Announcement:

- A few extra positions for enrollment.
- send your (name, ID) to me.
- has to be through my special permission.

$$M \cdot M^T = I$$

Examples of Orthogonal Matrices

① $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ (trivial example)

② $R_\theta = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$ $\theta \in [0, 2\pi]$

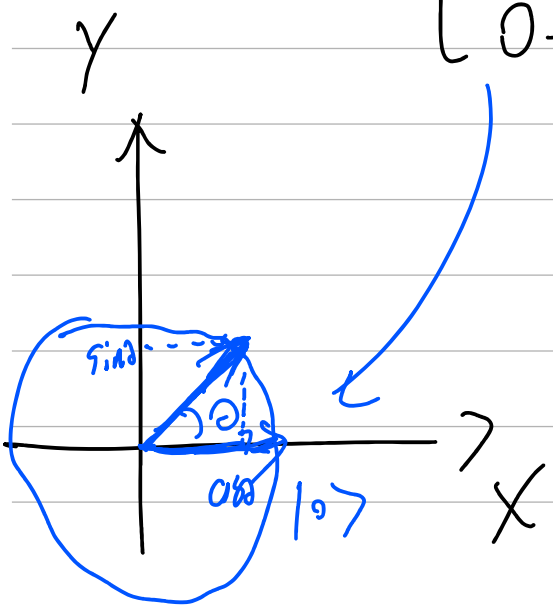
(counter clock-wise rotation)

$R(-\theta) = ?$

$$R_\theta \cdot |0\rangle = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$\downarrow$$

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \cos\theta \\ \sin\theta \end{bmatrix}$$



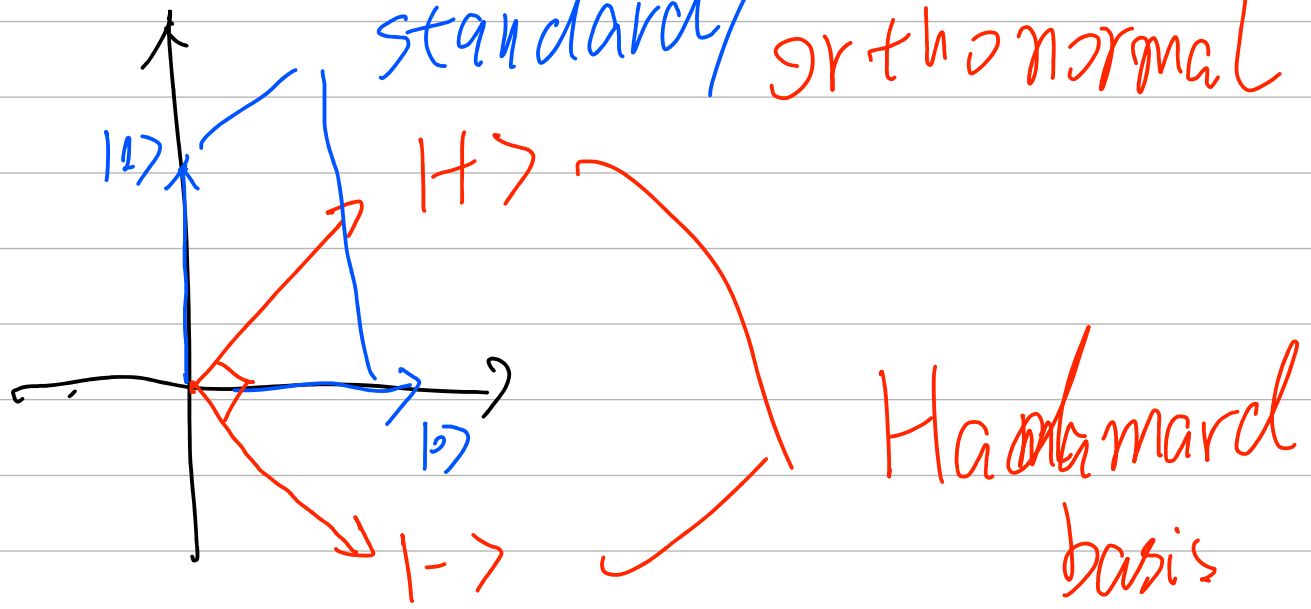
③

$$H = \frac{1}{\sqrt{2}} \cdot \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad \text{(Hadamard gate)}$$

$$H \cdot |0\rangle = \frac{1}{\sqrt{2}} \cdot \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = |+\rangle$$

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

- Hadamard basis, standard / computational basis, orthonormal



$$\sigma_z |+\rangle = |-\rangle$$

$$\sigma_z |-\rangle = |+\rangle$$

③ $\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ (Pauli X)

$\sigma_x |0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$

$\sigma_x |1\rangle = \cdots = |0\rangle$

superposition

$\sigma_x (\alpha|0\rangle + \beta|1\rangle) = ?$ $\alpha|1\rangle + \beta|0\rangle$

NOT-gate in classical computing.

