Clarifications

Every quantum state $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ is a unit vec.

$$\begin{pmatrix} \psi(0\ldots0) \\ \psi(0\ldots1) \\ \psi(0\ldots10) \\ \vdots \\ \psi(1\ldots1) \end{pmatrix} = \begin{pmatrix} \psi(0) \\ \psi(1) \\ \vdots \\ \psi(2^n-1) \end{pmatrix}$$

$$|\psi\rangle = \sum_{x=0}^{2^n-1} \underbrace{\psi(x_1 x_2 \ldots x_n)}_{\text{amplitude}} |x_1, \ldots, x_n\rangle = \sum \psi(x)\,|x\rangle$$

$|\psi\rangle$ is classical if all amplitudes are 0 except 1.

$|\psi\rangle$ is in superposition if there are multiple non-zero amplitudes.

Unitary transforms:

A unitary $\mathcal{U} \in \mathbb{C}^{2^k \times 2^k}$ is also called a k-qubit unitary. In particular, $\mathcal{U} \in \mathbb{C}^{2\times 2}$ is a single-qubit unitary and $\mathcal{U} \in \mathbb{C}^{4\times 4}$ is a 2-qubit unitary.

$$\underbrace{\mathbb{1}_2}_{\substack{\text{acting on}\\ \text{qubit } 1}} \otimes \cdots \otimes \mathbb{1}_2 \otimes \underbrace{\mathcal{U}}_{\substack{\text{acting on}\\ \text{qubits } i \,\&\, i+1}} \otimes \mathbb{1}_2 \cdots \otimes \underbrace{\mathbb{1}_2}_{\substack{\text{acting on}\\ \text{qubit } n}}$$

is a general q.c. unitary transform.

say $\mathcal{U} = \begin{pmatrix} \mathcal{U}_{(0,0),(0,0)} & \mathcal{U}_{(0,0),(0,1)} & \cdots & \mathcal{U}_{(0,0),(1,1)} \\ \vdots & & & \\ \mathcal{U}_{(1,1),(0,0)} & \cdots & & \mathcal{U}_{(1,1),(1,1)} \end{pmatrix}$

i.e. $$\mathcal{U} = \sum_{k_1,k_2,j_1,j_2 \in \{0,1\}} \mathcal{U}_{(k_1,k_2)(j_1,j_2)} |k_1,k_2\rangle\langle j_1,j_2|$$

Then,

$$\left(\mathbb{1}_2 \otimes \cdots \otimes \mathbb{1}_2 \otimes U \otimes \mathbb{1}_2 \cdots \otimes \mathbb{1}_2\right) |x_1 \ldots x_n\rangle$$

$$= \left(|x_1\rangle|x_2\rangle \ldots |x_{i-1}\rangle\right) \otimes U|x_i, x_{i+1}\rangle \otimes \left(|x_{i+2}\rangle \ldots |x_n\rangle\right)$$

$$= \left(|x_1\rangle|x_2\rangle \ldots |x_{i-1}\rangle\right) \otimes \sum_{k_1, k_2} U_{(k_1,k_2)(x_i, x_{i+1})} |k_1, k_2\rangle \otimes \left(|x_{i+2}\rangle \ldots |x_n\rangle\right)$$

By linearity we can compute

$$\left(\mathbb{1}_2 \otimes \cdots \otimes \mathbb{1}_2 \otimes U \otimes \mathbb{1}_2 \cdots \otimes \mathbb{1}_2\right) |\Psi\rangle$$

for any $|\Psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ by expressing

$$|\Psi\rangle = \sum_{x_1 \ldots x_n} \underbrace{\Psi(x_1 \ldots x_n)}_{\text{amplitude.}} |x_1, \ldots, x_n\rangle$$

Today: Quantum's power over classical

1. Elitzar-Vaidman Bomb Tester
2. Deutsch-Josza 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 $U \in \mathbb{C}^{4\times 4}$, we can transform the state $|\psi\rangle$ to
$$\left[\underbrace{\mathbb{1}_2 \otimes \cdots \otimes \mathbb{1}_2}_{l_1} \otimes U \otimes \underbrace{\mathbb{1}_2 \otimes \cdots \otimes \mathbb{1}_2}_{l_2} \right] |\psi\rangle$$
$l_1 + 2 + l_2 = n$

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

Obs 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 $|\langle b_1|\psi\rangle|^2$.

Ans 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 $\mathcal{U}^\dagger|b_i\rangle = |i\rangle$.

Algorithm

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.

