Entanglement

A property of multiple quantum systems. The individual systems have undergone some interaction and are no longer independent. The overall state of the system is somehow correlated in a special quantum manner which we call entanglement.

Def^n (Entanglement-Bipartite)

Let A, B be quantum systems with associated Hilbert spaces $\mathcal{H}_A, \mathcal{H}_B$. The state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is product if $\exists$ $|\phi_A\rangle \in \mathcal{H}_A$ and $|\phi_B\rangle \in \mathcal{H}_B$ such that

$$|\psi\rangle = |\phi_A\rangle \otimes |\phi_B\rangle.$$

Otherwise, we say that $|\psi\rangle$ is entangled.

Examples

1) $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is entangled
$\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$ is product.

2) $\sum_i \sqrt{\lambda_i}\, |\phi_i\rangle \otimes |\psi_i\rangle$ for ONBs $\{|\phi_i\rangle\}_i, \{|\psi_i\rangle\}_i$.
is entangled if λ_i is nonzero for more than 1 index i.

(Multipartite entanglement)

For more that two systems you can classify entanglement in different ways as certain subsystems may not be entangled. I.e., $|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |110\rangle)$, is entangled on the first two systems but in product with the third.

The rest of this lecture will be dedicated to some interesting properties and advantages afforded to us by entanglement and we will focus mainly on bipartite entanglement

Exercise: Suppose Alice and Bob each have their own quantum system and that the state of the joint system is a product state, i.e. $|\psi\rangle = |\phi_A\rangle \otimes |\phi_B\rangle$. If Alice measures her system with a measurement $\{M_a\}$ and Bob measures his system with a measurement $\{N_b\}$, show that the joint distribution of the measurement outcomes factorizes

$$P(a,b) = P(a)P(b).$$

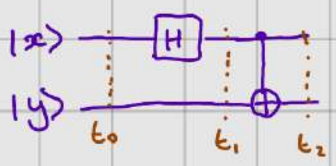
Bell-States

The following two-qubit states will be used frequently:

$$|\Phi_{00}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$
$$|\Phi_{01}\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)$$
$$|\Phi_{10}\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)$$
$$|\Phi_{11}\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$$

They are known as Bell-states and form a basis for $\mathbb{C}^2 \otimes \mathbb{C}^2$. This is a basis of entangled states as opposed to product bases like $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

They can be generated via the circuit:



$\longrightarrow |\Phi_{xy}\rangle$

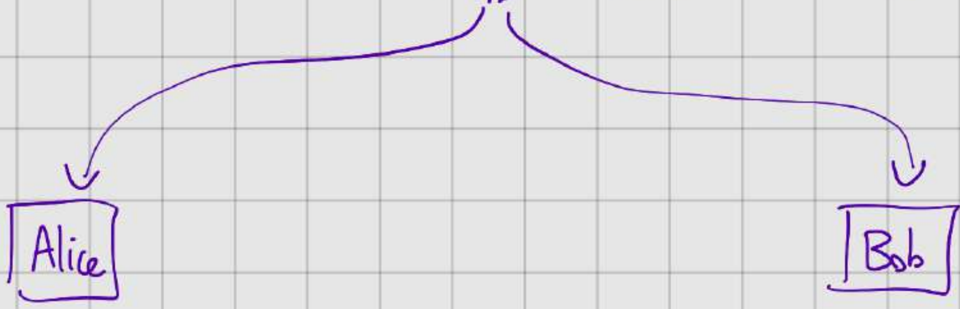
$$|\psi_{t_0}\rangle = |x\rangle|y\rangle$$
$$|\psi_{t_1}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^x|1\rangle\right)|y\rangle$$
$$|\psi_{t_2}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|y\rangle + (-1)^x|1\rangle|y\oplus 1\rangle\right) = |\Phi_{xy}\rangle$$

The EPR Paradox

- Objection to QT's apparent lack of properties defined independently of measurement.

Suppose we begin with the state

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$



Suppose Alice measures in the Z basis $\{|0\rangle, |1\rangle\}$.
On outcome 0 the state after measurement is

$$|00\rangle$$

On outcome 1 the " "

$$|11\rangle.$$

After measurement Alice can predict with <u>certainty</u> what Bob will measure if he measures in Z basis also.

