NAS-IF Summer School for Young Physicists 2022

Quantum Information

Scope of QIS

Exploratory field. No single grand question.

- Building a quantum computer (QC) Acronym coined by John Preskill

  Now we have 50-100 qubit NISQ (Noisy Intermediate-Scale Quantum) devices. We want to build a scalable, fault-tolerant quantum computer that can perform large scale quantum computation of indefinite length

- What to do with QCs once we have them?

  Quantum algorithms, simulation of quantum systems e.g. quantum chemistry, drug discovery

- Quantum vs Classical information

  Quantum Shannon theory, communication

- Applications to classical computer science e.g. quantum-inspired algorithms

- Applications to physics e.g. HEP, cond-mat

Statistical experiment

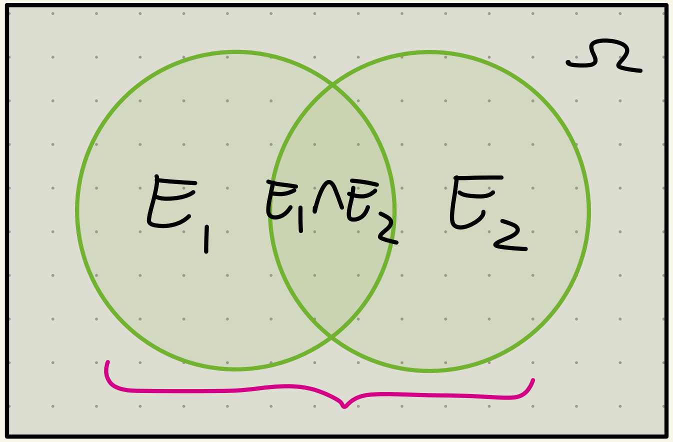
Denote by Ω the set of all possible outcomes/events. (Ω is called a sample space.)
A model (possibly unknown) of a statistical experiment assigns probabilities to all events $E \subset \Omega$.

Random variable

$\Pr(X=E)$

Logical AND $\wedge$, OR $\vee$, NOT $\neg$

Probability axioms



$E_1 \vee E_2$

1. $\Pr(E) \geq 0$
2. $\Pr(\Omega) = 1$
3. $\Pr(E_1 \vee E_2) = \Pr(E_1) + \Pr(E_2)$
   if $E_1 \wedge E_2 = 0$

Everything else can be derived from these three axioms, for example that $\Pr(\neg E) = 1 - \Pr(E)$ or $\Pr(E_1 \vee E_2) = \Pr(E_1) + \Pr(E_2) - \Pr(E_1 \wedge E_2)$ for an arbitrary pair of events.

$$\Pr(E_1 | E_2) := \frac{\Pr(E_1 \wedge E_2)}{\Pr(E_2)}$$ (Conditional probability)

$$\Pr(E_1 | E_2) = \frac{\Pr(E_2 | E_1)\Pr(E_1)}{\Pr(E_2)}$$ (Bayes' rule)

Mutually exclusive $\iff E_1 \wedge E_2 = \phi$

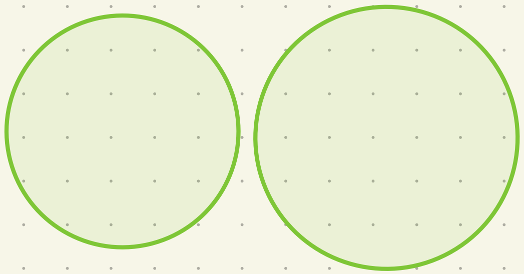
Independent $\iff Pr(E_1 \wedge E_2) = Pr(E_1) Pr(E_2)$

Remarks

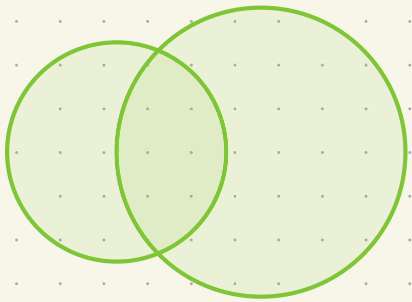
① Mutually exclusive events can't be independent; if a coin flip comes up head, I know that it did not come up tail.

- $E_1 \wedge E_2 = \phi \Rightarrow Pr(E_1 \wedge E_2) = 0$. But $Pr(E_1 \wedge E_2) = Pr(E_1) Pr(E_2)$ can't be 0 if $Pr(E_1), Pr(E_2) > 0$. □

② Independence can't be easily visualized on a Venn diagram, in contrast to mutual exclusivity, since an area in a Venn diagram doesn't conventionally represent probability



Mutually exclusive



Merely overlapping doesn't gaurantee independence

Space of probability distributions (Discrete random variables)

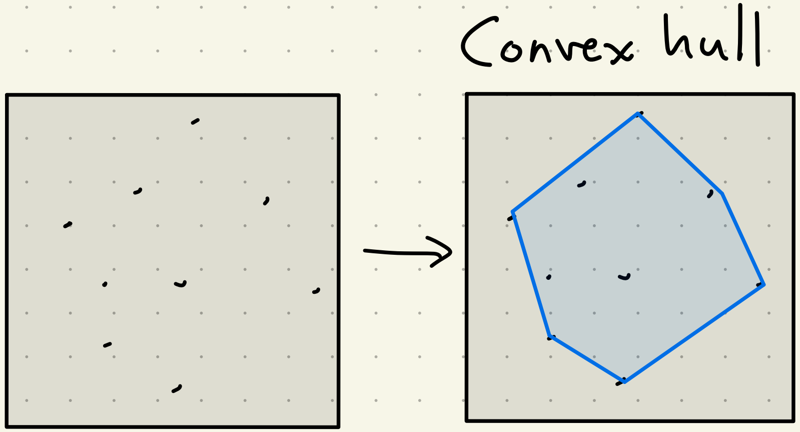
Probability distributions are real vectors, the components of which are positive and sum to 1.

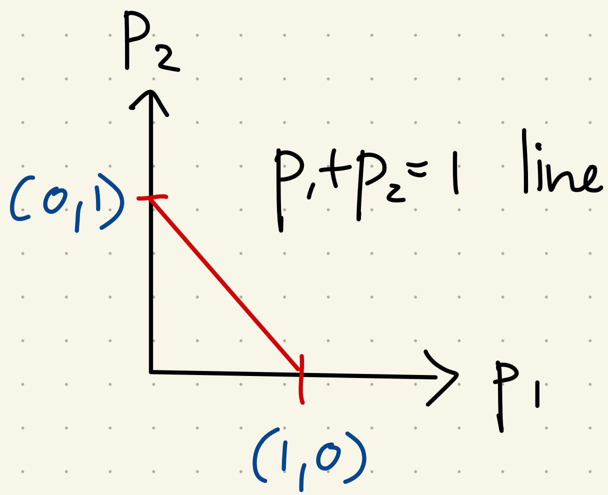
$$\vec{p} = \begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_d \end{pmatrix} \qquad \forall p_j \geq 0 \qquad \sum_j p_j = 0$$

