Lecture 2

Sep 29, 2025

Important math review : Prob. Theory.

Let $X \geq 0$ be a pos. random variable.

(1)

Markov's Ineq. $\Pr[X \geq a] \leq \frac{\mathbb{E}X}{a}$ for all $a > 0$.

Pf. $\mathbb{E}X = \underbrace{\mathbb{E}[X \mid X \geq a]}_{a} \cdot \Pr[X \geq a] + \underbrace{\mathbb{E}[X \mid X < a]}_{0} \underbrace{\Pr[X < a]}_{0}$

$\geq a \Pr[X \geq a] + 0 \cdot 0$

(2)

Let X be a r.v. with $\mathrm{Var}\, X = \sigma^2$ finite and $\mathbb{E}X = \mu$.

Chebyshev's Ineq. $\forall\, k > 0$,

$$\Pr\left[\, |X - \mu| \geq k\sigma \,\right] \leq \frac{1}{k^2}.$$

Pf. Apply Markov for $Y = (X-\mu)^2$ and $a = k^2\sigma^2$.

$$\Pr\left[\,|X-\mu| \geq k\sigma\right] = \Pr\left[(X-\mu)^2 \geq k^2\sigma^2\right]$$

$$= \Pr\left[\,Y \geq k^2\sigma^2\right]$$

$$\leq \frac{\mathbb{E}Y}{k^2\sigma^2} = \frac{\sigma^2}{k^2\sigma^2} = \frac{1}{k^2}.$$

(3) Chernoff bounds:

$$\Pr\left[\,X \geq a\right] = \Pr\left[e^{tX} \geq e^{ta}\right]$$

$$\leq \frac{\mathbb{E}\left[e^{tX}\right]}{e^{ta}} \qquad \text{(Markov's)}$$

So, $\Pr\left[X \geq a\right] \leq \inf_{t>0} \dfrac{\mathbb{E}\left[e^{tX}\right]}{e^{ta}}$.

If $X = X_1 + \dots + X_n$, then

$$\Pr\left[X \geq a\right] = \inf_{t>0} e^{-ta} \prod_{i=1}^{n} \mathbb{E}\left[e^{tX_i}\right].$$

If $X_i \in \{0,1\}$ then $e^{tX_i} = \begin{cases} e^t & \text{pr } p_i := \mathbb{E} X_i \\ 1 & \text{pr } 1-p_i \end{cases}$

$$\mathbb{E}\, e^{tX_i} = (e^t - 1)\, p_i + 1 \le e^{p_i(e^t-1)}.$$

So, $$\prod_i \mathbb{E}\, e^{tX_i} \le e^{(p_1+\dots+p_n)(e^t-1)}.$$
$$= e^{\mu(e^t-1)} \qquad \mu = \mathbb{E} X = p_1 + \dots + p_n.$$

Let $a = (1+\delta)\mu$.

$$\inf_{t>0} e^{-ta} \prod_i \mathbb{E}[e^{tX_i}]$$

$$\le \inf_{t>0} e^{-t(1+\delta)\mu}\, e^{\mu(e^t-1)}$$

$$\le \inf_{t\ge 0} \left(e^{\left(\frac{e^t-1}{(1+\delta)t}\right)} \right)^{\mu}.$$

Ex. inf at $t = \ln(1+\delta)$.

$$= \left(\frac{e^{\delta}}{(1+\delta)^{1+\delta}} \right)^{\mu} \underbrace{\le}_{\text{exercise.}} e^{-\delta^2\mu/(2+\delta)}.$$

Chernoff bounds: $X_1, \ldots X_n \in \{0,1\}$. $X = \sum X_i$, $\mu = \mathbb{E}X$,

$$\Pr[X \geq (1+\delta)\mu] \leq e^{-\delta^2\mu/(2+\delta)}$$

$$\Pr[X \leq (1-\delta)\mu] \leq e^{-\delta^2\mu/2}$$

$$\Pr[|X-\mu| \geq \delta\mu] \leq 2e^{-\delta^2\mu/3}$$

Today: Quantum's power over classical

1. Elitzur-Vaidman Bomb Tester
2. Deutsch-Jozsa game.

Recall axioms of quantum computation:

1. The state of a n qubit system is a unit vec in

$$\underbrace{\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{n \text{ times}} = (\mathbb{C}^2)^{\otimes n} \cong \mathbb{C}^{2^n}$$

(2) For any unitary $\mathcal{U} \in \mathbb{C}^{4\times 4}$, we can transform the state $|\psi\rangle$ to

$$\Big[\underbrace{\mathbb{1}_2 \otimes \dots \otimes \mathbb{1}_2}_{\ell_1} \otimes \mathcal{U} \otimes \underbrace{\mathbb{1}_2 \otimes \dots \otimes \mathbb{1}_2}_{\ell_2} \Big] |\psi\rangle$$

$\ell_1 + 2 + \ell_2 = n$

(3) Measure the first qubit: $|\psi\rangle = |0\rangle|\psi_0\rangle + |1\rangle|\psi_1\rangle$

Transform to $\dfrac{|i\rangle|\psi_i\rangle}{\||\psi_i\rangle\|}$ with pr $\||\psi_i\rangle\|^2$.

(4) Given state $|\psi\rangle$ on n-qubits, we can generate the state $|\psi\rangle \otimes |0\rangle$ on $(n+1)$-qubits

<u>Obs</u> General basis single-qubit measurements.

Let $|b_0\rangle, |b_1\rangle$ be orthonormal vectors in $\mathbb{C}^2$.

Axioms give us a way to measure $|\psi\rangle$ and get

$|0\rangle$ w pr $|\langle 0|\psi\rangle|^2$ and

$|1\rangle$ w pr $|\langle 1|\psi\rangle|^2$.

Can we generate a method to get

$|b_0\rangle$ w pr $|\langle b_0|\psi\rangle|^2$ and

$|b_1\rangle$ w pr $|\langle b_1|\psi\rangle|^2$.

<u>Ans</u> let $\mathcal{U} = \begin{pmatrix} | & | \\ |b_0\rangle & |b_1\rangle \\ | & | \end{pmatrix}$

$\mathcal{U}$ is unitary as $\mathcal{U}^\dagger = \begin{pmatrix} - \langle b_0| - \\ - \langle b_1| - \end{pmatrix}$

Then $\mathcal{U}^\dagger \mathcal{U} = \begin{pmatrix} \langle b_0|b_0\rangle & \langle b_0|b_1\rangle \\ \langle b_1|b_0\rangle & \langle b_1|b_1\rangle \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbb{1}_2$.

For $i \in \{0,1\}$, $\mathcal{U}|i\rangle = |b_i\rangle$ so $\mathcal{U}^\dagger |b_i\rangle = |i\rangle$.

<u>Algorithm</u>

1. Apply $\mathcal{U}^\dagger$ (also unitary)
2. Measure
3. Apply $\mathcal{U}$.

Pf. state after ① is $\mathcal{U}^\dagger |\psi\rangle$

For $i \in \{0,1\}$, measuring produces $|i\rangle$ with pr

$$|\langle i | \mathcal{U}^\dagger | \psi\rangle|^2 = |\langle b_i | \psi\rangle|^2$$

Then applying $\mathcal{U}$ means we produce $\mathcal{U}|i\rangle = |b_i\rangle$ w pr

$$|\langle b_i | \psi\rangle|^2.$$

A physics motivation for qubits.

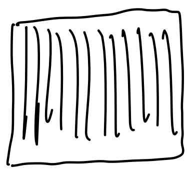
Polarization of light.

Photons have a polarization:

Photons that travel $\leftrightarrow$ "in state" $|0\rangle$

Photons that travel $\updownarrow$ "in state" $|1\rangle$

Photons that travel $\nearrow\!\!\!\!\swarrow$ "in state" $\frac{|0\rangle + |1\rangle}{\sqrt{2}} =: |+\rangle$.

Build a sieve:  so that

output photons are polarized as $|1\rangle$.

What is happening as photon hits the sieve?