④ $\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ (Pauli z)

phase

$\sigma_z \cdot |0\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$

$\sigma_z \cdot |1\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ -1 \end{bmatrix} = -|1\rangle$

$\sigma_z \cdot (\alpha|0\rangle + \beta|1\rangle) = ?$

$\sigma_z \cdot |+\rangle = ?$

(Pauli Y ?)

Postulate 4: Null.

It's about how multiple qubits compose into a whole system

Summary:

Postulate 1: A quantum register encode a "unit circle" $|\psi\rangle = \alpha|0\rangle + \beta \cdot |1\rangle$.

Postulate 2: When we "measure" a qubit $|\psi\rangle = \alpha|0\rangle + \beta \cdot |1\rangle$, it "collapses" to $|0\rangle$ with probability α^2, and "collapses" to $|1\rangle$ with probability β^2.

Postulate 3: Evolution of a single qubit must be a 2X2 orthogonal matrix multipled on the left side of the qubit I.e. $|\phi\rangle = M \cdot |\psi\rangle$, where M is a 2X2 orthogonal matrix

Applications of our over-simplified one-qubit quantum system:

- Truely random number generator
- Elitzur-Vaidman Bomb
- BB84 Quantum Key Exchange / Distribution (QKD)

Truly random number generator

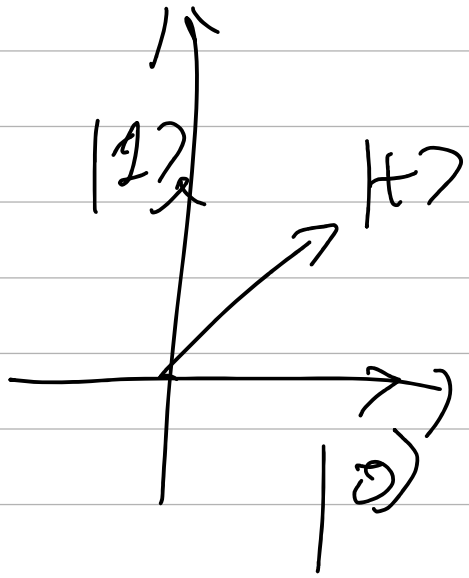
- "True" randomness is expensive,
- You can never be sure about if a source of randomness is truly random. in classical physics. (Past Choices.)
  - Sunspot activities / solar phenomenon (solar flares, blackspot bursts)

(highly complex and chaotic processes)

Problematic !

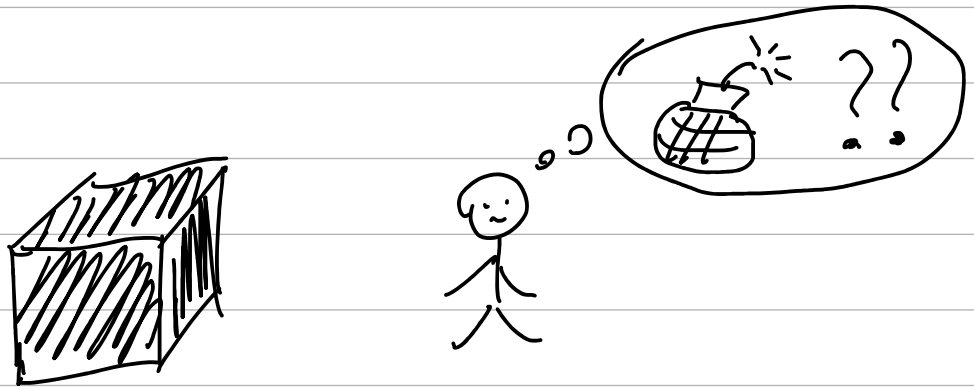
$$H \cdot |0\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$\begin{bmatrix} \alpha|0\rangle + \beta|1\rangle \\ \alpha^2 \quad\quad \beta^2 \end{bmatrix}$$



Elitzur-Vaidman Bomb: Shor 1994

(First proposed in the early 1990's)



If there is a bomb inside, it will immediately explode once the box is opened

We can solve the problem safely by using a "quantum interrogation"

0 — not open } decision.

