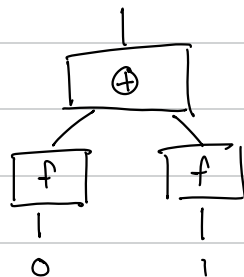


Classical algorithmic for  $f(0) \stackrel{?}{=} f(1)$  :



What does quantum access to  $f$  mean?

Attempt 1: apply transform  $\begin{pmatrix} f(0) & 0 \\ 0 & f(1) \end{pmatrix} |x\rangle \mapsto |f(x)\rangle$

Why does this not work? Ans: not necessarily unitary

Attempt 2: what about  $\begin{pmatrix} (-1)^{f(0)} & 0 \\ 0 & (-1)^{f(1)} \end{pmatrix} (= : V_f)$

$|x\rangle \mapsto (-1)^{f(x)} |x\rangle$  Unitary ✓

Issue: Is this actually physically realistic?

Attempt 3: Reversible version of  $f$ :

$U_f: (x, y) \mapsto (x, y \oplus f(x)).$

This is its own self-inverse. So a unitary transform.

$$\begin{aligned} \sum_{x,y \in \{0,1\}} \alpha_{xy} |x,y\rangle &= \sum_{x,y} \alpha_{xy} |x, y \oplus f(x)\rangle \\ &= \sum_{x,y} \alpha_{x, y \oplus f(x)} |x,y\rangle \end{aligned}$$

Ex.  $f(0)=1, f(1)=0$   $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = U_f$

Claim Def 3  $\Rightarrow$  Def 2.

Pf by direct calculation + introduction to q. circuit notation

$$\begin{aligned} (-1)^{f(x)} |x\rangle &= \text{Circuit} \\ |0\rangle & \end{aligned}$$

$\underbrace{\hspace{15em}}_{=: V_f}$

$$|x\rangle|0\rangle \mapsto |x\rangle|-\rangle \mapsto |x\rangle \left( \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

$$\xrightarrow{U_f} \frac{|x\rangle|f(x)\rangle - |x\rangle|1 \oplus f(x)\rangle}{\sqrt{2}}$$

$$= \begin{cases} |x\rangle \otimes |-\rangle & f(x) = 0 \\ |x\rangle \otimes -|-\rangle & f(x) = 1 \end{cases}$$

$$= (-1)^{f(x)} |x\rangle|-\rangle$$

$$\mapsto (-1)^{f(x)} |x\rangle|0\rangle.$$

$$\text{By linearity, } \sum \alpha_x |x\rangle|0\rangle \mapsto \sum \alpha_x \underbrace{(-1)^{f(x)}}_{\text{relative phase}} |x\rangle|0\rangle$$

relative phase  
as opposed to global phase

With an "ancilla"  $|0\rangle$ , we implemented Def 2 from Def 3.

$U_f$  is sometimes called the phase kick-back query/oracle.

Alg using  $V_f$  for  $f(0) \stackrel{?}{=} f(1)$ .

$$-\boxed{X} - \boxed{H} - \boxed{V_f} - \boxed{H} - |0\rangle$$

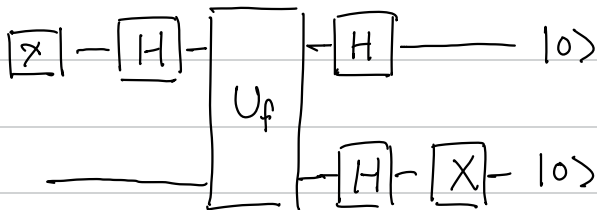
PP.  $|0\rangle \mapsto |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$

$$\xrightarrow{V_f} \frac{(-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle}{\sqrt{2}}$$

$$= (-1)^{f(0)} \left( \frac{|0\rangle + (-1)^{f(0) \oplus f(1)} |1\rangle}{\sqrt{2}} \right)$$

$$\xrightarrow{H} |f(0) \oplus f(1)\rangle \leftarrow \text{classical state.}$$

Full alg:



# Exploiting entanglement

Multiqubit systems.  $n_1 + n_2$  qubits

$$(\mathbb{C}^2)^{\otimes (n_1 + n_2)} \cong \underbrace{(\mathbb{C}^2)^{\otimes n_1}}_{\text{Alice } \mathcal{H}_A} \otimes \underbrace{(\mathbb{C}^2)^{\otimes n_2}}_{\text{Bob } \mathcal{H}_B}$$

A state  $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$  is called product if

$$|\psi\rangle = \underbrace{|a\rangle}_{\mathcal{H}_A} \otimes \underbrace{|b\rangle}_{\mathcal{H}_B}$$

If not product, then the state is called entangled.

$$\text{EPR state: } \frac{|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle}{\sqrt{2}} \in \mathbb{C}^2 \otimes \mathbb{C}^2.$$

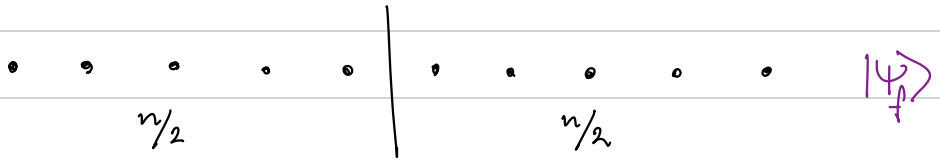
Claim  $|EPR\rangle$  is entangled.

$$\text{Pf. } |EPR\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \otimes \begin{pmatrix} \gamma \\ \delta \end{pmatrix} \Rightarrow$$

$$\alpha\gamma = \beta\delta = \frac{1}{\sqrt{2}} \Rightarrow \text{all 4 coefficients are non-zero.}$$

But  $0 = \langle 0_1 | \text{EPR} \rangle = \alpha\delta$ , a contradiction.  $\square$

Ex Entanglement is not a corner case.



From Pset 1, argue that the phase state  $|\psi_f\rangle$  is unentangled between the two halves iff

$$f(x, y) = g(x) \oplus h(y)$$

Then show that almost all of the phase states are entangled.

Entanglement is not a probability distribution.

Claim If Alice & Bob measure their halves of  $|\text{EPR}\rangle$  in the standard basis, they will always agree.

Pf. Wlog, Alice measures first (wlog, from pset).

Alice's outcome is  $|a\rangle$  w pr  $\|(\langle a| \otimes \mathbb{1})|EPR\rangle\|^2$

and Bob's state is  $\propto (\langle a| \otimes \mathbb{1})|EPR\rangle$

$$\begin{aligned}(\langle a| \otimes \mathbb{1})|EPR\rangle &= \langle a| \otimes \mathbb{1} \left( \frac{1}{\sqrt{2}} \sum_{a' \in \{0,1\}} |a'\rangle \otimes |a'\rangle \right) \\ &= \frac{1}{\sqrt{2}} |a\rangle.\end{aligned}$$

So, pr =  $\frac{1}{2}$  and Bob's state is also  $|a\rangle$ .

□

Claim If Alice measures in basis  $\{|v_0\rangle, |v_1\rangle\}$  then each outcome  $|v_i\rangle$  has probability  $\frac{1}{2}$  and the resulting state for Bob is  $|v_i^*\rangle$ .

Pf.  $|v_i\rangle = \alpha_i |0\rangle + \beta_i |1\rangle$ . Then,

$$\begin{aligned}\langle v_i| \otimes \mathbb{1} |EPR\rangle &= \left( \alpha_i^* \langle 0| \otimes \mathbb{1} + \beta_i^* \langle 1| \otimes \mathbb{1} \right) \left( \frac{|00\rangle + |11\rangle}{\sqrt{2}} \right) \\ &= \frac{\alpha_i^* |0\rangle + \beta_i^* |1\rangle}{\sqrt{2}}\end{aligned}$$

$$= \frac{|v_i^*\rangle}{\sqrt{2}}.$$

□

Why does this not imply faster-than-light communication?

Ans: Alice can choose a basis, but the statistics of any experiment Bob does on his qubits will not change. What is more powerful is the correlations that can be developed.

