$FT(|\text{subgroup } H\rangle) = |H^{\perp}\rangle$

More linear algebra review

Linear transformations $\longleftrightarrow$ matrices (in a basis)

M

- Hermitian if $M = M^{+}$
- normal if $MM^{+} = M^{+}M$
- unitary if $MM^{+} = I$
- projection/projector if $M^2 = M$
- positive semi-definite if $\langle v|M|v\rangle \geq 0 \;\forall |v\rangle$

Thm: M is diagonalizable iff M is normal.

i.e. $\exists$ an o.n. basis $\{|i\rangle\}$ with $M|i\rangle = \lambda_i|i\rangle$

Hermitian $\Rightarrow$ real eigenvalues $M^{+}|i\rangle = \bar{\lambda}_i|i\rangle = M|i\rangle = \lambda_i|i\rangle$ ✓

unitary $\Rightarrow$ unit eigenvalues $\langle i|U^{+}U|i\rangle = |\lambda_i|^2 \cdot \langle i|i\rangle$
$= \langle i|i\rangle$

$M \geq 0 \Rightarrow$ Hermitian, nonnegative eigenvalues

Thm: Singular value decomposition (SVD)

For any M, M can be written as UDV^{+}, where U and V are unitary and D is diagonal (nonnegative).

i.e. $\exists$ o.n. bases $\{|v_i\rangle\}, \{|w_i\rangle\}$ s.t.

$$M = \sum_i \lambda_i |v_i\rangle\langle w_i| \quad , \lambda_i \geq 0$$

Commutator & anticommutator $\qquad [A,B] = 0 \Leftrightarrow$ simult. diagonalizable

Trace $\quad \operatorname{Tr} M = \sum_i M_{ii}$

- linear $\operatorname{Tr}(A+B) = \operatorname{Tr}A + \operatorname{Tr}B$
- cyclic $\operatorname{Tr}(ABC) = \operatorname{Tr}(CAB) = \operatorname{Tr}(BCA)$
- $\operatorname{Tr}(A|v\rangle\langle v|) = \langle v|A|v\rangle \quad \Rightarrow \operatorname{Tr}|v\rangle\langle v| = \langle v|v\rangle = \||v\rangle\|^2$

Lie-Trotter formula $e^{A+B} = \left(e^{A/n}e^{B/n}\right)^n + O\left(\frac{\|[A,B]\|}{n}\right)$ (first order)

Claim: The ensembles

$$\left\{\begin{matrix}|0\rangle \text{ with prob. } 1/2 \\ |1\rangle \text{ with prob. } 1/2\end{matrix}\right\} \quad \text{and} \quad \left\{\begin{matrix}|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \text{ w/ prob. } 1/2 \\ |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \text{ w/ prob. } 1/2\end{matrix}\right\}$$

are indistinguishable in every way. They are equivalent states, i.e., the same.

"Proof" 1: Let Π_1, Π_2 be two orthogonal one-qubit projections.

$\mathbb{P}$[measure Π_1 in ensemble 1]

$$= \tfrac{1}{2}\cdot \mathbb{P}[\text{measure } \Pi_1 \text{ from } |0\rangle] + \tfrac{1}{2}\mathbb{P}[\text{measure } \Pi_1 \text{ from } |1\rangle]$$
$$= \tfrac{1}{2}\|\Pi_1|0\rangle\|^2 + \tfrac{1}{2}\|\Pi_1|1\rangle\|^2$$
$$= \tfrac{1}{2}\left(\langle 0|\Pi_1|0\rangle + \langle 1|\Pi_1|1\rangle\right)$$
$$= \mathrm{Tr}\left[\Pi_1 \cdot \tfrac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)\right]$$
$$= \tfrac{1}{2}\mathrm{Tr}\,\Pi_1 = \tfrac{1}{2}.$$