This will work even if Alice and Bob are spacelike/causally separated.

Remark (Special Relativity)

At first glance this appears to violate the laws of relativity that information cannot travel faster than light. But actually Alice cannot use this to transmit information.

Suppose she tries to transmit some information by choosing different bases to measure in. Bob can try to receive this information by also measuring in different Bases. However one can show that

$$\sum_b p(a,b|xy) = p(a|x,y) = p(a|x) \quad \text{AND}$$

$$\sum_a p(ab|xy) = p(b|x,y) = p(b|y)$$

That is, Alice and Bob's local statistics do not depend on the inputs of the other party. Hence we cannot use this experiment to transmit any information.

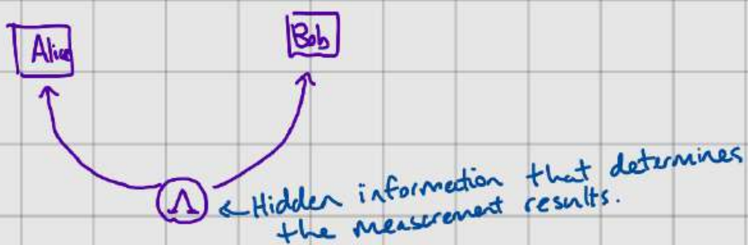
Like two correlated coins. Hidden information reveals that the experiment is not surprising.

Back to EPR Paradox

EPR had the following issue with QT. They argued that if you could know the value of a measurement with certainty without disturbing the system then the value of that measurement should be predetermined.

They then argued that the above experiment implies that the outcomes of the measurements should be determined. Because QT does not predict this, they argue that quantum theory is not a complete description of reality.

They wanted something like:



Hidden variables are not sufficient

Consider an experiment

$a, b, x, y \in \{0,1\}$.

CHSH Game

x, y are randomly chosen questions $\qquad p(x,y) = \frac{1}{4}$

a, b are answers

Alice and Bob win (score 1) if $a \oplus b = xy$

lose (score 0) if $a \oplus b \neq xy$

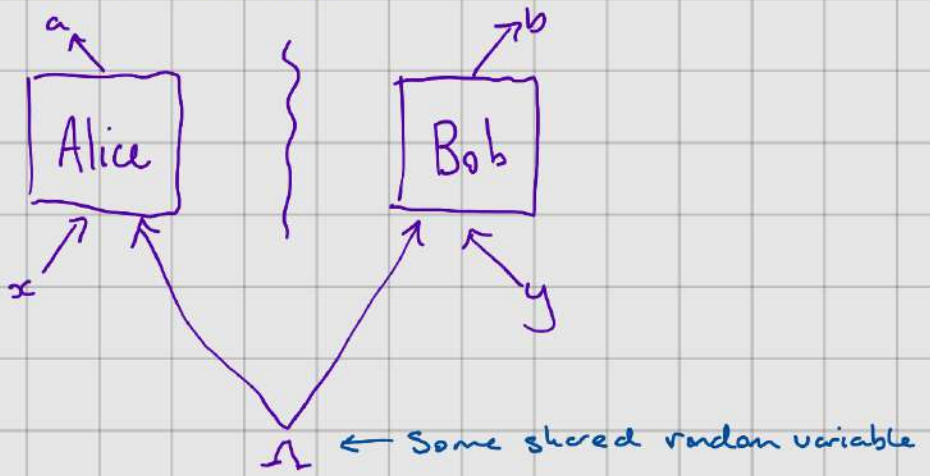
For $(x,y) \in \{(0,0), (0,1), (1,0)\}$ respond with same answer

For $(x,y) = (1,1)$ respond with different answers.

$$P_{win} = \frac{1}{4} \sum_{a \oplus b = xy} p(ab|xy)$$ – expected probability to win.

Local Hidden Variable

EPR would argue that the experiment should be predictable by some hidden local information



Such an experiment can be modelled by a distribution

Any correlations are mediated by λ

$$p(ab|xy) = \sum_{\lambda} p(\lambda)\, p(a|x,\lambda)\, p(b|y,\lambda)$$

We call any distribution of the above form a local distribution. $\mathcal{L}$

Quantum Explanation

Instead we may model the experiment using QT.