<u>Ans</u> measurement:

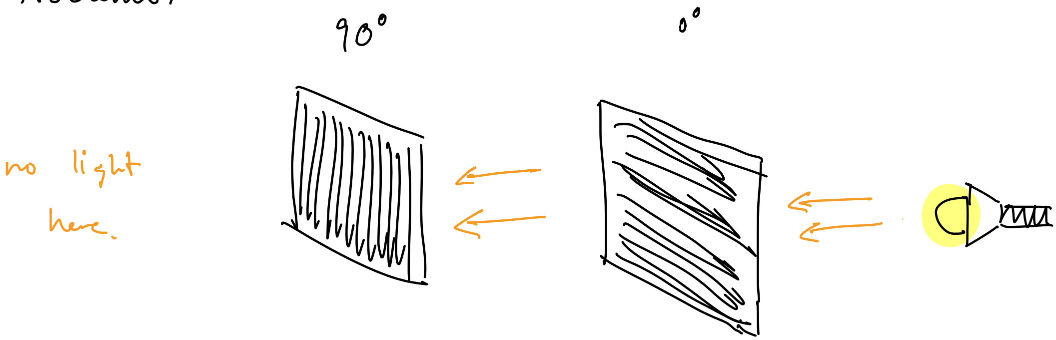
$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ state of photon before.

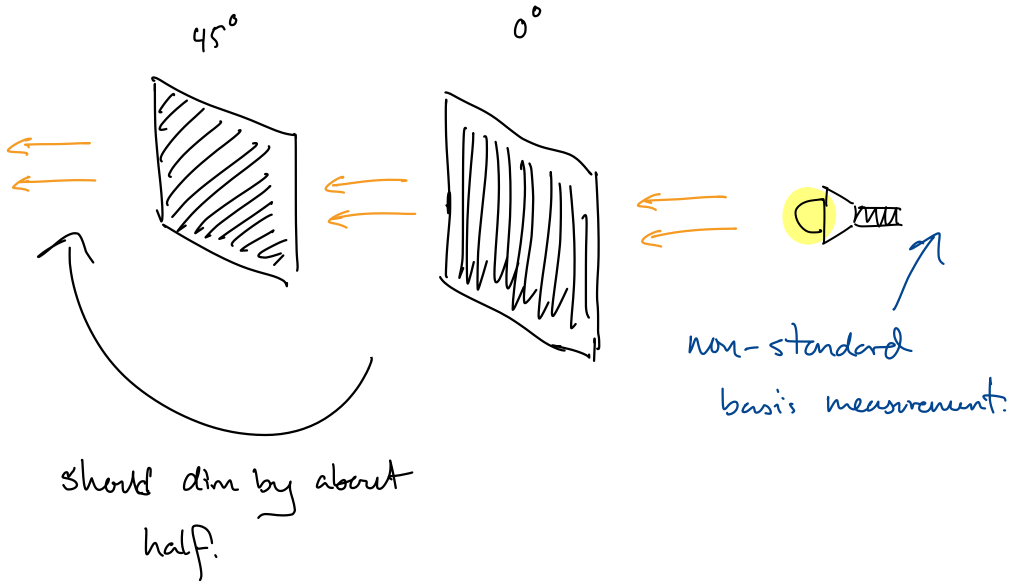
collapses to either $|0\rangle$ "absorbed" w pr $|\alpha|^2$

$|1\rangle$ "goes through" w pr $|\beta|^2$.

Random light's polarization can be thought of as a random angle. Easy to show that $\sim 1/2$ of photons pass through in the stat. mech. limit.

Problems:

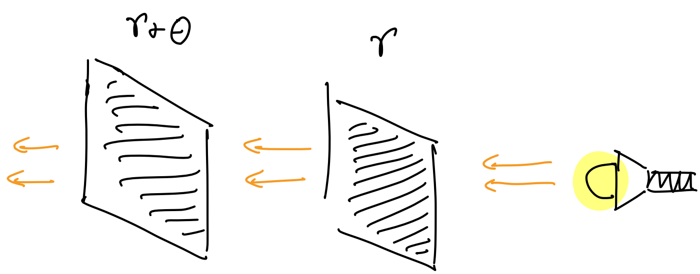




Another way to analyze this is to notice that a sieve at angle θ is measuring the qubit in a non-standard basis given by

$$|b_0^\theta\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle \quad \text{"pass through"}$$

$$|b_1^\theta\rangle = -\sin\theta\,|0\rangle + \cos\theta\,|1\rangle. \quad \text{"absorb".}$$



What fraction of light passes through?