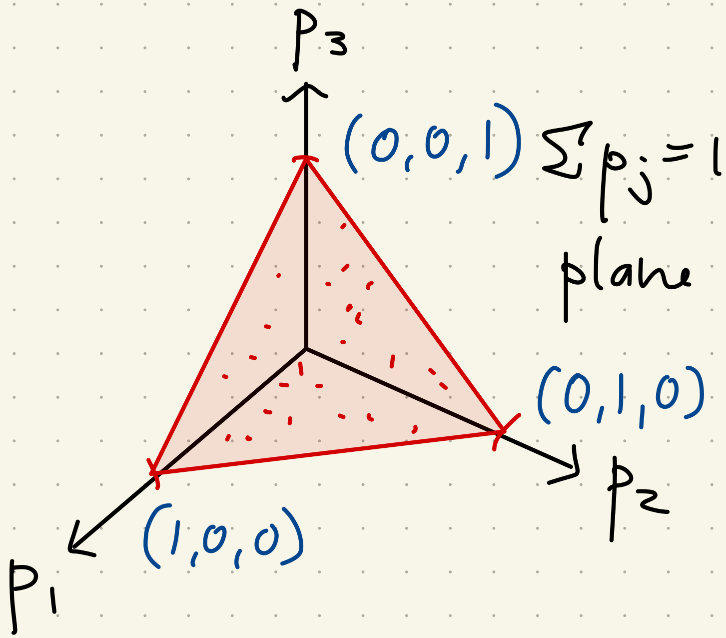
Geometrically, probability vectors are convex combinations of unit vectors $(0 \cdots 0\,1\,0 \cdots 0)^T$, which represents experiments with no randomness.

$$\lambda \vec{p} + (1-\lambda)\vec{q}, \quad \lambda > 0$$

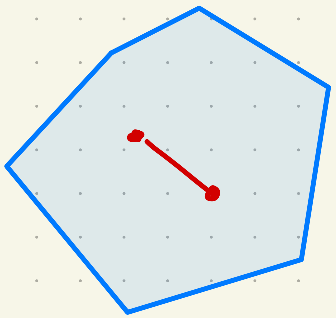
So the set of all probability distributions is the convex hull of these unit vectors.



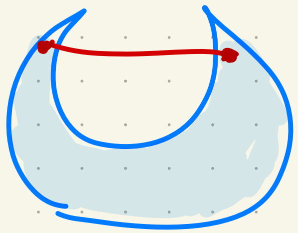




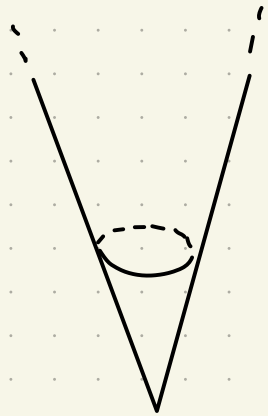
These $(d-1)$-dimensional hyperplanes are called d-simplices (Singular: simplex)
They are examples of closed and bounded convex sets. Every point in such a convex set can be written as a convex combination of extremal points, by virtue of the Krein-Milman theorem.



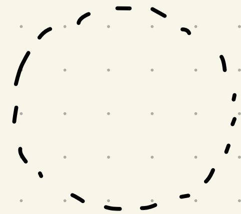
Convex
✓



Not convex
✗



Cone
Not bounded



Open set
No extremal points

In the context of generalized probabilistic theories (Quantum theory is one such theory), extremal points are also called pure states as opposed to mixtures or mixed states similar to how all colors but the primary colors are mixtures of the primary colors.

Comments

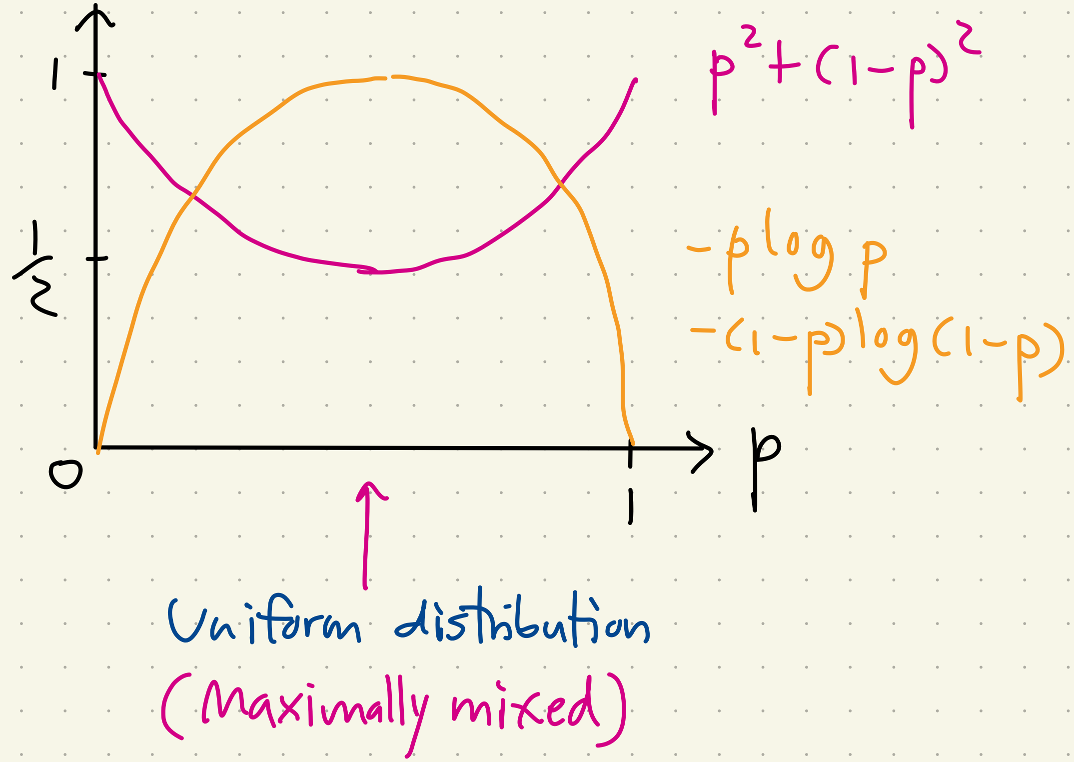
① In classical theory, every mixture is a unique convex combination of pure states. The fact that this doesn't hold in quantum theory is associated to several non-classical features such as entanglement, as we will see.

② The more mixed the distribution is, the more randomness. And there're many way to measure "mixedness"!

2.1 $\sum_j p_j^2$ (Purity)

2.2 $-\sum_j p_j \log p_j$ (Shannon entropy) base-2 log

2.3 or just the number of non-zero elements in the probability vector.