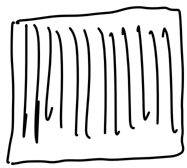
Photons have a polarization:

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:

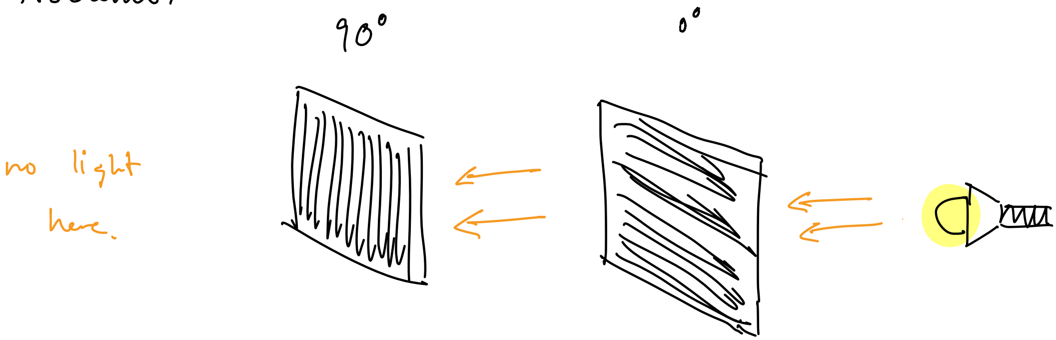
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix}\alpha \\ \beta\end{pmatrix}$$ state of photon before.

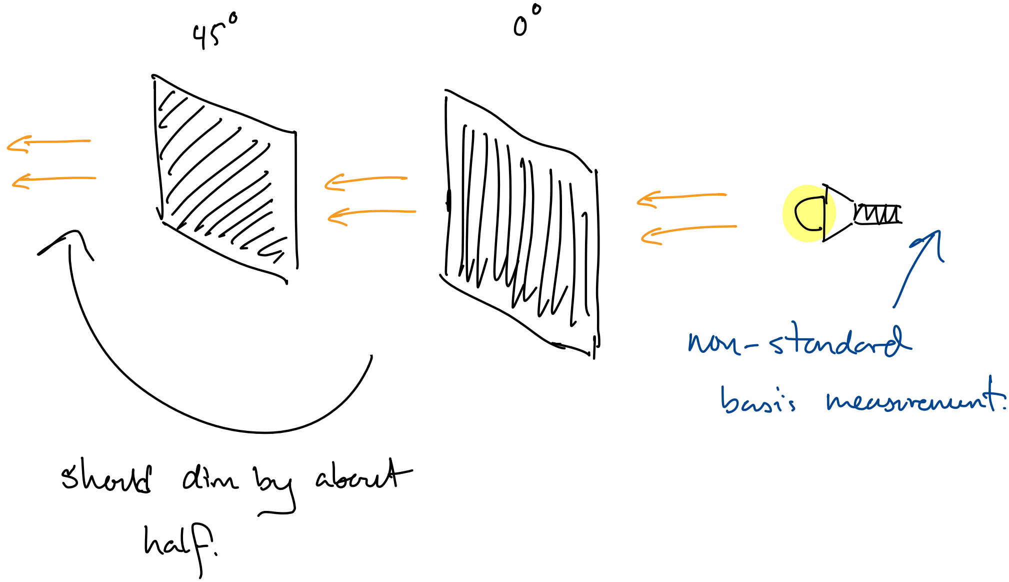
collapses to either $|0\rangle$ "bounces back" w pr $|\alpha|^2$

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

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

Problems:

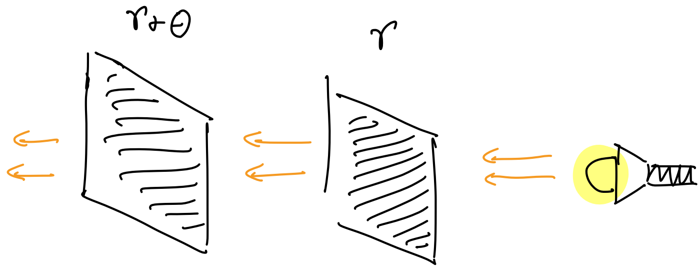




Another way to analyze this is to notice that a sieve at angle θ is measuring the qubit in a non-standard basis given by

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

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



What fraction of light passes through?

$$\Pr\left[\ \boxed{7}_{\theta+\gamma} \text{ measurement accepts } |b_0^\gamma\rangle\right]$$

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

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

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

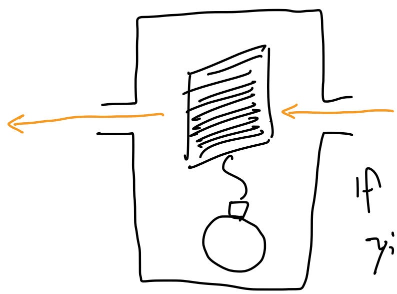
Elitzur-Vaidman Bomb Tester (1993)

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

(a) A photon enters and a photon leaves.

(b) you know it is 1 of 2 possibilities:

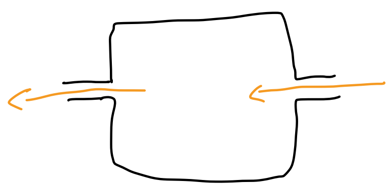
"Bomb"



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

no difference.

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

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

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

Bomb: Explosion

too much difference.