$$\Pr\left[\ \boxed{\mathbin{/\!\!/}_{\theta+\gamma}}\ \text{measurement accepts } |b_0^\gamma\rangle\right]$$

$$= \left|\langle b_0^{\theta+\gamma}|b_0^\gamma\rangle\right|^2$$

$$= \left(\cos\gamma\cos\theta+\gamma + \sin\gamma\sin\theta+\gamma\right)^2$$

$$= \cos^2\left((\theta+\gamma)-\gamma\right) = \boxed{\cos^2\theta}.$$

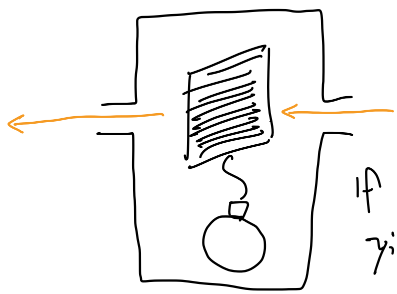
Elitzur-Vaidman Bomb Tester (1993)

Suppose there is a black box (cannot open/see components) s.t.

ⓐ A photon enters and a photon leaves.

ⓑ you know it is 1 of 2 possibilities:

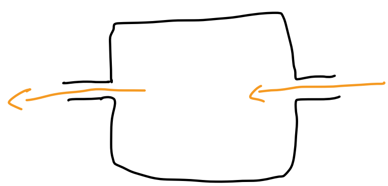
"Bomb"



If sieve measurement yields $|1\rangle$, bomb explodes.

Otherwise photon passes through.

"Dud"



Question: Can we detect which box is in front of us without setting off the bomb?

Ideas:

send $|\psi_{in}\rangle = |0\rangle$

Dud: $|\psi_{out}\rangle = |0\rangle$.

Bomb: $|\psi_{out}\rangle = |0\rangle$.

no difference.

send $|\psi_{in}\rangle = |1\rangle$

Dud: $|\psi_{out}\rangle = |1\rangle$.

Bomb: Explosion

too much difference.

Model the Dud as the identity transform

the Bomb as a standard basis measurement.

Let's send in a rotated state

and measure the output in a rotated basis.

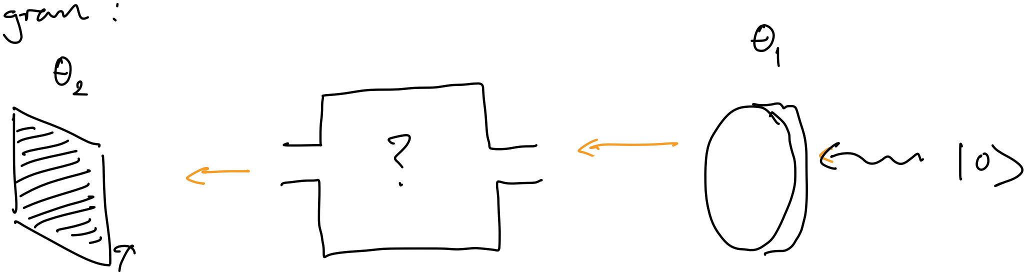
Introduce a rotational gate:

$$R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

$$R_\theta|0\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle$$

$$R_\theta^\dagger = R_{-\theta}.$$

Diagram:



measure if passes or reflects.

Quantum circuit:

θ_2 basis measurement

$$-\boxed{\nearrow_{\theta_2}}-\boxed{?}-\boxed{R_{\theta_1}}-|0\rangle$$

by prev. we can write it as

$$\underbrace{\boxed{R_{\theta_2}}}_{\text{irrelevant}}-\boxed{\nearrow_{\text{standard}}}-\boxed{R^{\dagger}_{\theta_2}}-\boxed{?}-\boxed{R_{\theta_1}}-|0\rangle$$

$$R^{\dagger}_{\theta_2}=R_{-\theta_2}=R_{\theta_1-\theta_2}R_{-\theta_1}$$

$$-\boxed{\nearrow}-\boxed{R_{\theta_1-\theta_2}}-\boxed{R_{-\theta_1}}-\boxed{?}-\boxed{R_{\theta_1}}-|0\rangle$$

when $-\boxed{?}- = -\boxed{\mathbb{1}}-$ "dud"

this simplifies to $-\boxed{X}-\boxed{R_{\theta_1-\theta_2}}-|0\rangle$

which "accepts" w pr $\cos^2(\theta_1-\theta_2)$, (no explosion)

"rejects" w pr $\sin^2(\theta_1-\theta_2)$. (no explosion)

when $-\boxed{?}- = -\boxed{X}-$ "bomb"

$$-\boxed{X}-\boxed{R_{\theta_1-\theta_2}}-\boxed{X_{-\theta_1}}-|0\rangle$$

"explode" w pr $\sin^2(-\theta_1) = \sin^2(\theta_1)$.