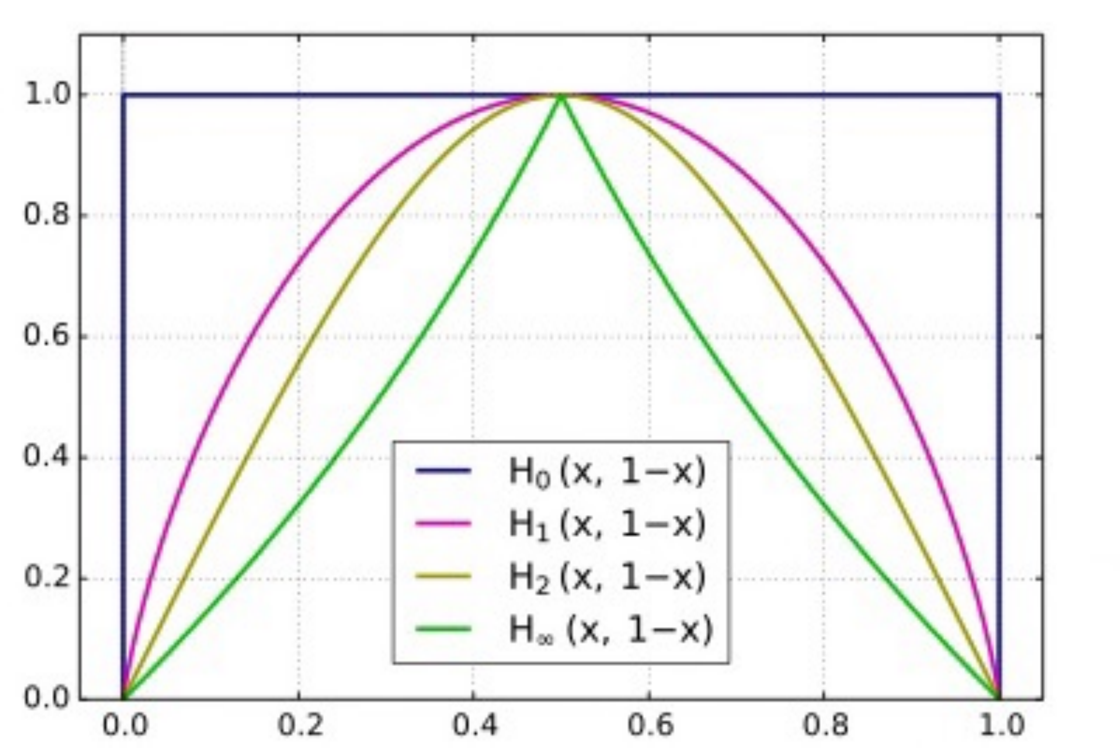


In fact, all three measures are related.

Entropy axioms (Khinchin)

1. H is invariant under re-labelling of the outcomes.
2. H is maximum at the uniform distribution.
3. Padding the probability vector by zeros does not change H.
4. $H(X,Y) = H(X) + \sum_j p_j H(Y|X=j)$

The Shannon entropy satisfies all four axioms, but the first three also seem to be perfectly good criteria for measures of uncertainty by themselves. In fact, they characterize the infinite family of Rényi entropies.



Rényi entropies

$$H_\alpha(\vec{p}) = \frac{1}{1-\alpha} \log\left(\sum_j p_j^\alpha\right)$$

(Defining $0 \log 0 = 0$ and $0^0 = 0$)

① $H_0 = \log$ (# nonzero elements)

② $H_1 = \frac{0}{0}$ so we have to take the limit as $\alpha \to 1$ using L'Hospital rule, which gives the Shannon entropy

③ $H_2 = -\log\left(\sum_j p_j^2\right)$ Negative log of the purity

The point is that there are many measures of randomness from which you can choose based on the application and ease of calculation.

Setup and the bra-ket notation

① Complex vectors $u = \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_d \end{pmatrix}$ $\forall a_j \in \mathbb{C}$

Inner product $\sum_{j=1}^{d} u_j^* v_j$

This representation of vectors implicitly identify the vector space V as the space of d-tuples $\mathbb{C}^d$ (that is, fixing the "standard basis")

Reminder

$z = a + ib$ (Argand) $= re^{i\theta}$ (Polar)

$a, b \in \mathbb{R}$ $\qquad r \geq 0,\ \theta \in [0, 2\pi)$

$z^* = a - ib$ (Complex conjugate)

$|z| = \sqrt{zz^*} = \sqrt{a^2 + b^2} = r$

② Complex functions $f(x)$ Inner product $\int dx\, f^*(x)\, g(x)$

We will focus exclusively on the first example (finite dimension)

The point of linear algebra is to understand which quantities/formulas depend on a basis and which do not. (basis independent/coördinate-free)

Basis $\{|e_j\rangle\}_{j=1,2,\dots,d}$ $\qquad |\psi\rangle = \sum_j c_j |e_j\rangle$

Inner product

$u, v, w \in V$
$a, b \in \mathbb{C}$

Pairing map $V \times V \to \mathbb{C}$ with the following properties.

1. Linearity (in the 2nd argument): $(u, av + bw) = a(u,v) + b(u,w)$
2. Conjugate symmetry: $(u,v)^* = (v,u)$
3. Positive definiteness: $(u,u) \geq 0$ with equality iff $u = 0$

Remark

② $\Longrightarrow$ Conjugate linearity in the 1st argument.

■ If $(av+bw, u) = (u, av+bw)^* = a^*(v,u) + b^*(w,u)$ □

An inner product comes from considering the space V^* (the dual space) of linear maps from V to $\mathbb{C}$ (linear functionals). Denote $\underset{V^*}{v}(\underset{V}{u}) =: \langle v | u \rangle$.

$\dim V^* = \dim V = d$

■ Picking a basis $\{|e_j\rangle\}_j$ for V also pick a basis $\{\langle f_j|\}_j$ for V^* by the defining relation $\langle f_j | e_k \rangle = \delta_{jk}$ (bi-orthogonal system), and there can't be $\langle v| \neq 0$ s.t. $\langle v|u\rangle = 0 \ \forall u$. □

Note that at this point, we don't have an inner product yet. We only have a pairing $V^* \times V \to \mathbb{C}$ of vectors from different spaces. We need a rule to translate between vectors in V and V^*. This can always be done but there is no unique way to do this. The most convenient way is to pick an orthonormal basis

$$(e_j, e_k) = \delta_{jk}.$$

To reproduce $(v,u) = v(u) =: \langle v|u\rangle$ then, we just need to identify a linear functional $v \in V^*$ with the vector $\sum_j [v(e_j)]^* e_j \in V$.

Why? Because

$$\underset{\substack{\uparrow \\ V}}{(v,u)} = \sum_j c_j\, v(e_j) \qquad \text{(Linearity in the 2nd argument)}$$

$$= \sum_{jk} c_j\, v(e_k)(e_k, e_j) \qquad \text{(Conjugate linearity in the 1st argument)}$$

$$= \sum_{jk} c_j\, v(e_k)\,\delta_{jk} = \sum_j c_j\, v(e_j) = v\Big(\sum_j c_j e_j\Big) = \overset{\substack{V^* \\ \downarrow}}{v}(u) =: \langle v|u\rangle$$

This may look confusing, but the upshot is that, in an orthonormal basis (ONB) $\{|e_j\rangle\}_j$ s.t. $\langle e_j|e_k\rangle = \delta_{jk}$, we have the identification

$$|u\rangle = \sum_j c_j |e_j\rangle \longleftrightarrow \langle u| = \sum_j c_j^* \langle e_j|$$

(Riez representation theorem)

$$\begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{d-1} \end{pmatrix} \longleftrightarrow \begin{pmatrix} c_0^* & c_1^* & \cdots & c_{d-1}^* \end{pmatrix}$$

One-to-one correspondence between bras and kets

In such an ONB, the inner product becomes

$$\langle u|v\rangle = \sum_{jk} u_j^* v_k \langle e_j|e_k\rangle = \sum_{jk} u_j^* v_k .$$

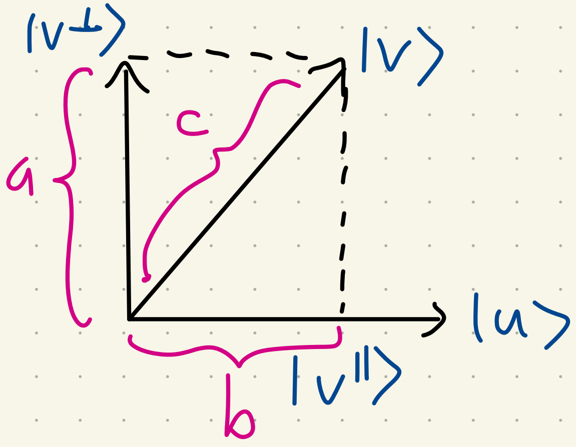
The norm

$$\|u\| = \sqrt{\langle u|u\rangle} = \sqrt{\sum_j |u_j|^2} .$$

But beware that there are only true in an ONB!