Entanglement  $\neq$  prob dist. Let  $\{|v_0\rangle, |v_1\rangle\} = \{|+\rangle, |-\rangle\}$ , and Alice & Bob have state  $|0\rangle|0\rangle$  and  $|1\rangle|1\rangle$  with equal prob.  $\frac{1}{2}$ .

If Alice measures  $|+\rangle$ , what is Bob's prob of measuring  $|+\rangle$ ?

Show in class that it equals  $\frac{1}{2}$ .

Superdense coding

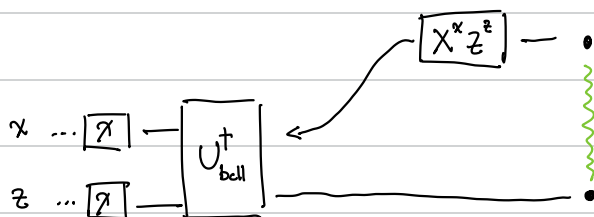
Alice & Bob prepare an  $|EPR\rangle$ . Alice then wants to send a 2-bit message  $(x, z) \in \{0, 1\}^2$ . Can she save on postage?

$$|\Phi_{xz}\rangle = (X^x Z^z \otimes \mathbb{I}) |\text{EPR}\rangle$$

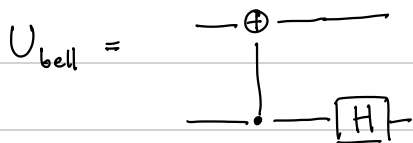
(write out all 4)

Claim "Bell" basis for  $\mathbb{C}^4$ .

Protocol



Since Bell basis,  $\exists$  unitary  $U_{\text{bell}} : |x\rangle|z\rangle \mapsto |\Phi_{xz}\rangle :$



where  $\text{CNOT}_{2 \rightarrow 1} = \text{"CNOT"}_{2 \rightarrow 1}$

$$\text{CNOT}_{2 \rightarrow 1} |x, y\rangle = |x \oplus y, y\rangle.$$

In class conversation about what's happening.

Reconciling entanglement and prob theory.

How do we describe prob dists over quantum states?

Note about generality and deal with  $|\psi\rangle \in \mathbb{C}^d$  as much as possible.

Ans: Density matrices

For  $|\psi\rangle \in \mathbb{C}^d$ , the corresponding d.m. is  $|\psi\rangle\langle\psi|$ .

Def. Let  $\{(p_a, |\psi_a\rangle)\}_a$  be an ensemble of pure states

meaning  $p_a$  is a prob. dist.  $p_a \geq 0$ ,  $\sum_a p_a = 1$ .

Then, the corresponding d.m. is  $\rho := \sum_a p_a |\psi_a\rangle\langle\psi_a|$ .

If d.m. is rank 1,  $\rho = |\psi\rangle\langle\psi|$  then called pure.

If not rank 1, then called mixed.

Central thesis: d.m. formalization is necessary and sufficient.

## Examples

$$|0\rangle \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad |1\rangle \mapsto \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$|+\rangle \mapsto \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \quad |-\rangle \mapsto \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$\text{coin-flip} = \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{|+\rangle\langle +| + |-\rangle\langle -|}{2}.$$

$$|EPR\rangle \mapsto \frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

$$\text{shared randomness} = \frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

## Thm (Total characterization)

① Let  $\rho$  correspond to  $\{(\rho_a, |\psi_a\rangle)\}$ .

Then  $\rho \geq 0$ ,  $\text{tr}(\rho) = 1$ .

② If  $\rho \geq 0$ ,  $\text{tr}(\rho) = 1 \Rightarrow \exists$  corresponding ensemble yielding  $\rho$ .

Def  $\rho$  is a d.m. iff  $\rho \geq 0$ ,  $\text{tr}(\rho) = 1$ .

Pf of ① Since each  $p_a \in \mathbb{R}$ ,  $|\psi_a\rangle\langle\psi_a|$  Hermitian  $\Rightarrow \rho$  is Hermitian.