"survive" w pr $\cos^2(\theta_1)$.

$$\Pr[\text{"accept"} \mid \text{"survive"}] = \cos^2(\theta_2).$$

$$\Pr[\text{"reject"} \mid \text{"survive"}] = \sin^2(\theta_2).$$

say we are willing to tolerate ϵ prob. of explosion.

Want to pick Θ_1 s.t. $\epsilon = \sin^2(\Theta_1)$.

What Θ_2 should we pick?

Equivalent to comparing two biased coins.

Coin_{dud} tails with prob. $\sin^2(\Theta_1 - \Theta_2)$

$\text{Coin}_{\text{bomb}}$ tails with prob. $\sin^2(\Theta_2)$.

Pset 2 will discuss optimal distinguishing measurements.

For now, notice $\Theta_2 = \Theta_1$ yields that "dud" always accepts

and "bomb": explodes w pr ϵ,

rejects w pr $\epsilon(1-\epsilon) \approx \epsilon$

accepts w pr $(1-\epsilon)^2 \approx 1-2\epsilon$

some amount of bomb detection is going on!

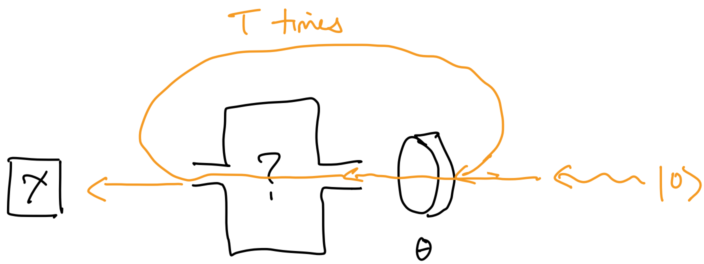
Can we do better?

Not if we send a fresh photon in each time.

(in class discussion as detectability and explosion prob. are roughly commensurate)

<u>Recycle photon.</u>

measure if $|0\rangle$ or $|1\rangle$



$$\boxed{X} - \underbrace{\boxed{?} - \cdots \boxed{?} - \boxed{R_\theta} - \boxed{?} - \boxed{R_\theta}}_{T \text{ times.}} - |0\rangle$$

pick $T = \dfrac{\pi}{2\theta}$.

If "dud", then $\left(-\boxed{R_\theta}-\right)^T = -\boxed{R_{T\theta}}- = -\boxed{R_{\pi/2}}-$

so circuit always outputs $|1\rangle$.

If "bomb", each pass through the black box either explodes with probability $\sin^2\theta$ or resets to $|0\rangle$ with prob. $\cos^2\theta$.

$$\text{Prob}[\text{explosion}] = \Pr[1^{st}\text{ exp.}] + \Pr[2^{nd}\text{ exp} \mid 1^{st}\text{ not}] + \dots + \Pr[T^{th}\text{ exp} \mid 1\text{–}T\text{ not}]$$

$$\leq \sum_{i=1}^{T} \Pr[i^{th}\text{ explosion}]$$

$$= T\sin^2\theta.$$

End state will be $|0\rangle$ then with prob. $\geq 1 - T\sin^2\theta$ and explosion with pr $\leq T\sin^2\theta$.

If explosion tolerance is ϵ then

$$T\sin^2\theta \approx \left(\frac{\pi}{2\theta}\right)\theta^2 = \frac{\pi\theta}{2} \leq \epsilon$$

pick $\theta = \frac{2\epsilon}{\pi} = O(\epsilon)$. $\quad T = O(\frac{1}{\epsilon})$.

Can detect if Bomb with only ϵ risk of explosion in time $O(\frac{1}{\epsilon})$.