. [Perfect! A++]

[Your Dad comes to you and says "Darling, I have a test for you. I prepared this beautiful photon, and I...]

Dad's Promise: $|test\rangle$ is either $|+\rangle$ or $|-\rangle$



Question: Yes or no:

$|test\rangle = |+\rangle$?

[Bad idea now to just Measure. If $|test\rangle = |+\rangle$, you'll see 0/1 with 50% each. But same if $|test\rangle = |-\rangle$! Better idea?]

- Measure in $|+\rangle, |-\rangle$ basis.
- If readout = "+", say "yes".
- If readout = "−", say "no".

Case 1: $|test\rangle = |+\rangle$. Then Pr[readout = "+"] = 100%

= Pr[you say "yes"]

= Pr[you're correct].

Case 2: $|test\rangle = |-\rangle$. Then Pr[readout = "−"] = 100%

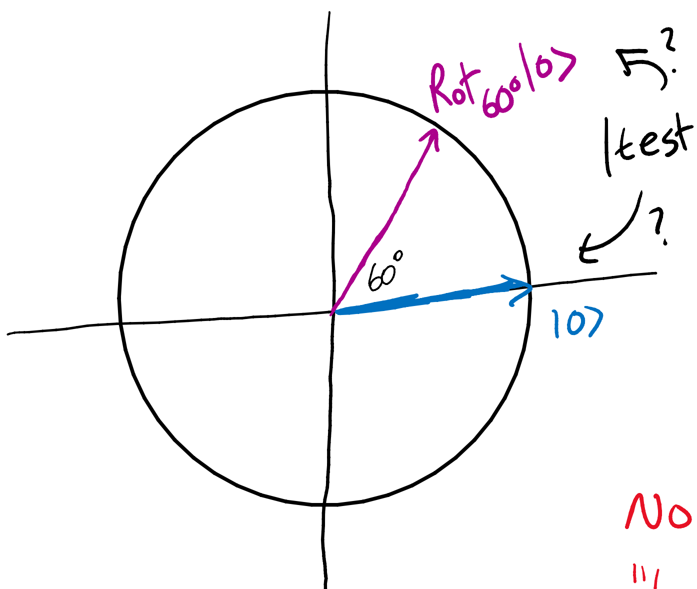
= Pr[you say "no"]

= Pr[you're correct].

Perfect! [Again, A++, 100% correctness]

[Now it's the real world. Prof. Ada comes and says, "I have prepared a photon for you..."]

Ada's Promise: $|test\rangle$ is either $|0\rangle$ or $Rot_{60°}|0\rangle$.



Question: Yes or no: $|test\rangle = Rot_{60°}|0\rangle$?

["Measure in the ($|0\rangle$, $Rot_{60°}|0\rangle$) basis?"

No, that's not valid, this is not a "basis". Can only do this for perpendicular basis vectors.]

Idea 1: Measure in the "standard" $|0\rangle, |1\rangle$ basis.

If readout = "1", say... yes. [Only possible if $|test\rangle = Rot_{60°}|0\rangle$.]

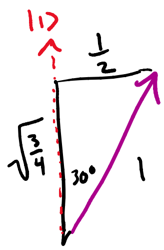
If readout = "0", say ... no. [I guess.]

Case 1: $|test\rangle = |0\rangle$. Pr[readout = "0"] = 100%

= Pr[say "no"]

= Pr[you're correct]

Case 2: $|test\rangle = Rot_{60°}|0\rangle$



$$Pr[\text{readout} = \text{"1"}] = (\cos 30°)^2 = 3/4$$

$$Pr[\text{say "yes"}] \overset{\text{"}}{=} Pr[\text{you're correct}].$$

[$Pr[\text{readout} = \text{"0"} / \text{say "no"}] = (\sin 30°)^2 = 1/4.$]

This is a 1-sided error alg.

No "false positives". $Pr[\text{false negative}] = 1/4$

(saying "no" when "yes" is correct)

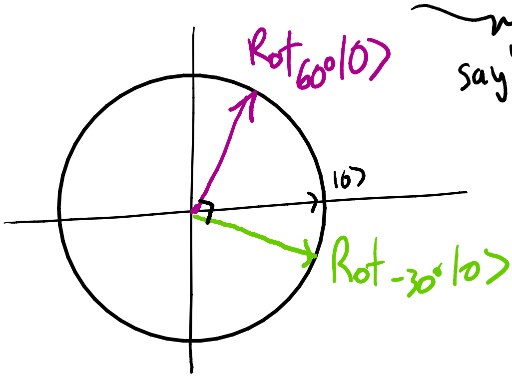
"Yes means yes".

[What about 1-sided error the other way?]

[How to achieve...] No false negatives ("no means no") alg.?