Cauchy-Schwarz inequality

$$|\langle u|v\rangle|^2 \leq \langle u|u\rangle\langle v|v\rangle$$

- 

$$|v^\perp\rangle = |v\rangle - |v^\parallel\rangle = |v\rangle - \frac{\langle u|v\rangle}{\langle u|u\rangle}|u\rangle$$

By Pythagorean Theorem, $a^2 + b^2 = c^2$

$$\langle v^\perp|v^\perp\rangle + \langle v^\parallel|v^\parallel\rangle = \langle v|v\rangle$$

$$0 \leq \langle v^\parallel|v^\parallel\rangle = \langle v|v\rangle - \frac{|\langle u|v\rangle|^2}{\langle u|u\rangle}$$

$$\Longrightarrow \quad |\langle u|v\rangle|^2 \leq \langle u|u\rangle\langle v|v\rangle \quad \square$$

Used in quantum computation/algorithm, quantum metrology

Linear operator $A(a|u\rangle + b|v\rangle) = aA|u\rangle + bA|v\rangle$

The action of A is completely determined by its action on basis vectors.

Fix an ONB $\{|j\rangle\}_{j=0,1,\dots,d-1}$, $|j\rangle\langle k|$ is a linear operator that map a bais vector $|k\rangle$ to $|j\rangle$ (and maps $|\ell\rangle$, $\ell \neq k$, to 0).

$$A_{00}|0\rangle\langle 0| + A_{01}|0\rangle\langle 1| + A_{10}|1\rangle\langle 0| + A_{11}|1\rangle\langle 1| \longleftrightarrow \begin{pmatrix} A_{00} & A_{01} \\ A_{10} & A_{11} \end{pmatrix}$$

$$\begin{tikzcd} \text{Operator} \arrow[r, bend left, "A_{jk} = \langle j|A|k\rangle"] & \text{Matrix elements} \arrow[l, bend left, "A = \sum_{jk} A_{jk}|j\rangle\langle k|"] \end{tikzcd}$$

Tranformation of components and bais vectors are in a sense "opposite"

$$\begin{pmatrix} v_0 \\ v_1 \end{pmatrix} = \begin{pmatrix} A_{00} & A_{01} \\ A_{10} & A_{11} \end{pmatrix} \begin{pmatrix} u_0 \\ u_1 \end{pmatrix}$$

$$\iff v_j = \sum_k A_{jk} u_k$$

(The jth bais vector is mapped to the jth column) $\quad A|e_j\rangle = \sum_k A_{kj}|e_j\rangle$

Resolution of the identity $\mathbb{1} = \sum_j |e_j\rangle\langle e_j|$ for any ONB $\{|e_j\rangle\}_j$

Extremely useful, make conversions to different bases / matrix forms automatic.

Examples

$$|\psi\rangle = \mathbb{1}|\psi\rangle = \sum_j |e_j\rangle\langle e_j|\psi\rangle = \sum_j \overbrace{\langle e_j|\psi\rangle}^{c_j} |e_j\rangle$$

$$A = \mathbb{1} A \mathbb{1} = \sum_{jk} |e_j\rangle\langle e_j|A|e_k\rangle\langle e_k| = \sum_{jk} \overbrace{\langle e_j|A|e_k\rangle}^{A_{jk}} |e_j\rangle\langle e_k|$$

$$|\psi\rangle = \int dx\, |x\rangle\langle x|\psi\rangle = \int dx\, \overbrace{\langle x|\psi\rangle}^{\psi(x)} |x\rangle$$ (Wave Function)

$$|\psi\rangle = \int dp \int dx\, |p\rangle\langle p|x\rangle\langle x|\psi\rangle = \int dp \underbrace{\left(\int dx\, \psi(x) \overbrace{\langle p|x\rangle}^{e^{-ipx/\hbar}}\right)}_{\tilde{\varphi}(p)} |p\rangle$$

(Fourier transform to momentum-space wave function)

Adjoint Implicit definition $(u, Av) = (A^\dagger u, v)$

$$\langle u|(A|v\rangle) = (\langle u|A)|v\rangle \text{ where } \langle u|A \leftrightarrow A^\dagger|u\rangle$$

$$(aA+bB)^\dagger = a^* A^\dagger + b^* B^\dagger$$

$$(AB)^\dagger = B^\dagger A^\dagger$$

$$(A^\dagger)^\dagger = A$$

$$(|u\rangle\langle v|)^\dagger = |v\rangle\langle u|$$

In ONB, the matrix form of $A^\dagger$ is the conjugate transpose

$$A^\dagger \leftrightarrow \begin{pmatrix} A_{00}^* & A_{10}^* \\ A_{01}^* & A_{11}^* \end{pmatrix}$$

Again, this is only true in an ONB!

Hermitian $A^\dagger = A$

Unitary $A^\dagger A = AA^\dagger = \mathbb{1} \Leftrightarrow A^\dagger = A^{-1}$

$$\langle Uu|Uv\rangle = \langle u|U^\dagger U|v\rangle = \langle u|v\rangle$$

In particular, any unitary operator maps an ONB to an ONB.

$$\begin{pmatrix} | & & | \\ A^{(1)} & \cdots & A^{(d)} \\ | & & | \end{pmatrix} |j\rangle = \begin{pmatrix} | \\ A^{(j)} \\ | \end{pmatrix}$$

Spectrum of a linear operator

Similarity transformation $A \mapsto B^{-1}AB$ (Conjugation)

Eigenvalue

$\lambda \in \mathbb{C}$

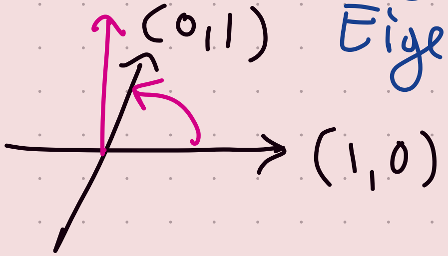
$A|u\rangle = \lambda|u\rangle$

Eigenvector $|u\rangle \neq 0$

The set of all eigenvalues of A is called the spectrum, which is invariant under any similarity transformation.