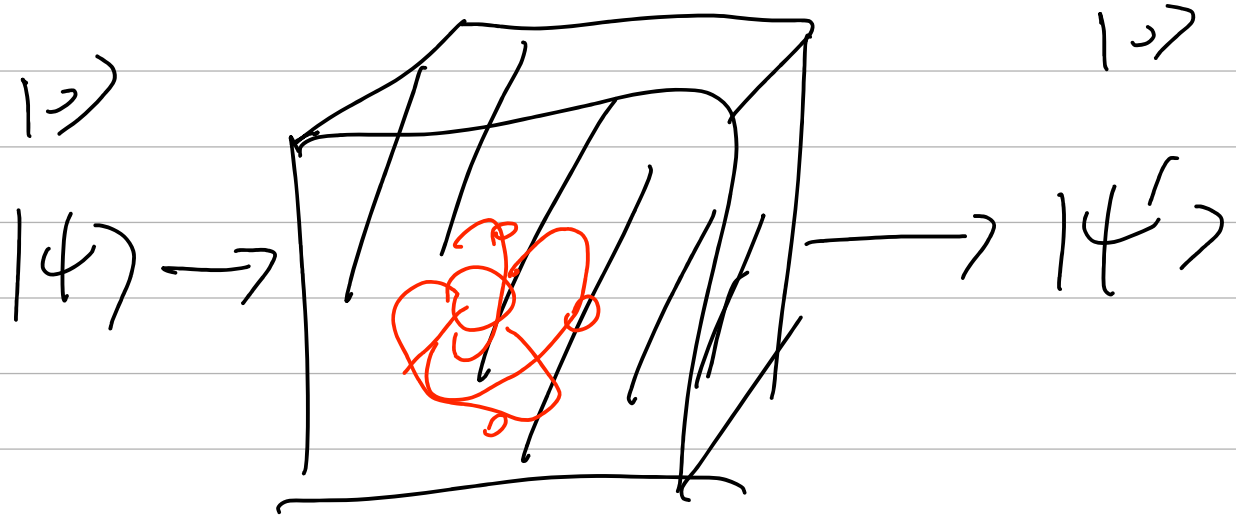
1 — open

Derivation:

2. Version

2. decision(qu)bit

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$



Q suitcase

If bomb: measure $|\psi\rangle$ in $\{|0\rangle, |1\rangle\}$

- outcome: $|0\rangle$ → nothing. ✓
- outcome: $|1\rangle$ → explode ✗

No bomb:

return $|\psi\rangle$ back to you, untouched.

R_ε $\quad \varepsilon \in [0, 1)$

Pick a number $T = \frac{\pi}{2\varepsilon}$

Init $|\psi_0\rangle = |0\rangle$

For i in $\{1, 2, \ldots, T\}$:

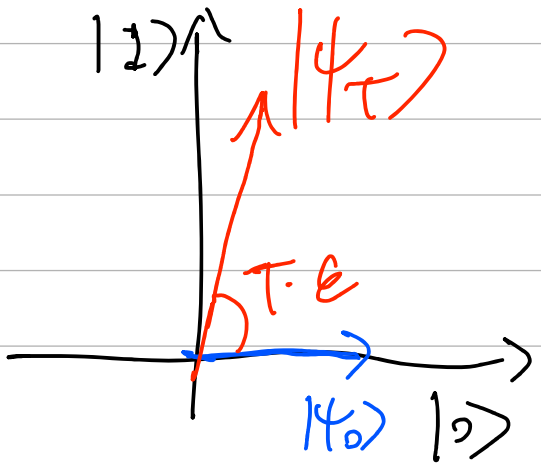
- Update $|\psi_i\rangle = R_\varepsilon \cdot |\psi_{i-1}\rangle$
- Query using $|\psi_i\rangle$

At the end:

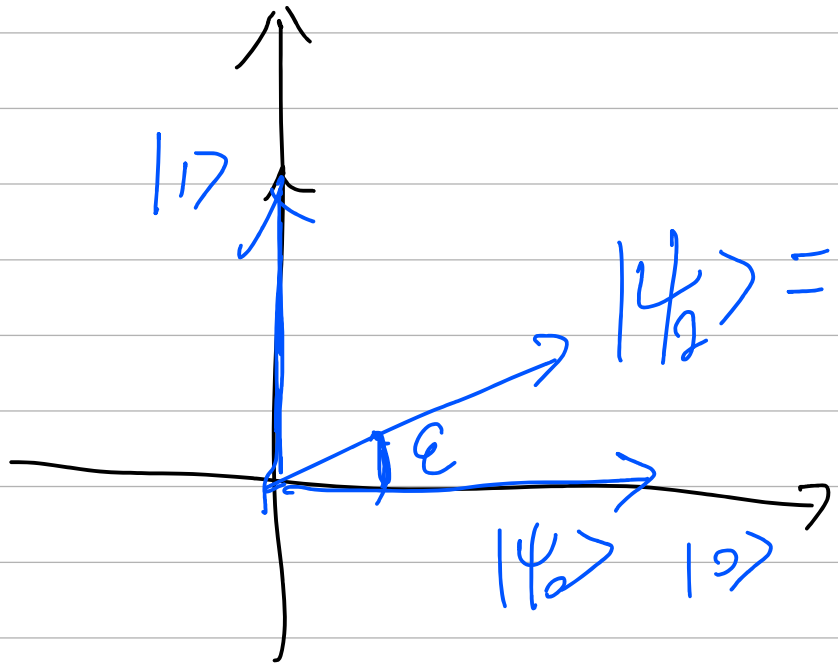
measure $|\psi_T\rangle$ $\begin{cases} |1\rangle \text{ — no bomb} \\ |0\rangle \text{ — bomb} \end{cases}$

- $\{|0\rangle, |1\rangle\}$ comp/stand basis

If No bomb:



bomb.