Measure in $(Rot_{-30°}|0\rangle, Rot_{60°}|0\rangle)$ basis:

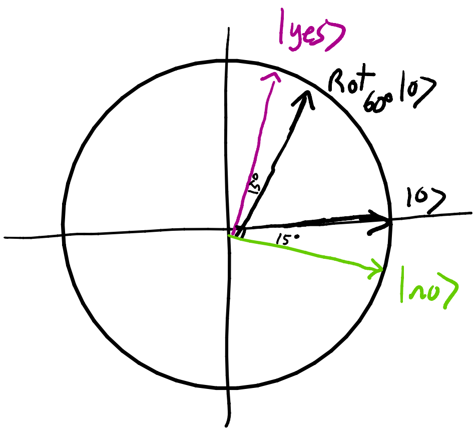
$$(\underbrace{Rot_{-30°}|0\rangle}_{\text{say "no"}}, \underbrace{Rot_{60°}|0\rangle}_{\text{say "yes"}})$$



- $|test\rangle = Rot_{60°}|0\rangle \Rightarrow Pr[\text{say "yes"}] = 100\%$
- $|test\rangle = |0\rangle \Rightarrow Pr[\text{say "no"}] = (\cos 30°)^2 = 3/4.$

2-sided error alg? [[Can we get "error" $\le \frac{1}{4}$ by allowing false pos. & neg.?]]

Idea 2: Let $|yes\rangle := Rot_{75°}|0\rangle$
$|no\rangle := Rot_{-15°}|0\rangle$ } [[Both are 15° "off".]]



Case 1: $|test\rangle = |0\rangle$. Then
$\Pr[\text{readout} = \text{"no"}] = (\cos 15°)^2 \approx .933$
[[use a calculator]]

Case 2: $|test\rangle = Rot_{60°}|1\rangle$. Then
$\Pr[\text{readout} = \text{"yes"}] = (\cos 15°)^2 \approx .933$.

$\text{Prob}[\text{error}] = (\sin 15°)^2 \approx .067$.

($\pi/12 \approx .26 \approx$ small, so $\sin\frac{\pi}{12} \approx .26$
$(\sin\frac{\pi}{12})^2 \approx (.26)^2 \approx .0676$ ✓)

Hey, with 2-sided error, 93.3% correct!

[[That's an A! ☺]]

[[Note also .067 error is $\le$ half of $\frac{1}{4}$-one-sided error...]]

[The final boss?] Prof. Eckhardt [gives you a photon.]

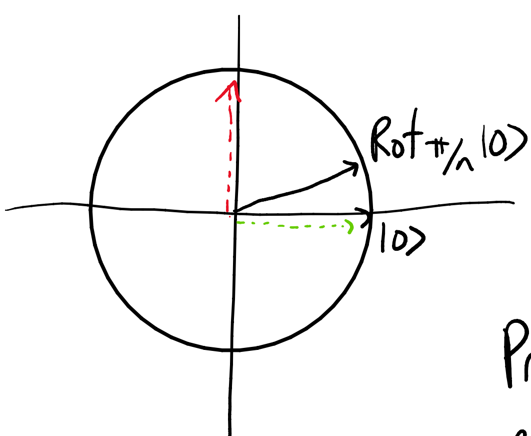
His promise: state $|test\rangle$ is either $|0\rangle$ or $Rot_{\frac{\pi}{100}}|0\rangle$. $\leftarrow$ 1.8°

Actually, say $Rot_{\frac{\pi}{n}}|0\rangle$, but you know n's value.

Question: Yes or no, is $|test\rangle = Rot_{\frac{\pi}{n}}|0\rangle$?

[Let's start by trying to get a 1-sided error alg.]

- Measure in $|0\rangle, |1\rangle$ basis.
- If readout "1", say "yes".
- If readout "0", say... "no", I guess ☹



Case 1: $|test\rangle = |0\rangle$. Then

$Pr[\text{say "no" / correct}] = 100\%$.

Case 2: $|test\rangle = Rot_{\pi/n}|0\rangle$. Then

$$Pr[\text{readout "0"}] = \cos(\pi/n)^2$$

$$Pr[\text{correct}] \rightarrow Pr[\text{readout "1"}] = \sin(\pi/n)^2$$

(say "yes")

small

$\pi^2 \approx 10$

$$\approx (\pi/n)^2 = \frac{\pi^2}{n^2} \approx \frac{10}{n^2}.$$

e.g.: $n = 100 \Rightarrow Pr[\text{correct}] \approx \frac{1}{1000}$ ☹ [Pretty bad failure percentage.]

[[So... ask to retake the test?]]

Note: Must ask Eckhardt for new copy of $|\text{test}\rangle$.