For any vector  $|v\rangle$ ,

$$\langle v | \rho | v \rangle = \langle v | \left( \sum_a p_a |\psi_a\rangle\langle\psi_a| \right) | v \rangle$$

$$= \sum_a p_a \langle v | \psi_a \rangle \langle \psi_a | v \rangle$$

$$= \sum_a p_a |\langle v | \psi \rangle|^2 \geq 0.$$

$$\text{tr}(\rho) = \text{tr} \left( \sum_a p_a |\psi_a\rangle\langle\psi_a| \right)$$

$$= \sum_a p_a \text{tr}(|\psi_a\rangle\langle\psi_a|)$$

$$= \sum_a p_a \langle \psi_a | \psi_a \rangle = \sum_a p_a = 1.$$

Pf of ②

Spectral thm:  $\rho = \sum_a \lambda_a |v_a\rangle\langle v_a|$  eigendecomposition

$\rho \geq 0 \Rightarrow \lambda_a \geq 0$  and  $1 = \text{tr}(\rho) = \sum_a \lambda_a$   
so  $\lambda$  is a prob. dist.

So  $\{(\lambda_a, |v_a\rangle)\}$  is a well-defined ensemble.

Updating density matrices

Derived consequences

If a state is represented by  $\rho$  and unitary  $U$  is applied.

Then,  $\rho \mapsto U\rho U^\dagger$ .

Pf. Consider any ensemble  $\{(p_a, |\psi_a\rangle)\}$  corresponding to  $\rho$ .

New ensemble  $\{(p_a, U|\psi_a\rangle)\}$ . Corresponds to

$$\rho = \sum_a p_a U|\psi_a\rangle\langle\psi_a|U^\dagger = U\left(\sum_a p_a |\psi_a\rangle\langle\psi_a|\right)U^\dagger = U\rho U^\dagger. \quad \square$$

Measurements :

For bit  $b$ , define  $\Pi_b = |b\rangle\langle b| \otimes \mathbb{1}$ .

If first qubit measured, then

$$\Pr[b] = \text{tr}(\Pi_b \rho)$$

post-measurement state is  $\sigma = \frac{\Pi_b \rho \Pi_b}{\text{tr}(\Pi_b \rho)}$

and if no measurement is recorded, then state equals

$$\Pi_0 \rho \Pi_0 + \Pi_1 \rho \Pi_1.$$

Pf.  $\rho = \sum_a p_a |\psi_a\rangle\langle\psi_a|$  be any ensemble decomposition.

Observe  $\Pi_0 + \Pi_1 = \mathbb{1}$  and  $\Pi_0 \Pi_1 = 0$ , then

$$|\psi_a\rangle = \Pi_0 |\psi_a\rangle + \Pi_1 |\psi_a\rangle$$

$$\begin{aligned}
 \text{Then } \Pr[b|a] &= \|(\langle b| \otimes \mathbb{I})|\Psi_a\rangle\|^2 \\
 &= \|\Pi_b |\Psi_a\rangle\|^2 \\
 &= \langle \Psi_a | \Pi_b | \Psi_a \rangle
 \end{aligned}$$

$$\begin{aligned}
 \text{Then } \Pr[b] &= \sum_a p_a \Pr[b|a] \\
 &= \sum_a p_a \langle \Psi_a | \Pi_b | \Psi_a \rangle \\
 &= \sum_a p_a \operatorname{tr}(\Pi_b |\Psi_a\rangle\langle\Psi_a|) \\
 &= \operatorname{tr}\left(\Pi_b \sum_a p_a |\Psi_a\rangle\langle\Psi_a|\right) \\
 &= \operatorname{tr}(\Pi_b \rho).
 \end{aligned}$$

If  $b$  observed, so  $\Pr[b] > 0$ . Then for event  $a$ , post-state is

$$\frac{\Pi_b |\Psi_a\rangle}{\|\Pi_b |\Psi_a\rangle\|} = \frac{\Pi_b |\Psi_a\rangle}{\sqrt{\langle \Psi_a | \Pi_b | \Psi_a \rangle}}$$

$$\text{as a d.m. } \sigma_b^a := \frac{\Pi_b |\Psi_a\rangle\langle\Psi_a| \Pi_b}{\langle \Psi_a | \Pi_b | \Psi_a \rangle}$$