{ Safe: w.p. $\cos^2(\varepsilon)$

Explode: w.p. $\sin^2(\varepsilon) \approx \varepsilon^2$

$\varepsilon = 0.00000001$

[$\sin(x) \sim x$ if x small

Assume safe for T times, $|\psi_T\rangle = |0\rangle$

$Safe_T$

$\Pr[Safe_T] \geq 1 - T \cdot \sin^2\varepsilon$ ← union bound

$= 1 - T \cdot \varepsilon^2$

$$T = \frac{\pi}{2\varepsilon}$$

$$1 - T \cdot \varepsilon^2 = \underbrace{1 - \frac{\pi}{2}\varepsilon}$$

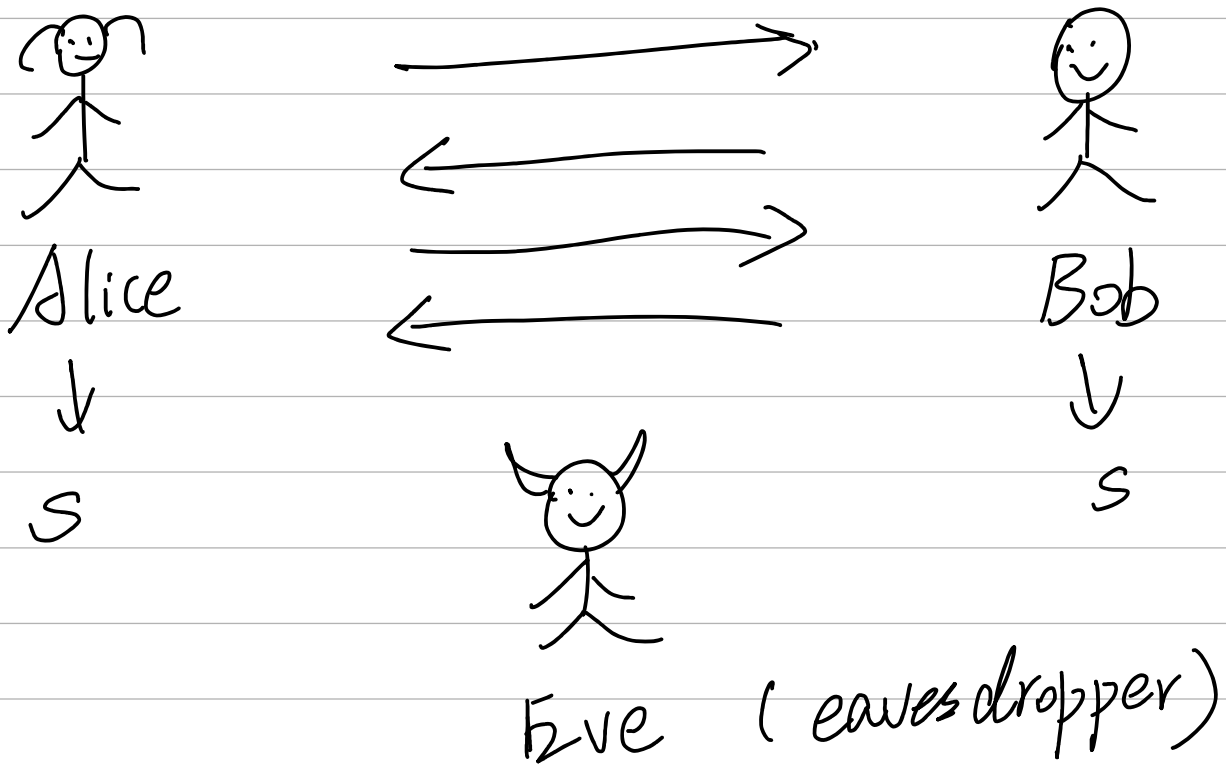
Risk tolerance bound

$$\varepsilon = \frac{0.0000001}{\pi/2}$$

$$\Pr[\text{safe}] \geq 1 - 0.0000001$$

Year 1984

BB84 Quantum Key Distribution. (QKD)



Classical Solution:

Public-key Encryption (PKE)

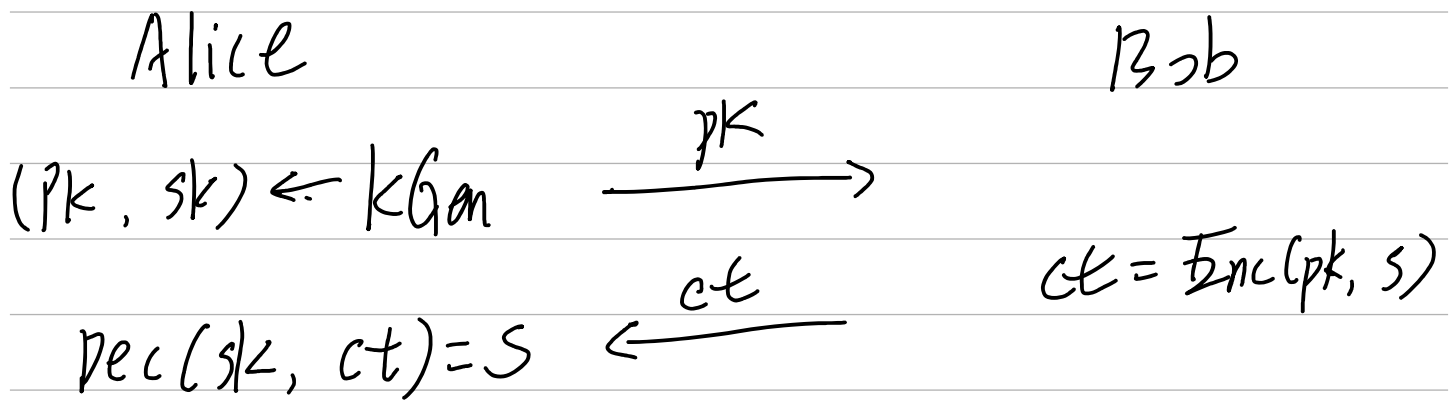
- KGen → (pk, sk)
- Enc(pk, m) → ct
- Dec(sk, ct) → m

- RSA
- DH
- Factoring
- Dislog

Two requirements for PKE:

- Correctness.

- Security;



"Problems."

- PKE requires "hardness assumptions"

RSA, Factoring.

- Classically, PKE is necessary for this task,

⇒ "assumptions" are necessary for classical key distribution.

The BB84 Solution:

Alice

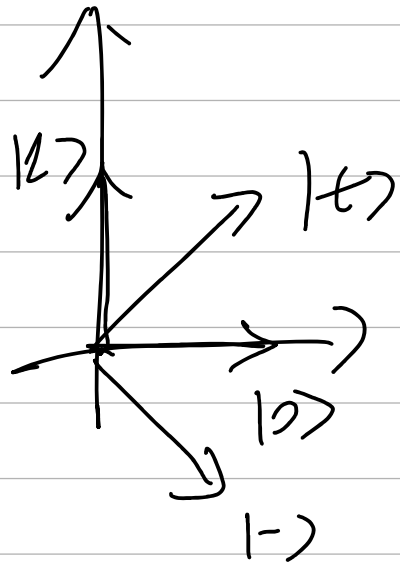
For $i = 1$ to n.