[["Remeasuring" won't work, as photon already "collapsed" to measurement outcome.]]

Given another copy (same as last time):

Again:
- $|\text{test}\rangle = |0\rangle \Rightarrow \Pr[\text{"no"}] = 100\%$
- $|\text{test}\rangle = \text{Rot}_{\frac{\pi}{n}}|0\rangle \Rightarrow \Pr[\text{"yes"}] \approx \frac{10}{n^2}$. $\left(\le \frac{10}{n^2}\right)$

Say you get n copies of test, do the measurement strat, take "OR" of all results.

- $|\text{test}\rangle = |0\rangle \Rightarrow \Pr[\text{overall "no"}] = 100\%$
- $|\text{test}\rangle = \text{Rot}_{\frac{\pi}{n}}|0\rangle \Rightarrow \Pr[\text{overall "yes"}]$

[["union bound"]] $\rightarrow \le \Pr[\text{yes on } 1^{st}] + \dots + \Pr[\text{yes on } n^{th}]$

$$\underset{(\le)}{\approx} \frac{10}{n^2} + \dots + \frac{10}{n^2} \quad (n \text{ times})$$

$$= 10/n$$

☹

[[Still pretty bad. Like 10% success if $n = 100$.
Well, but success rate up from $\frac{10}{n^2}$ to $\frac{10}{n}$.
Keep repeating?]]

Say instead you get n^2 copies of Eckhardt's $|\text{test}\rangle$. Say $|\text{test}\rangle = \text{Rot}_{\frac{\pi}{n}}|0\rangle$.

Each measurement, have prob. $\approx \frac{10}{n^2}$ of saying "yes".

$\Rightarrow E[\#\text{ of times you say yes}] \approx n^2 \cdot \frac{10}{n^2} = 10$. ☺

[[Probably going to see ≥ 1 "yes", indeed ≈ 10 yeses. So quite likely now to overall say "yes"!]]

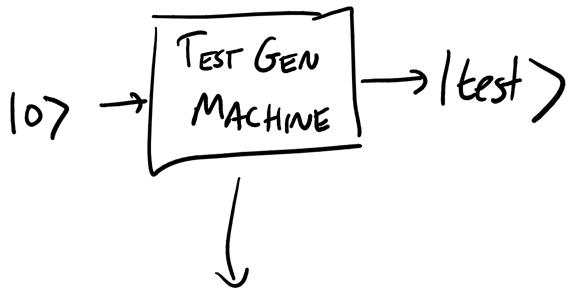
(Math: $\Pr[\underline{\text{not}} \text{ overall "yes"}] \approx e^{-10} \approx .00005$.

$$\left(1 - \sin\left(\tfrac{\pi}{n}\right)^2\right)^{n^2} \approx \left(1 - \tfrac{\pi^2}{n^2}\right)^{n^2} \underbrace{\approx}_{\text{actually } \leq} \left(e^{-\pi^2/n^2}\right)^{n^2} = e^{-\pi^2}. \checkmark$$
)

<u>Summary</u>: With n copies, very low prob. of distinguishing $|0\rangle$ from $\text{Rot}_{\frac{\pi}{n}}|0\rangle$.
(1-sided error) With n^2 copies, very high prob.

<u>Exercise</u>: Think about 2-sided error strats.
(Unfortunately, with just 1 copy, best strat still has $\Pr[\text{correct}] \approx \frac{1}{2} + \frac{\pi}{2n}$. ($\approx 51\%$ if $n = 100$)
Still need $\approx n^2$ copies to succeed w/ high probability ☹)

[But! I don't condone this, but what if you could break into Eckhardt's office & steal his Test Generation Machine?]



[Imagine the machine is a black box. Or, you see the code, but it's super-obfuscated....]

effectively: Mystery Rotation(A):

// either nothing or $Rot_{\frac{\pi}{n}}$

// but you don't know which

[Well, now you can make your n^2 copies of $|test\rangle$ if you want. But can you crack the case more quickly?]

Make A // state $|0\rangle$

for $t = 1 \ldots n/2$: // assume n even for simplicity

  Mystery Rotation(A)

<u>Case 1</u>: $|test\rangle = |0\rangle$ ≡ Mystery Rot does nothing

$\rightarrow$ A's final state is $|0\rangle$

<u>Case 2</u> $|test\rangle = Rot_{\frac{\pi}{n}}|0\rangle$ ≡ Mystery Rot is by π/n

$\rightarrow$ A's final state is $Rot_{\frac{\pi}{2}}|0\rangle = |1\rangle$!

[So after $\frac{n}{2}$ "time", you have...]

either $|0\rangle$ or $|1\rangle$ ← your Mom's promise!

Measure & find out which, 100% prob.