$\mathbb{P}$[measure Π_1 in ensemble 2]

$$= \tfrac{1}{2}\|\Pi_1|+\rangle\|^2 + \tfrac{1}{2}\|\Pi_1|-\rangle\|^2$$
$$= \mathrm{Tr}\Big[\Pi_1\, \tfrac{1}{2}\big(\underbrace{|+\rangle\langle +|}_{\frac{1}{2}\begin{pmatrix}1&1\\1&1\end{pmatrix}} + \underbrace{|-\rangle\langle -|}_{\frac{1}{2}\begin{pmatrix}1&-1\\-1&1\end{pmatrix}}\big)\Big] = \tfrac{1}{2} \quad \checkmark \qquad \square$$

Proof 2: Purifications of the two ensembles are

$$\tfrac{1}{\sqrt{2}}(|0\rangle\otimes|0\rangle + |1\rangle\otimes|1\rangle), \text{ and } \tfrac{1}{\sqrt{2}}(|+\rangle\otimes|+\rangle + |-\rangle\otimes|-\rangle)$$

These are the <u>same</u> states. $\square$

(Shorter proof, but required a guess. <u>Density matrices</u> are a systematic formalism that always works.)

<u>Density matrices</u>

<u>Def</u>: The density matrix of a pure state $|\psi\rangle$ is $\rho = |\psi\rangle\langle\psi|$.

Example:

$$\alpha|0\rangle + \beta|1\rangle \longrightarrow \begin{pmatrix}\alpha\\ \beta\end{pmatrix}(\bar\alpha \;\; \bar\beta) = \begin{pmatrix}|\alpha|^2 & \alpha\bar\beta \\ \bar\alpha\beta & |\beta|^2\end{pmatrix}$$

$$\alpha|00\rangle + \beta|11\rangle \longrightarrow \begin{pmatrix}|\alpha|^2 & 0 & 0 & \alpha\bar\beta \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \bar\alpha\beta & 0 & 0 & |\beta|^2\end{pmatrix}$$

<u>Def</u>: The density matrix for a mixed state $\{|\psi_i\rangle$ with prob. $p_i\}$ is

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

Operations on density matrices:

1. Unitaries $\quad \mathcal{U} : |\psi\rangle \mapsto \mathcal{U}|\psi\rangle.$

$$\rho \mapsto \mathcal{U}\rho\,\mathcal{U}^\dagger$$

since
$$\sum_i p_i\, \mathcal{U}|\psi_i\rangle (\mathcal{U}|\psi_i\rangle)^\dagger$$
$$= \sum_i p_i\, \mathcal{U}|\psi_i\rangle\langle\psi_i|\mathcal{U}^\dagger$$
$$= \mathcal{U}\rho\,\mathcal{U}^\dagger$$

2. Measurements

Theorem: Consider a mixture $p_j \; |\psi_j\rangle \longrightarrow \rho$

Measuring in the basis $|\beta_1\rangle, \cdots, |\beta_N\rangle$, ie. $\Pi_i = |\beta_i\rangle\langle\beta_i|$,
outcome $|\beta_i\rangle$ is observed with probability
$$\langle\beta_i|\rho|\beta_i\rangle = \mathrm{Tr}(\rho\,\Pi_i).$$

Proof.
$$\mathbb{P}[i] = \sum_j p_j\, |\langle\psi_j|\beta_i\rangle|^2 = \sum_j p_j \langle\beta_i|\psi_j\rangle\langle\psi_j|\beta_i\rangle$$
$$= \langle\beta_i|\Big(\sum_j p_j |\psi_j\rangle\langle\psi_j|\Big)|\beta_i\rangle = \langle\beta_i|\rho|\beta_i\rangle. \quad \square$$

Corollary: Measuring ρ in the standard basis,
$$\mathbb{P}[\text{outcome } i] = \rho_{ii}.$$

~~Adult~~ properties ~~examples~~ partial Tr

Mixtures with the same density matrix are indistinguishable.