When eigenvectors of A span V, A can be put into a diagonal form
$$B^{-1}AB = \begin{pmatrix} \lambda_1 & & & 0 \\ & \lambda_2 & & \\ & & \ddots & \\ 0 & & & \lambda_d \end{pmatrix}$$

Not all matrices are diagonalizable!

Over $\mathbb{R}$	Over $\mathbb{C}$
$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ $\theta = \pi/2$ $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$  Eigenvalue $\pm i$ Eigenvector $\begin{pmatrix} 1 \\ \mp i \end{pmatrix}$	$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ Eigenvalue 0 Eigenvector $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ If diagonalizable $\Rightarrow \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, but A is not zero $\Rightarrow$ Contradiction

A is normal if $[A, A^\dagger] = 0$

$\boxed{A \text{ is diagonalizable} \iff A \text{ is normal}}$

The $\Leftarrow$ is immediate given two well known facts about Hermitian operators.

Let A and B be Hermitian operators.

1. The spectral theorem
   - 1.1 All eigenvalues of A are reals
   - 1.2 Eigenvectors of A form an ONB.

See next page for the degenerate case

$$\boxed{A = \sum_j \lambda_j |a_j\rangle\langle a_j|,}$$

2. If $[A, B] = 0$, then we can choose an ONB in which A and B are simultaneously diagonalized.

- $$A = \underbrace{\frac{A + A^\dagger}{2}}_{\text{Hermitian}} + i\underbrace{\left(\frac{A - A^\dagger}{2i}\right)}_{\text{Hermitian}} = B + iC$$

Can show that

$$[A, A^\dagger] = -2i\,[B, C]$$

So $[A, A^\dagger] = 0 \iff [B, C] = 0$

1 + 2 $\Rightarrow$ $[B, C] = 0$ implies that B and C can be simultaneously diagonalized, hence A can be diagonalized. $\square$

A normal, $\{|a_j^{(k)}\rangle\}_k$ an orthonormal set that spans an eigenspace with possibly degenerate eigenvalue λ_j

$$A = \sum_{jk} \lambda_j |a_j^{(k)}\rangle\langle a_j^{(k)}| = \sum_j \lambda_j P_j \quad \text{where } P_j = \sum_k |a_j^{(k)}\rangle\langle a_j^{(k)}|$$

are orthogonal projection operators

Mutually exclusive events $\longleftarrow$ $P_j^\dagger = P_j, \quad P_j P_k = \delta_{jk} P_j$

$P^\dagger = P, \quad P^2 = P$ characterizes a projection operator

Counterexample if this condition is omitted:

$$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$$

$\Downarrow$

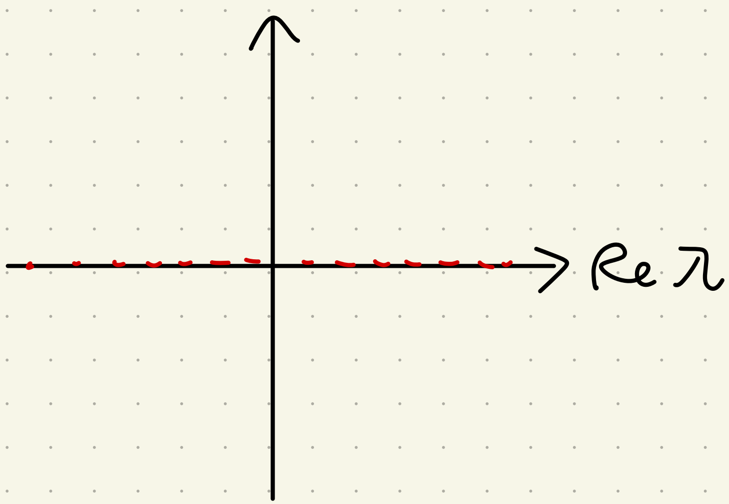
Eigenvalue 0 or 1. $\quad \mathrm{tr}\, P = \mathrm{rank}\, P$

Can always define an orthogonal projector $P^\perp = \mathbb{1} - P$ which can be easily shown to also be a projector

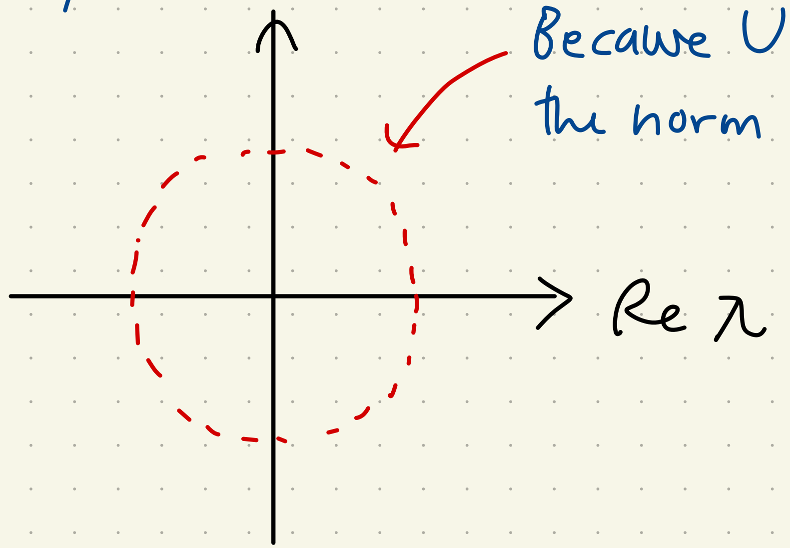
Split V into $+1$ eigenspaces of orthogonal projectors

$$V = \bigoplus_j V_j$$

Hermitian



Unitary



$\lambda_j = e^{i\theta_j}$

Because U preserves the norm

Symmetric functions of eigenvalues are also basis-invariant.

	General definition	A is normal	Properties
det A	$\sum_{\sigma \in S_d} \left(\operatorname{sgn} \sigma \prod A_{j\sigma(j)} \right)$	$\prod_j \lambda_j$	$\det(AB) = \det A \det B$
tr A	① In ONB, $\operatorname{tr} A = \sum_j A_{jj}$ ② $\operatorname{tr}(\lvert u\rangle\langle v\rvert) = \langle v \vert u\rangle$	$\sum_j \lambda_j$	$\operatorname{tr}(aA + bB) = a \operatorname{tr} A + b \operatorname{tr} B$ $\operatorname{tr}(AB) = \operatorname{tr}(BA)$
rank A	# of linearly independent columns/rows	# of nonzero λ_j	

Axioms of QM I

(Not complete, but good enough for now)

① A complete description of a physical system is given by its quantum state, a normalized vector $|\psi\rangle$ in a complex inner product space $\mathcal{H}$ ("Hilbert space")

② An observable quantity is associated to a Hermitian operator $A^\dagger = A$.