Alice and Bob share a state $|\psi\rangle_{AB}$ and use measurements $\{M_{a|x}\}_a$ and $\{N_{b|y}\}$.

$$p(a,b|x,y) = \langle\psi| M_{a|x} \otimes N_{b|y} |\psi\rangle$$

$\mathcal{Q}$

Local bound $\quad \sup_{p \in \mathcal{L}} \frac{1}{4} \sum_{a \oplus b = xy} p(ab|xy) = 3/4$

Example strategy

x	y	a	b	win
0	0	0	0	✓
0	1	0	0	✓
1	0	0	0	✓
1	1	0	0	✗

win 3/4 times

Quantum Bound

We consider a strategy

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Alice measures:

$x=0 \longrightarrow Z \quad \{|0\rangle, |1\rangle\}$

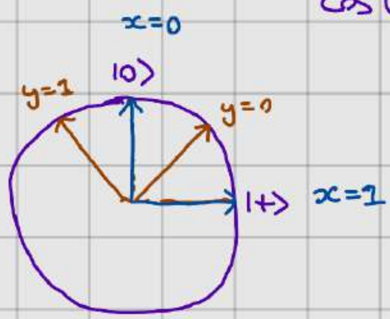
$x=1 \longrightarrow X \quad \{|+\rangle, |-\rangle\}$

Bob measures

$y=0 \longrightarrow \frac{Z+X}{\sqrt{2}} \quad \{\cos(\frac{\pi}{8})|0\rangle + \sin(\frac{\pi}{8})|1\rangle, \cos(\frac{\pi}{8}+\frac{\pi}{2})|0\rangle + \sin(\frac{\pi}{8}+\frac{\pi}{2})|1\rangle\}$

$y=1 \longrightarrow \frac{Z-X}{\sqrt{2}} \quad \{\cos(-\frac{\pi}{8})|0\rangle + \sin(-\frac{\pi}{8})|1\rangle, \cos(-\frac{\pi}{8}+\frac{\pi}{2})|0\rangle + \sin(-\frac{\pi}{8}+\frac{\pi}{2})|1\rangle\}$

In the Bloch sphere



Distribution looks like

$$P_{ab|xy} = \begin{pmatrix} \varepsilon & \frac{1}{2}-\varepsilon \\ \frac{1}{2}-\varepsilon & \varepsilon \end{pmatrix} \quad \text{for } (x,y) \neq (1,1)$$

with $\varepsilon = \frac{1}{2}\cos^2(\frac{\pi}{8})$

$$P_{ab|xy} = \begin{pmatrix} \frac{1}{2}-\varepsilon & \varepsilon \\ \varepsilon & \frac{1}{2}-\varepsilon \end{pmatrix} \quad \text{for } (x,y) = (1,1)$$

Overall we win with probability $\quad 4 \cdot \frac{1}{4} \cdot 2\varepsilon = 2\varepsilon = \cos^2\left(\frac{\pi}{8}\right)$
$\approx 0.853\ldots$

As $\cos^2(\pi/8) > 3/4$ quantum theory cannot be described by the EPR hidden variable model! We say QT is <u>nonlocal</u>. The above CHSH game is known as a <u>nonlocal game</u> and it is designed to allow you to refute a local description of the experiment.

$$V(a,b,x,y) = \begin{cases} 1 & \text{if } a \oplus b = xy \\ 0 & \text{otherwise} \end{cases}$$ game predicate

<u>Remark (Tsirelson Bound)</u>

The maximal quantum value of a game $\quad \sup_{p \in Q} \sum_{\substack{ab \\ xy}} p(xy)\, p(ab|xy)\, V(a,b,x,y)$ is known as the quantum value or the Tsirelson bound. For CHSH the maximal expected winning probability is $\quad \cos^2(\pi/8) = \frac{1}{2} + \frac{\sqrt{2}}{4}$. (See exercises)

Nonlocal games are not just fondational curiosities. They have important applications to cryptography and elsewhere.

<u>Device-independent Crytography</u>

We have two untrusted devices A and B. Suppose we use them to play the CHSH game and we win with prob $\omega > 3/4$.
What can we conclude?

* The devices must be using some quantum systems.