<u>Summary</u>: • Just with <u>copies</u> of $|\text{test}\rangle$, need $\approx n^2$ to distinguish $|0\rangle$ & $\text{Rot}_{\frac{\pi}{n}}|0\rangle$, w/ high prob.

• With black-box access to the "code" producing $|\text{test}\rangle$, can distinguish with after $\approx n$ uses (with certainty)

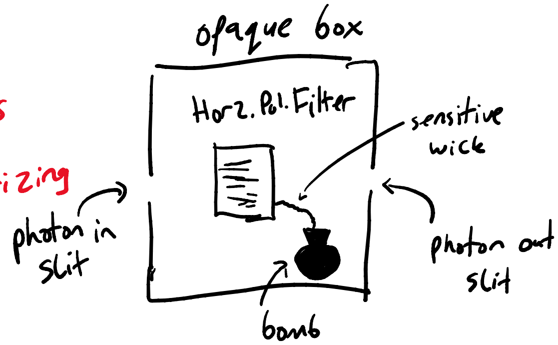
[This is a key quantum concept; as we'll see, it exactly underlies the quadratic speedup in Grover's alg., & also most other quadratic speedups in quantum comp. It even slightly presages the quantum factoring alg....]

[Let's see a cool "use" of this idea...]

"Elitzur-Vaidman Bomb problem" (1993)

[You are a supervillain, Your schtick is making booby-trapped boxes that look like this:]

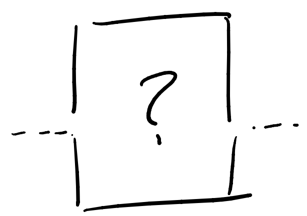
[Single photon goes in. Hits polarizing filter...



... if measured to $|0\rangle$, passes thru. If measured to $|1\rangle$, heat $\Rightarrow$ bomb explodes!]

[You're in the attic of your super lair, and you run across an old box, You can't remember...]

Empty box or Bomb box?

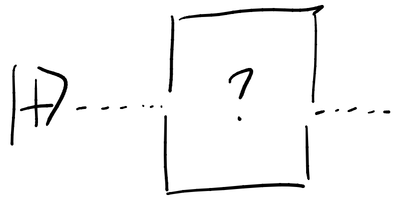


[Can't tamper with it. Can only shoot in photons. What to do?]

Put in $|1\rangle$? Too risky! Explosion, if bomb.

" " $|0\rangle$? Useless! Empty $\Rightarrow$ $|0\rangle$ comes out.
Bomb $\Rightarrow$ $|0\rangle$ comes out.
No info! (prob. 100%)

Put in $|+\rangle$? [Better, but kinda risky....]



Case Bomb:
- $|+\rangle$ measured in $(|0\rangle, |1\rangle)$
- 50% chance of "1" - explode! :(
- 50% chance of "0", state collapses to, comes out as, $|0\rangle$

Case Empty:
- $|+\rangle$ comes out as $|+\rangle$

Now what? Like a "$|0\rangle$ vs. $|+\rangle$ test"!

Ex: Can get 1-sided error ½ (*) or 2-sided error ≈ 15%.

Summary: 50% explosion chance,

using (*) { 25% survive & certain box has Bomb
25% survive & inconclusive

[[Better?]]

make this →

$$\boxed{\begin{array}{l}\text{def Mystery Rotation (A):}\\ \quad \cdot\ \mathrm{Rot}_{\pi/n}(A)\\ \quad \cdot\ \text{Put A in Box}\end{array}}$$

Case Empty: MysteryRot $\equiv$ $\mathrm{Rot}_{\pi/n}$ on any input

Case Bomb: MysteryRot$(|0\rangle)$: explode w. prob... $\sin(\pi/n)^2 \approx \left(\frac{\pi}{n}\right)^2 \approx 10/n^2$

else... comes out $|0\rangle$

↳ Acts like nothing on $|0\rangle$, except $\approx 10/n^2$ chance of exploding

Ignoring explosions for now, this is exactly like Eckhardt's Test Generation Machine (distinguishing $Rot_{\pi/n}$ from Rot_0):

Make A // $|0\rangle$

for $t = 1 \ldots n/2$

  MysteryRot(A)

Measure A : "0" → Bomb, "1" → Empty } 100% prob.!

$\Pr[\text{explosion}] \leq \Pr[\text{explode on try } 1] + \ldots + \Pr\left[\text{explode on try } n/2\right]$

[union bound]

$\approx \frac{n}{2} \cdot \frac{10}{n^2} = 5/n.$

Time vs. safety tradeoff!

Take, e.g., $n = 1{,}000{,}000$.

500k steps, $\Pr[\text{explode}] \approx$ 5 in a million,

& no explode ⇒ learning w/ certainty if Bomb or Empty!

["seeing without looking"]