③ A measurement of an observable $A = \sum_j \lambda_j P_j$ gives an outcome λ_j with probability $\| P_j |\psi\rangle \|^2 = \langle \psi | P_j | \psi \rangle$ and a post-measurement state

$$P_j |\psi\rangle / \| P_j |\psi\rangle \| = P_j |\psi\rangle / \sqrt{\langle \psi | P_j | \psi \rangle} .$$

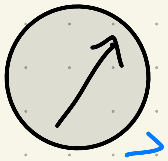
④ The quantum state evolves in time via a unitary operator

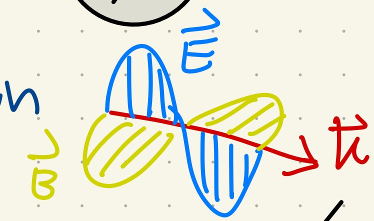
$$|\psi(t)\rangle = U(t, t_0) |\psi(t_0)\rangle$$

Qubit

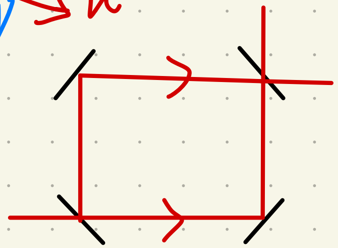
A qubit is any quantum system described by a two-dimensional vector space, an ONB for which corresponds to two possible measurement outcomes.

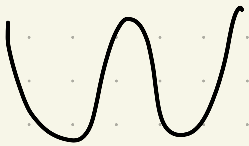
Examples

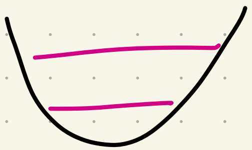
① Spin-1/2  $\{|\uparrow\rangle, |\downarrow\rangle\}$ Spin up or spin down (along $\hat{z}$)

② Polarization of light 

$\{|H\rangle, |V\rangle\}$ Horizontal or vertical

③ Mach-Zehnder interferometer  $\{|U\rangle, |L\rangle\}$ Photon travels in the upper arm or the lower arm

④ Double well  $\{|L\rangle, |R\rangle\}$ Particle is in left or right well

⑤ Nonlinear oscillator (Josephson junction)  $\{|g\rangle, |e\rangle\}$ Ground or first excited state

(To address only the transition between these two levels, need the ΔE between other pairs of states to be different.)

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \langle\psi|\psi\rangle = |\alpha|^2 + |\beta|^2 = 1$$

$\theta \in [0,\pi]$ $\qquad \varphi \in [0, 2\pi)$

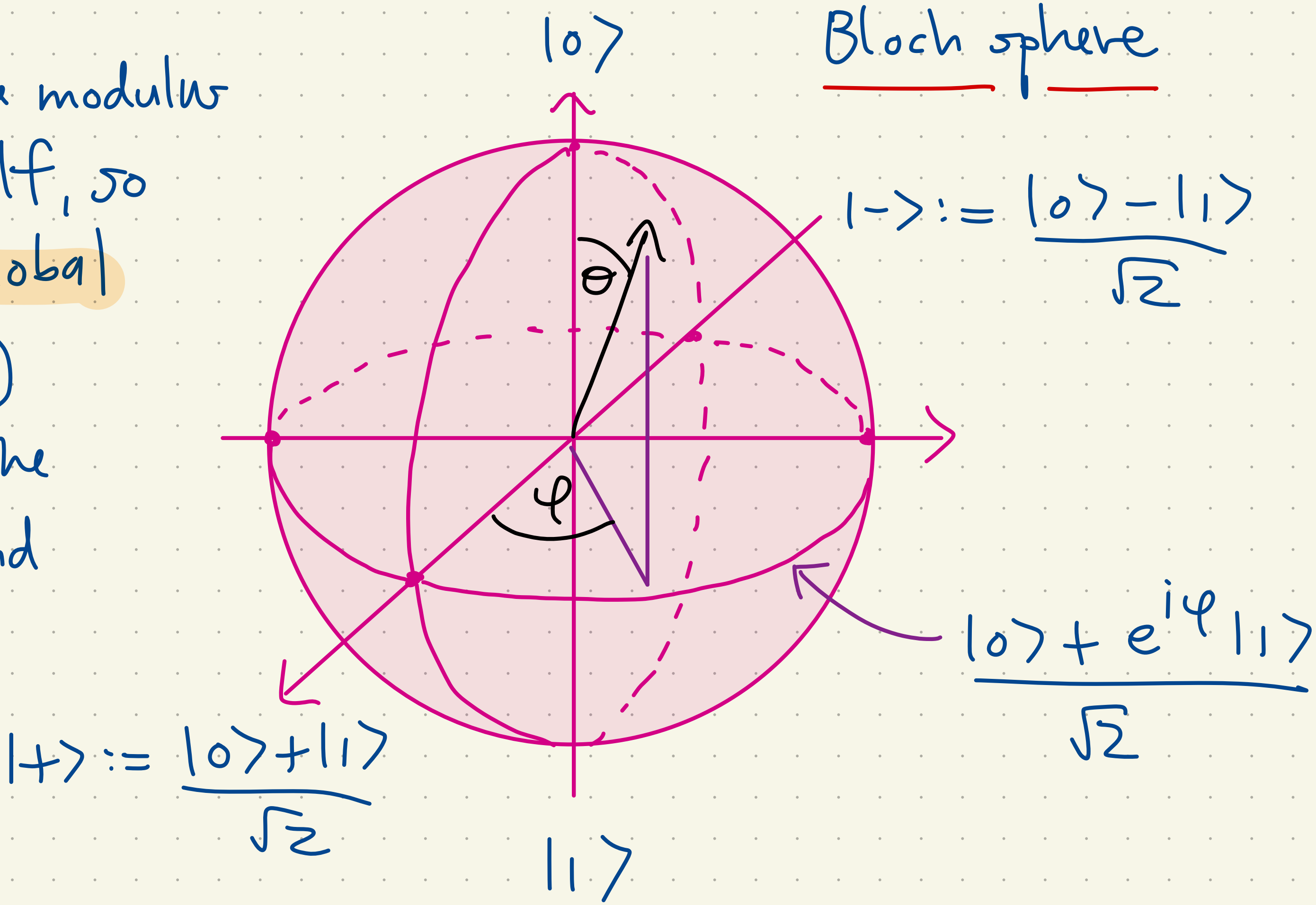
$$a e^{i\gamma}|0\rangle + b e^{i\delta}|1\rangle = e^{i\gamma}\left[\cos\left(\tfrac{\theta}{2}\right)|0\rangle + \sin\left(\tfrac{\theta}{2}\right) e^{i\overbrace{(\delta-\gamma)}^{\varphi}}|1\rangle\right]$$

Can choose to be cosine and sine

$$\boxed{|\psi\rangle = \cos\left(\tfrac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\tfrac{\theta}{2}\right)|1\rangle}$$

Any prediction depends on the modulus square $|\alpha_j|^2$ and not α_j itself, so states that differ only by a global phase (e.g. $|\psi\rangle$ vs $e^{i\delta}|\psi\rangle$) give the same predictions; the global phase is unphysical and only a redundancy in our own theory.