If  $b$  has occurred, then  $\Pr[a|b] = \frac{p_a \Pr[b|a]}{\Pr[b]}$ .

post-measurement d.m.

$$\sigma_b = \sum_a \Pr[a|b] \sigma_b^a$$

$$= \sum_a \frac{p_a \cancel{\langle \Psi_a | \Pi_b | \Psi_a \rangle}}{\Pr[b]} \cdot \frac{\Pi_b | \Psi_a \rangle \langle \Psi_a | \Pi_b}{\cancel{\langle \Psi_a | \Pi_b | \Psi_a \rangle}}$$

$$= \frac{\Pi_b \left( \sum_a p_a |\Psi_a\rangle\langle\Psi_a| \right) \Pi_b}{\text{tr}(\Pi_b \rho)}$$

$$= \frac{\Pi_b \rho \Pi_b}{\text{tr}(\Pi_b \rho)}.$$

Lastly, use that if measurement is not known then

$$\Pr[0] \sigma_0 + \Pr[1] \sigma_1 = \Pi_0 \rho \Pi_0 + \Pi_1 \rho \Pi_1.$$

## List evolution rules for density matrices

Exercise Show that  $\text{tr}(\rho^2) = 1$  iff  $\rho$  is pure.

Pf.  $\rho = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i|$  spectral decomposition. Then

$$\begin{aligned}\rho^2 &= \sum_{i,j} \lambda_i \lambda_j |\psi_i\rangle\langle\psi_i| \psi_j\rangle\langle\psi_j| \\ &= \sum_i \lambda_i^2 |\psi_i\rangle\langle\psi_i|\end{aligned}$$

$$\text{so } \text{tr}(\rho^2) = \sum_i \lambda_i^2 \leq \sum_i \lambda_i = 1.$$

equality iff each  $\lambda_i \in \{0, 1\}$ . But at most 1 eigenvalue of 1.

So,  $\text{tr}(\rho^2) = 1$  iff pure state.

Aside: For fn  $f: \mathbb{R} \rightarrow \mathbb{R}$ , we define

$$f(\rho) = \sum_i f(\lambda_i) |\psi_i\rangle\langle\psi_i|.$$

Why study density matrices?

Lem If  $\Pr[b] > 0$ , then  $\sigma_b$  is a well-defined d.m.

Pf. Each  $\Pi_b |\Psi_a\rangle\langle\Psi_a| \Pi_b$  is Hermitian and psd, then

$\sigma_b$  is Hermitian and psd as linear combination of.

$$\text{tr}(\sigma_b) = \frac{\text{tr}(\Pi_b \rho \Pi_b)}{\text{tr}(\Pi_b \rho)} = \frac{\text{tr}(\Pi_b \rho)}{\text{tr}(\Pi_b \rho)} = 1.$$

Prop If, with prob  $p_a$ , setup  $\rho_a$  on one system and  $\sigma_a$  on second system, then  $\sum_a p_a (\rho_a \otimes \sigma_a)$ .

We have extended our update rules for d.m.

- ① Describe prob. dist. + entanglement at the same time.
- ② Describe partial states of larger entangled systems.

## The state of a subsystem

Alice & Bob currently are described by  $\rho_{AB} \in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$ .

Bob goes away, never to return. How do we describe Alice's system?

Case 1:  $\rho_{AB} = \rho_A \otimes \rho_B$ .      unentangled      Ans:  $\rho_A$ .

Case 2:  $\rho_{AB} = \sum_i p_i \rho_A^i \otimes \rho_B^i$ .      Ans:  $\sum p_i \rho_A^i$ .

giving rolling dice interpretation.

What about systems that are not linear combinations of unentangled?

The "state of a system" is a description from which all "experiments" can be calculated.

Goal today: figure out how to compute  $p_a$  from any d.m.  $\rho_{AB}$ .