$x_i \leftarrow \{0,1\}$

$y_i \leftarrow \{0,1\}$

$$|\psi_i\rangle = \begin{cases} |0\rangle & x_i = 0,\ y_i = 0 \\ |1\rangle & x_i = 0,\ y_i = 1 \\ |+\rangle & x_i = 1,\ y_i = 0 \\ |-\rangle & x_i = 1,\ y_i = 1 \end{cases}$$

Bob



$|\psi_1\rangle \cdots |\psi_n\rangle$ →

For $i = 1$ to n

$x_i' \leftarrow \{0,1\}$

measure $|\psi_i\rangle$ { if $x_i' = 0$, in $\{|0\rangle, |1\rangle\}$ basis; if $x_i' = 2$, in $\{|+\rangle, |-\rangle\}$ basis }

$\{x_i\}_{i=2}^{n}$ →

← $\{x_i'\}$

Outcome: y_i'

set s be concatenation of y_j's where $j \in \{j : x_j = x_j'\}$

set s be concatenation of y_j''s where $j \in \{j : x_j = x_j'\}$.

Why complex numbers in QM?

$$\alpha|\Sigma\rangle + \beta|\Phi\rangle$$

short-answer: Law of QM

long-answer:

1 (a) Complex numbers are not unique to QM

Oscillator / sound wave

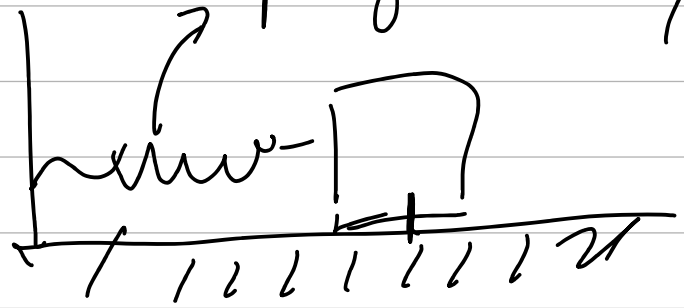
classical Vibration

Mechanics

(b) QM ↗ similar.

2. No. QM needs complex numbers in an essential way.

{ hyp 2: Real-QM
{ hyp 2: Comp-QM



Simple harmonic Oscillator.
(简谐振动)

$$\begin{cases} F = -kx \rightarrow \text{position} \\ \quad\quad \downarrow \\ \quad\quad \text{hook parameter} \\ F = m\vec{a} \end{cases}$$

$$\left(\frac{d^2}{dt^2}x\right) + \left(\frac{k}{m}\right)x = 0$$

$$\left[i\hbar\frac{d}{dt}|\psi\rangle = \hat{H}(|\psi\rangle)\right]$$

$\frac{k}{m}$

$$x(t) = C \cdot \cos(\omega t + \varphi)$$

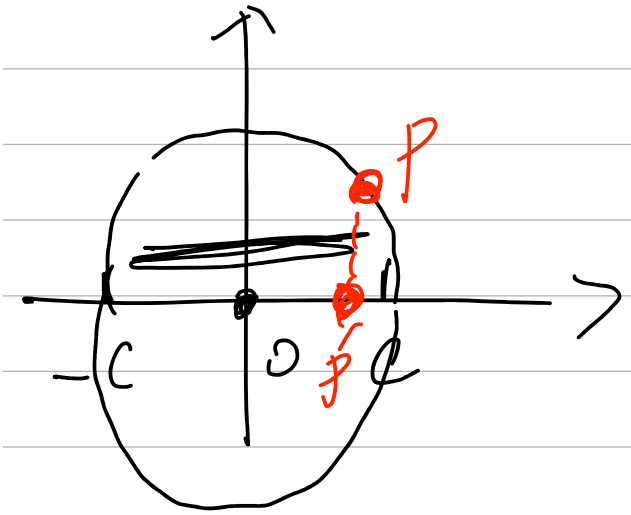
C ↑ ω ↑ φ ↑

angular frequency.

full solution

$$x(t) = C \cdot e^{i(\omega t + \varphi)}$$

$$= C \cdot \left[\cos(\omega t + \varphi) + i\sin(\omega t + \varphi)\right]$$



$$\int_0^{\frac{1}{2}} \cos^2(x)\,dx$$

Full-fledged Postulates of (Complex-number) QM

Postulate 1: An isolated quantum system is completed described by its vector of state, which is a unit vector in a Hilbert space.

- vector space (Real / complex)
- inner-product space
- complete.