Bloch sphere



$$|\hat{n}\rangle = \cos(\theta/2)|0\rangle + e^{i\varphi}\sin(\theta/2)|1\rangle$$

$$|-\hat{n}\rangle = e^{-i\varphi}\sin(\theta/2)|0\rangle - \cos(\theta/2)|1\rangle$$

$$\hat{n} = \begin{pmatrix} \sin\theta\cos\varphi \\ \sin\theta\sin\varphi \\ \cos\theta \end{pmatrix} = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

Get rid of a global phase by going to projectors.

$$P_{\hat{n}} = |\hat{n}\rangle\langle\hat{n}| = \begin{pmatrix} \cos^2(\theta/2) & e^{-i\varphi}\sin(\theta/2)\cos(\theta/2) \\ \underbrace{e^{i\varphi}\sin(\theta/2)\cos(\theta/2)}_{\frac{1}{2}(\cos\varphi + i\sin\varphi)\sin\theta = \frac{x+iy}{2}} & \sin^2(\theta/2) \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1+z & x-iy \\ x+iy & 1-z \end{pmatrix}$$

$$= \boxed{\frac{\mathbb{1} + \hat{n}\cdot\vec{\sigma}}{2}}$$

Hermitian, trace-one

where $\vec{\sigma} = \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}$

$$\mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \underbrace{\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}}_{\text{traceless}}$$

Basis of the space of qubit Hermitian operators.

$$\sigma_j \sigma_k = \delta_{jk} \mathbb{1} + \sum_\ell i\epsilon_{jk\ell} \sigma_\ell \Rightarrow \begin{cases} \sigma_j \sigma_k - \sigma_k \sigma_j =: [\sigma_j, \sigma_k] = 2i \sum_\ell \epsilon_{jk\ell} \sigma_\ell \\ \sigma_j \sigma_k + \sigma_k \sigma_j =: \{\sigma_j, \sigma_k\} = 2\delta_{jk} \mathbb{1} \end{cases}$$

$$\sigma_j^\dagger = \sigma_j \qquad \sigma_j^2 = \mathbb{1}$$

$\{\mathbb{1}, \sigma_x, \sigma_y, \sigma_z\}$ forms an orthogonal basis for a real vector space of 2×2 Hermitian operators w.r.t. the Hilbert-Schmidt inner product

$$(A, B) = \mathrm{tr}(A^\dagger B)$$

Write $\mathbb{1} = \sigma_0$ and let a greek index runs from $\alpha = 0, 1, 2, 3$

$$\mathrm{tr}(\sigma_\alpha^\dagger \sigma_\beta) = 2\delta_{\alpha\beta} \Longleftrightarrow A = \sum_\alpha A_\alpha \sigma_\alpha \Rightarrow A_\alpha = \frac{1}{2}\mathrm{tr}(\sigma_\alpha A)$$

Observable $\hat{n}\cdot\vec{\sigma} = \frac{1 + \hat{n}\cdot\vec{\sigma}}{2} - \frac{1 - \hat{n}\cdot\vec{\sigma}}{2} = |\hat{n}\rangle\langle\hat{n}| - |-\hat{n}\rangle\langle -\hat{n}|$

$$\Updownarrow$$

$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ in the ONB $\{|\pm\hat{n}\rangle\}$

Lemma The unitary time evolution generated by a time-independent Hamiltonian H is $U = e^{-iHt/\hbar}$

- $i\hbar \frac{d}{dt}|\psi(t)\rangle = H|\psi(t)\rangle$

$$i\hbar \frac{d}{dt}U(t) = HU(t)$$

$$\text{"}\int \frac{dU(t')}{U(t')} = \frac{H}{i\hbar}\int_0^t dt'\text{"}$$

The DE has the intuitive solution

$$U(t,t_0) = e^{-iHt/\hbar} \qquad \square$$

The matrix exponential can be defined via the power series

$$U(t) = \mathbb{1} - \frac{it}{\hbar}H + \left(-\frac{it}{\hbar}H\right)^2 + \cdots$$

For a qubit Hamiltonian, we can show that

$$U(t) = \cos(\theta/2)\mathbb{1} - i\sin(\theta/2)\,\hat{n}\cdot\vec{\sigma}$$

Slicker derivation given θ is real

$$e^{-i\theta\hat{n}\cdot\vec{\sigma}} = e^{-i\theta}|\hat{n}\rangle\langle\hat{n}| + e^{+i\theta}|-\hat{n}\rangle\langle-\hat{n}|$$

$$= \left(\frac{e^{i\theta}+e^{-i\theta}}{2}\right)\mathbb{1} + \left(\frac{e^{-i\theta}-e^{+i\theta}}{2}\right)\hat{n}\cdot\vec{\sigma}$$

$$= \cos\theta\,\mathbb{1} - i\sin\theta\,\hat{n}\cdot\vec{\sigma}$$

Example Spin in a magnetic field

$$H = \underbrace{\vec{\mu}}_{\text{Magnetic moment}}\cdot\vec{B} = -\underbrace{\gamma}_{\text{Gyromagnetic ratio}}\hbar\,\vec{\sigma}\cdot\vec{B}/2 \Rightarrow e^{-iHt/\hbar} = e^{i\gamma\vec{B}\cdot\vec{\sigma}/2} \overset{\omega=\gamma|\vec{B}|}{=\!=} \cos\left(\frac{\omega t}{2}\right)\mathbb{1} + i\sin\left(\frac{\omega t}{2}\right)\hat{n}\cdot\vec{\sigma}$$

Mach-Zehnder interferometer

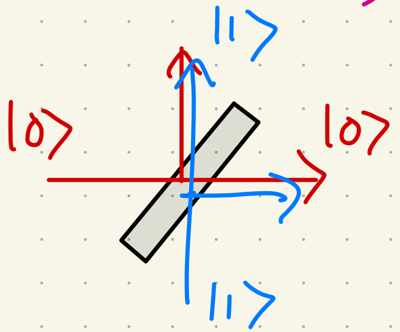
A testing ground for interference phenomena. Isomorphic to a qubit if there is only one photon.

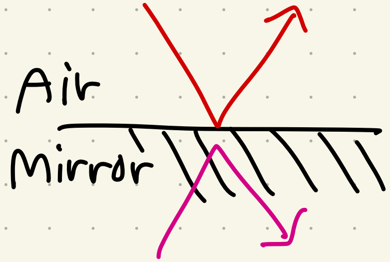
(Beam splitter) $B = \begin{pmatrix} t & r \\ r & t \end{pmatrix}$