Lem  $\rho_{AB}$ .  $\Pr(\text{Alice measures } a)$  is independent of

- ① Any unitary Bob applies to B.
- ② Any measurement Bob applies to B.

Pf. Alice measuring her first qubit as  $a$ :

$$\Pi_a = (|a\rangle\langle a| \otimes \mathbb{1}) \otimes \mathbb{1}_B. \quad \Pr(a) = \text{tr}(\Pi_a \rho_{AB}).$$

Imagine Bob first applies  $U_B$ . Then

$$\begin{aligned} & \text{tr}(\Pi_a (\mathbb{1} \otimes U_B) \rho_{AB} (\mathbb{1} \otimes U_B)^\dagger) \\ &= \text{tr}((\mathbb{1} \otimes U_B^\dagger) \left[ (|a\rangle\langle a| \otimes \mathbb{1}) \otimes \mathbb{1}_B \right] (\mathbb{1} \otimes U_B) \rho_{AB}) \\ &= \text{tr}(\Pi_a \rho_B). \end{aligned}$$

Bob's unitary transform cannot effect Alice's measurement.

If Bob measures a qubit of his system, like  $\Pi_a$ , we can define projectors  $Q_0, Q_1$  s.t.  $Q_0 + Q_1 = \mathbb{1}_B$  and action on whole system given by  $\mathbb{1}_A \otimes Q_b$ .

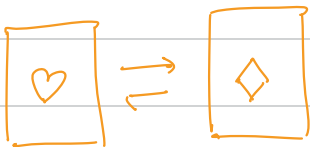
If we don't condition on Bob's outcome,

$$\sigma = \sum_b (\mathbb{1} \otimes Q_b) \rho_{AB} (\mathbb{1} \otimes Q_b). \quad \text{Then,}$$

$$\begin{aligned} \text{tr}(\Pi_a \sigma) &= \sum_b \text{tr}(\Pi_a (\mathbb{1} \otimes Q_b) \rho_{AB} (\mathbb{1} \otimes Q_b)) \\ &= \sum_b \text{tr}(\Pi_a (\mathbb{1} \otimes Q_b^2) \rho_{AB}) \\ &= \sum_b \text{tr}(\Pi_a (\mathbb{1} \otimes Q_b) \rho_{AB}) \\ &= \text{tr}(\Pi_a \rho_{AB}). \end{aligned} \quad \square$$

Alice

Bob



Alice's card random but Bob revealing informs Alice. Bob looking does not.

Operational property: Discarding Bob's system yields the same state if done before or after actions restricted to either half.

## Partial Trace

$$\mathcal{H}_A = \text{span} \{ |a_1\rangle, \dots, |a_{d_A}\rangle \}, \quad \mathcal{H}_B = \text{span} \{ |b_1\rangle, \dots, |b_{d_B}\rangle \}.$$

$$\mathcal{H}_A \otimes \mathcal{H}_B \text{ has basis } \{ |a_i\rangle \otimes |b_j\rangle : i \in [d_A], j \in [d_B] \}.$$

Def. If  $X$  an operator on  $\mathcal{H}_A \otimes \mathcal{H}_B$ .

$$\text{Then, } \text{tr}_B : \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B) \rightarrow \mathcal{L}(\mathcal{H}_A).$$

$$\text{tr}_B(X) := \sum_{j=1}^{d_B} (\mathbb{1}_A \otimes \langle b_j |) X (\mathbb{1}_A \otimes |b_j\rangle).$$

Note:  $\text{tr}_B$  is a linear transformation.

Ex.  $X = |a_i, b_j\rangle\langle a_k, b_\ell|$

Then  $\text{tr}_B(X) = \delta_{j\ell} |a_i\rangle\langle a_k|$ . Do out in class.