Examples: While any pure state $|\psi\rangle$ has a unique ensemble description ($|\psi\rangle$ with probability 1), any impure mixed state has an infinite number of equivalent ensemble representations.

$$\begin{pmatrix} \tfrac12 : & |0\rangle \\ \tfrac12 : & |1\rangle \end{pmatrix} \qquad \begin{pmatrix} \tfrac12 : & |+\rangle \\ \tfrac12 : & |-\rangle \end{pmatrix} \qquad \begin{pmatrix} \tfrac13 : & |0\rangle \\ \tfrac13 : & \tfrac12|0\rangle + \tfrac{\sqrt3}{2}|1\rangle \\ \tfrac13 : & \tfrac12|0\rangle - \tfrac{\sqrt3}{2}|1\rangle \end{pmatrix}$$

$$\rho = \begin{pmatrix} \tfrac12 & 0 \\ 0 & \tfrac12 \end{pmatrix}$$

Claim. ρ is impure $\iff \mathrm{Tr}(\rho^2) < 1.$
$$\mathrm{Tr}(\rho^2) = \sum_i \lambda_i^2$$

Properties of density matrices:

1. $\mathrm{Tr}\,\rho = 1$ (follows from the corollary, or...)
2. ρ is Hermitian $\rho = \rho^\dagger$
3. ρ is positive semidefinite, ie. has nonnegative eigenvalues

A matrix satisfying these properties can be diagonalized $\rho = \sum_i \lambda_i |e_i\rangle\langle e_i|$, thus corresponds to an ensemble. $\Rightarrow$ These properties characterize quantum states.

Example: Bloch sphere of one-qubit states

- full characterization of 1-qubit density matrices

<u>Claim</u>: Let $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ the Pauli matrices.

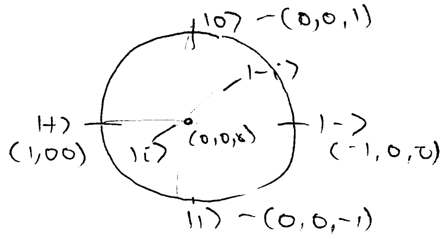
Any 2×2 matrix σ can be expanded

$$\sigma = sI + xX + yY + zZ$$

for $s, x, y, z \in \mathbb{C}$, or $\in \mathbb{R}$ if σ is Hermitian.

Then σ is a density matrix $\iff s = \frac{1}{2},\ x^2+y^2+z^2 \le \frac{1}{4}$.

Proof: Trivial. $\square$



$$\mathrm{Tr}(\sigma^2) = 2(s^2 + x^2+y^2+z^2)$$
$$= 1 \iff x^2+y^2+z^2 = \frac{1}{4}$$

$\Rightarrow$ pure states on the surface

Opposite pure states are orthogonal.

Unitaries $\iff$ Rotations
(up to a phase)

$$SU(2)/\pm 1 \cong SO(3)$$

$$\exp\left(i\frac{\theta}{2}(xX+yY+zZ)\right) \leftrightarrow \theta \text{ about } (x,y,z)$$

Removing + adding subsystems: The partial trace and purifications

<u>Def</u>: Partial trace

For a matrix $M \in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$

$$M = \begin{array}{cc} & jl \\ ik & \begin{pmatrix} & & \\ & m_{ik,jl} & \\ & & \end{pmatrix} \end{array} \quad \begin{array}{l} i,j = 1 \ldots \dim \mathcal{H}_A \\ k,l = 1 \ldots \dim \mathcal{H}_B \end{array}$$

$$= \sum_{ijkl} m_{ik,jl} \, |i\rangle\langle j| \otimes |k\rangle\langle l|$$

$$\mathrm{Tr}_B(M) \doteq \sum_{ij} \Big(\sum_k m_{ik,jk} \Big) |i\rangle\langle j| \quad \in \mathcal{L}(\mathcal{H}_A)$$

$$\mathrm{Tr}_A(M) \doteq \sum_{kl} \Big(\sum_i m_{ik,il} \Big) |k\rangle\langle l| \in \mathcal{L}(\mathcal{H}_B)$$