t = transmission coefficient

r = reflection — " —

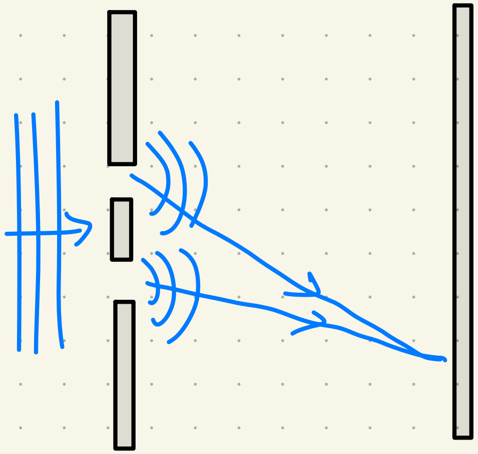
$|t|^2 + |r|^2 = 1$



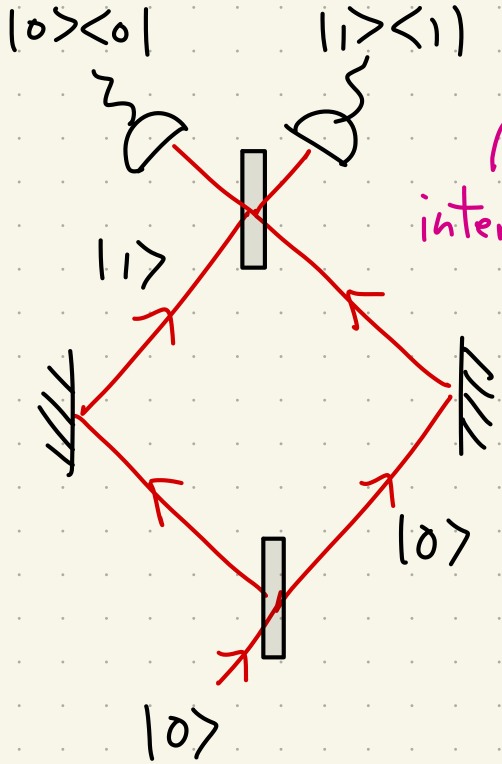


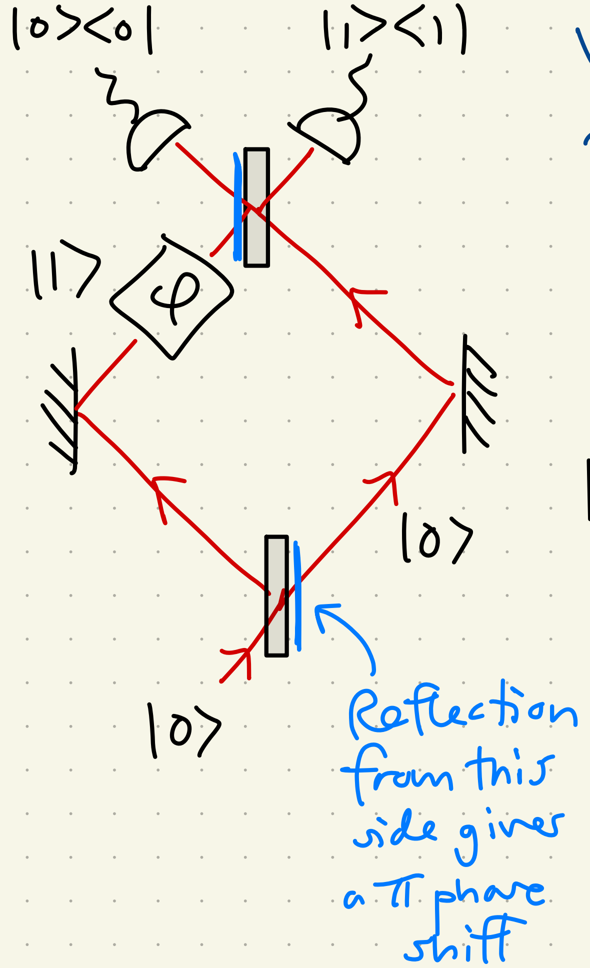
From classical EM, reflection on the side of lower index of refraction induces a π phase shift.

(Balanced (50/50) Beamsplitter) $B = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$



Constructive/destructive interference in the double-slit experiment is determined by the difference in the path lengths of the two waves $\Longrightarrow$





We usually set up the two arms of the interferometer to have the same path length, but simulate the path-length difference with a phase-shifter $\boxed{\varphi} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}$ in one arm.

$$|0\rangle - \boxed{B} - \boxed{M_0} - \boxed{M_1} - \boxed{\varphi} - \boxed{B} - \boxed{\text{measure}} \quad \begin{cases} Pr(0) = \cos^2(\varphi/2) \\ Pr(1) = \sin^2(\varphi/2) \end{cases}$$

$\frac{|0\rangle + |1\rangle}{\sqrt{2}}$ $\qquad -\left(\frac{|0\rangle + e^{i\varphi}|1\rangle}{\sqrt{2}}\right)$ $\qquad -e^{i\varphi/2}\left(\cos(\varphi/2)|0\rangle - i\sin(\varphi/2)|1\rangle\right)$

$\varphi = 0 \implies$ Always detect "0"

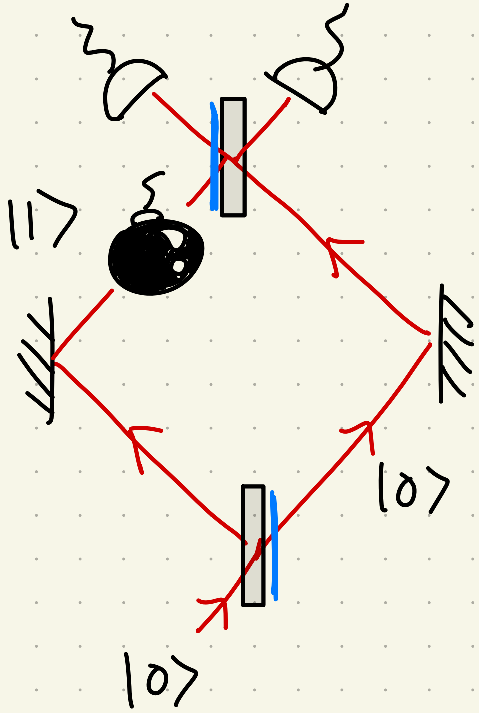
$\varphi = \pi \implies$ Never detect "0"

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix} = e^{i\varphi/2}\begin{pmatrix} e^{-i\varphi/2} & 0 \\ 0 & e^{i\varphi/2} \end{pmatrix} = e^{i\varphi/2} e^{-i\varphi Z/2}$$

Slicker calculation

Therefore, $H\hat{\varphi}H \propto e^{-i\varphi HZH/2} = e^{-i\varphi X/2} = \begin{pmatrix} \cos(\varphi/2) & -i\sin(\varphi/2) \\ -i\sin(\varphi/2) & \cos(\varphi/2) \end{pmatrix}$

Elitzur-Vaidman bomb detector



Working → Photon 

A dud → The photon simply passes through → Interference

Pr	Dud	Working
"0"	1	1/4
"1"	0	1/4
Explosion	0	1/2

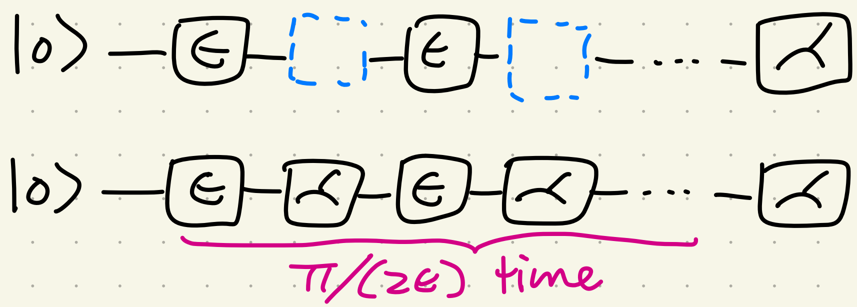
Detect a working bomb without interacting with the bomb!

However, we can do better by sending only a little portion of the quantum state into the arm with the bomb (so not a balanced beamsplitter anymore) and concatenate the interferometer to amplify the probability of measuring "1".

$$\hat{\epsilon} = R_y(\epsilon) = \begin{pmatrix} \cos\epsilon & -\sin\epsilon \\ \sin\epsilon & \cos\epsilon \end{pmatrix}$$

Dud

Working



	Dud	Working
"0"	0	≈ 1
"1"	1	
☆	0	$\lesssim \pi\epsilon/2$