Ex.  $X = |EPR\rangle\langle EPR|$ . Do out in class.

$$\text{tr}_A(X) = \sum_{i=1}^{d_A} (\langle a_i| \otimes \mathbb{1}_B) X (|a_i\rangle \otimes \mathbb{1}_B)$$

Consider 2 bit system:

$$X = \sum_{i,j \in \{0,1\}} \sum_{k,\ell \in \{0,1\}} x_{ij,kl} |i,j\rangle\langle k,\ell|$$

$$\text{tr}_A(X) = \sum_{b,b'} \left( \sum_a x_{ab,ab'} \right) |b\rangle\langle b'|$$

There is a nice picture.

|                |                |
|----------------|----------------|
| $\chi_{00,00}$ | $\chi_{00,01}$ |
| $\chi$         | $\chi$         |

|                |                |
|----------------|----------------|
| $\chi_{00,10}$ | $\chi_{00,11}$ |
| $\chi$         | $\chi$         |

|        |        |
|--------|--------|
| $\chi$ | $\chi$ |
| $\chi$ | $\chi$ |

|        |        |
|--------|--------|
| $\chi$ | $\chi$ |
| $\chi$ | $\chi$ |

$$\text{Then, } \text{tr}_A(X) = \begin{array}{|c|c|} \hline \chi_{00,00} & \chi_{00,01} \\ \hline \chi & \chi \\ \hline \end{array} + \begin{array}{|c|c|} \hline \chi & \chi \\ \hline \chi & \chi \\ \hline \end{array}$$

Exercise Verify that  $\text{tr}_B(\rho_A \otimes \rho_B) = \rho_A$ .

$$\xrightarrow{\text{Ex}} \text{tr}_B(\rho_{AB}) \quad \text{where} \quad \rho_{AB} = \begin{bmatrix} \frac{1}{6} & \frac{-i}{6} & 0 & \frac{-1}{6} \\ \frac{i}{6} & \frac{1}{3} & 0 & \frac{1-i}{6} \\ 0 & 0 & \frac{1}{6} & 0 \\ \frac{-1}{6} & \frac{1+i}{6} & 0 & \frac{1}{3} \end{bmatrix}.$$

Lem  $\rho_{AB}$  d.m. then define  $\rho_A := \text{tr}_B(\rho_{AB})$ . Then

①  $\rho_A$  is a d.m.

② For any operator  $M_A$  on  $\mathcal{H}_A$ ,

$$\text{tr}(M_A \rho_A) = \text{tr}((M_A \otimes \mathbb{1}_B) \rho_{AB}).$$

③ For any unitaries  $U_A, U_B$  on  $\mathcal{H}_A$  and  $\mathcal{H}_B$ , respectively,

$$\text{tr}_B((U_A \otimes U_B) \rho_{AB} (U_A \otimes U_B)^\dagger) = U_A \rho_A U_A^\dagger.$$

④ Any unrecorded measurement on Bob's system, does not change  $\rho_A$ .

$$\textcircled{b} \text{ For } \rho_{AB} = \sum_i p_i \rho_A^i \otimes \rho_B^i \Rightarrow \rho_A = \sum_i p_i \rho_A^i.$$

Pf. Start with ②,

$$\begin{aligned} \text{tr}(M_A \text{tr}_B(\rho_{AB})) &= \text{tr}\left(M_A \sum_j (\mathbb{1}_A \otimes \langle b_j |) \rho_{AB} (\mathbb{1}_A \otimes |b_j\rangle)\right) \\ &= \text{tr}\left(M_A \left(\sum_j \mathbb{1}_A \otimes |b_j\rangle \langle b_j|\right) \rho_{AB}\right) \text{ by cyclicity.} \end{aligned}$$

$$= \text{tr}((M_A \otimes \mathbb{1}_B) \rho_{AB}).$$

origin of name partial trace.

Take  $M_A = \mathbb{1}$  proves  $\boxed{\text{tr}(\rho_A) = \text{tr}(\rho_{AB}) = 1.}$

For positivity,  $\langle v | \rho_A | v \rangle = \sum_j (\langle v | \otimes \mathbb{1}) (\mathbb{1} \otimes \langle b_j |) \rho_{AB} (\mathbb{1} \otimes | b_j \rangle) (| v \rangle \otimes \mathbb{1})$

$$= \sum_j \langle v, b_j | \rho_{AB} | v, b_j \rangle$$

$$\geq 0.$$

For ③, suppose Alice & Bob apply  $U_A \otimes U_B$ .

$$\sigma_{AB} = (U_A \otimes U_B) \rho_{AB} (U_A \otimes U_B)^\dagger.$$

Calculate  $\text{tr}(M_A \sigma_A)$  and  $\text{tr}(M_A (U_A \rho_A U_A^\dagger))$

$$\Rightarrow \sigma_A = U_A \rho_A U_A^\dagger.$$

Cor. Partial trace is basis independent.