Examples: ① $M = \begin{pmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & o & p \end{pmatrix} \in \mathcal{L}(\mathbb{C}^2 \otimes \mathbb{C}^2)$

$$\mathrm{Tr}_B(M) = \begin{pmatrix} a+f & c+h \\ i+n & k+p \end{pmatrix} \qquad \mathrm{Tr}_A M = \begin{pmatrix} a+k & b+l \\ e+o & f+p \end{pmatrix}$$

② $M \otimes N \xrightarrow{\mathrm{Tr}_A} N \cdot \mathrm{Tr}(M)$

$M \otimes N \xrightarrow{\mathrm{Tr}_B} M \cdot \mathrm{Tr}(N)$

The state of a subsystem A of a state ρ_{AB} is $\rho_A = \mathrm{Tr}_B \, \rho_{AB}$.

e.g. $\mathbb{P}[\text{Alice measures } 0]$

$$= \sum_{b=0}^{1} (\langle 0|\langle b|) \rho (|0\rangle|b\rangle)$$
$$= \mathrm{Tr}\big[(|0\rangle\langle 0| \otimes \mathbb{1}) \rho\big]$$
$$= \langle 0| \rho_A |0\rangle$$

Note: Indeed $\rho_A^\dagger = \rho_A$, $\mathrm{Tr}\,\rho_A = \mathrm{Tr}\,\rho = 1$, and $\rho_A \geq 0$

$\big(\langle\psi|\rho_A|\psi\rangle = \sum_j \langle\psi|\langle j| \rho |\psi\rangle|j\rangle \geq 0\big)$

<u>Purification</u>: $\rho = \sum_i p_i |i\rangle\langle i| \underset{\text{partial trace}}{\overset{\text{purify}}{\rightleftarrows}} |\psi\rangle = \sum_i \sqrt{p_i} \, |i\rangle \otimes |i\rangle$

not unique!

Quantum bit commitment

Alice $\qquad\qquad$ Bob

$b \longrightarrow$

⋮

later

$\xrightarrow{\text{key}}$

① Bob gets no information

② Alice can't change her mind

Example: Coin-flipping over the telephone

BB'84

Observe: The ensembles $\overset{\text{I}}{\left\{\begin{array}{ll}\frac{1}{2} & |0\rangle \\ \frac{1}{2} & |1\rangle\end{array}\right\}}$ and $\overset{\text{II}}{\left\{\begin{array}{ll}\frac{1}{2} & |+\rangle \\ \frac{1}{2} & |-\rangle\end{array}\right\}}$

both have the same density matrix $\frac{1}{2}\begin{pmatrix}1&0\\0&1\end{pmatrix}$.

A $\qquad\qquad$ B

$b \in \{0,1\}$ $\quad$ commitment: k qubits drawn from I if $b=0$ or II if $b=1$

Bob measures each qubit in $|0\rangle/|1\rangle$ or $|+\rangle/|-\rangle$ basis at random.

revelation: Alice reveals her sequence

Property 1: ✓ $\rho_{\text{I}} = \rho_{\text{II}}$

Property 2: If Alice picks 0/1 and wants to change to +/−, she must predict Bob's measurements for all positions where Bob chose +/− $\quad \mathbb{P}[\text{success}] \simeq \frac{1}{2^{k/2}}$..

Alice's cheating strategy:

Send half of each of k Bell pairs to Bob

$$\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) = \frac{1}{\sqrt{2}}\left(|++\rangle + |--\rangle\right)$$

i.e. a purification of the protocol.

To commit to $b=0$ measure in the 0/1 basis

" $\quad b=1$ " $\quad$ +/− "

Bob sees the same density matrix in either case