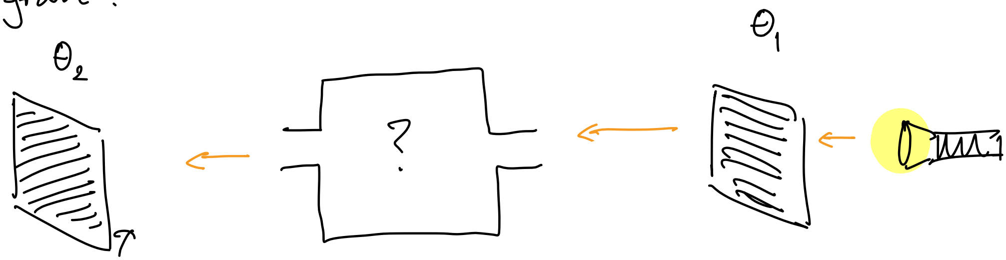
Model the Dud as the identity transform

the Bomb as a standard basis measurement.

Let's send in a rotated state

and measure the output in a rotated basis.

Diagram:



measure if
pass or reflects.

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

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

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

Quantum circuit:

θ_2 basis measurement

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

by prev. we can write it as

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

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

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

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

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

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

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

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

$$-\boxed{\chi}-\boxed{R_{\theta_1-\theta_2}}-\boxed{\chi_{-\theta_1}}-|0\rangle$$

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

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

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

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

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 $(1-\epsilon)^2 \approx 1-2\epsilon$

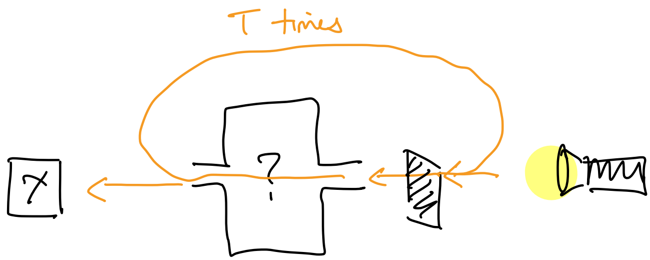
some amount of bomb detection is going on!

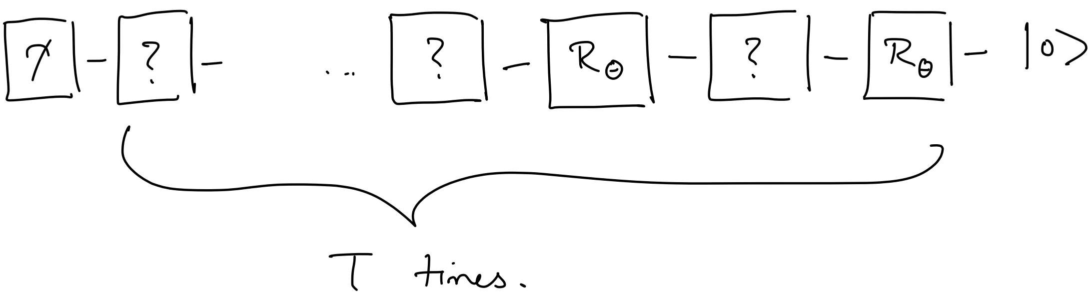
Can we do better?

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>.





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

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

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

post-measurement d.m.

$$\rho_a' = \frac{(|0\rangle\langle 0| \otimes \mathbb{1})\, |\psi_a\rangle\langle\psi_a|\, (|0\rangle\langle 0| \otimes \mathbb{1})}{tr(|0\rangle\langle 0| \otimes \mathbb{1}\, |\psi_a\rangle\langle\psi_a|)}.$$

put these 2 together, we get measurement of $|\psi_a\rangle\langle\psi_a|$ result. So now

ρ' ← post 0 measurement should be defined as

$$\rho' = \sum_a pr(a \mid x=0) \cdot \rho_a'$$

$$= \sum_a \frac{pr(a \mid x=0)}{pr(x=0 \mid a)} (|0\rangle\langle 0| \otimes \mathbb{1})\, |\psi_a\rangle\langle\psi_a|\, (|0\rangle\langle 0| \otimes \mathbb{1})$$

$$= \sum_a \frac{pr(a)}{pr(x=0)} (|0\rangle\langle 0| \otimes \mathbb{1})\, |\psi_a\rangle\langle\psi_a|\, (|0\rangle\langle 0| \otimes \mathbb{1})$$

$$= \frac{(|0\rangle\langle 0| \otimes \mathbb{1})\, \rho\, (|0\rangle\langle 0| \otimes \mathbb{1})}{\sum_a pr(x=0 \mid a)\, p_a}$$

$$= \frac{(|0\rangle\langle 0| \otimes \mathbb{1})\, \rho\, (|0\rangle\langle 0| \otimes \mathbb{1})}{\sum_a p_a\, tr(|0\rangle\langle 0| \otimes \mathbb{1}\, |\psi_a\rangle\langle\psi_a|)} =$$