Then the partial trace is the unique linear transform  $T_B$  s.t.

$$\text{tr}(M_A T_B(X)) = \text{tr}((M_A \otimes \mathbb{1}_B)X).$$

Return to EPR: Partial trace proves that after tracing out half the system, each is left with a coin flip.

Maximally mixed & entangled states.

Define  $\mathbb{1}/d$  and Maximally entangled, for  $\dim \mathcal{H}_A = \dim \mathcal{H}_B = d$ .

Generalized |EPR>.

Generalized measurements

$$\text{POVM } \{Q_a\} \text{ s.t. } Q_a \geq 0, \sum_a Q_a = \mathbb{1}.$$

$\Pr(a) = \text{tr}(Q_a \rho)$ . Note POVMs don't specify the post-measurement state.

Since  $Q_a \geq 0 \Rightarrow \langle \psi | Q_a | \psi \rangle \geq 0 \quad \forall |\psi\rangle$

$$\Rightarrow \text{tr}(Q_a \rho) \geq 0.$$

$$\sum_a \Pr(a) = \sum_a \text{tr}(Q_a \rho) = \text{tr}\left(\left(\sum_a Q_a\right) \rho\right) = 1.$$

Possible implementations:  $M_a^\dagger M_a = Q_a$

$$\text{then } \rho_a = \frac{M_a \rho M_a^\dagger}{\text{tr}(Q_a \rho)}.$$

Ex. Fix  $\eta \in [0, 1]$ . 2 outcome POVM

$$Q_\pm = \frac{1 \pm \eta Z}{2}. \quad \text{Eigenvalues of } Q_\pm \text{ are } \frac{1 \pm \eta}{2} \text{ so } Q_\pm \geq 0.$$

$$Q_+ + Q_- = \mathbb{1}.$$

$$Q_{\pm} = \frac{1 \pm \eta}{2} |0\rangle\langle 0| + \frac{1 \mp \eta}{2} |1\rangle\langle 1|.$$

$$\Pr[\text{outcome} = +] = \text{tr}(Q_+ \rho) = \frac{1}{2} + \frac{\eta}{2} \text{tr}(Z \rho).$$

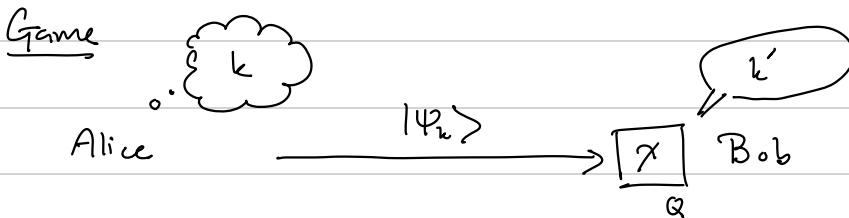
What is the operational interpretation of this POVM?

Ex.  $\omega = e^{2\pi i/3}$  and define for  $k = 0, 1, 2$ ,

$$|\psi_k\rangle := \frac{|0\rangle + \omega^k |1\rangle}{\sqrt{2}}. \quad \text{Let } Q_k = \frac{2}{3} |\psi_k\rangle\langle\psi_k|.$$

$$= \frac{1}{3} \begin{pmatrix} 1 & \omega^k \\ \omega^{-k} & 1 \end{pmatrix}$$

Since  $1 + \omega + \omega^2 = 0$ ,  $\sum Q_k = \mathbb{1}$ .



$$\Pr[k = k'] = \langle \psi_k | Q_k | \psi_k \rangle = \frac{2}{3}.$$

Turns out best possible algorithm (not easy to prove).

Implementing POVMs Pset problem!