These quantum systems have some interesting properties. In particular, they must be producing <u>private</u> randomness.

That is, there is no additional information E such that conditioned on that information the distribution $p(ab|xye) \in \{0,1\}$. $\forall$ $abxye$

All such distributions are in the local set!

Guaranteed even if you don't trust the devices.

From observing certain correlations one can guarantee a source of randomness!

* Randomness expanders
* Randomness amplifiers
* Secret Key expanders
* Self-testing
* Many more...

Experimental Verification

Recent experimental verification that QT is nonlocal.

2015/2016 - loophole free Bell-tests
Delft / NIST / Vienna

2019 + - First DI experiments.

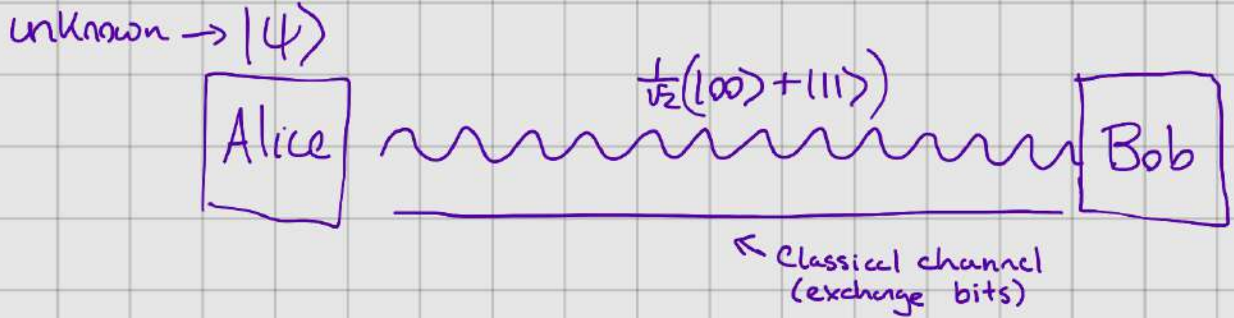
Loopholes

It is difficult to experimentally achieve nonlocality, many losses/noise push the statistics towards the local set.

* locality loophole - not achieving spacelike separation.
* Detection loophole - must record all events (even losses).

Quantum Teleportation

Entangled states + classical communication act as a quantum channel.

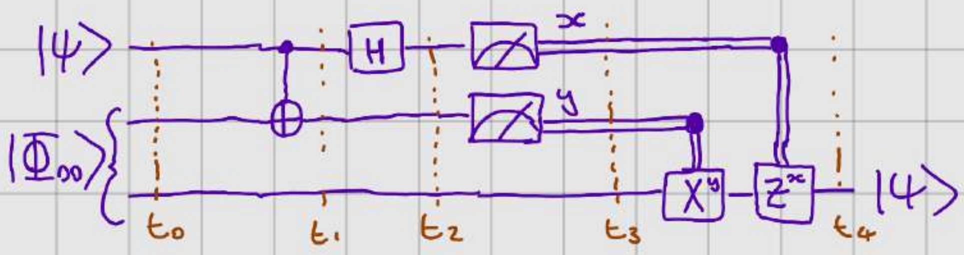


* Share a state $|\Phi_{00}\rangle$
* Can communicate classically

Alice wants to send a qubit $|\psi\rangle$ to Bob but there is no quantum channel to do so. How can Bob obtain $|\psi\rangle$?

* Measure and describe state to Bob?
  - Only one copy so can't determine state... (Measurement disturbs / No cloning)
  - Even knowing state you need potentially infinite bits because amplitudes are continuous.

Alice can use her part of the entangled state to change Bob's half of $|\Phi_{00}\rangle$ into $|\psi\rangle$!



Time t_0

Overall state is $\qquad |\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

$$|\psi\rangle|\Phi_{00}\rangle = \frac{1}{\sqrt{2}}\left(\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)\right)$$

Time t_1

Alice interacts $|\psi\rangle$ with her half of $|\Phi_{00}\rangle$. $\qquad |0\rangle\langle 0| \otimes \mathbb{1} \otimes \mathbb{1} + |1\rangle\langle 1| \otimes X \otimes \mathbb{1}$

$$\frac{1}{\sqrt{2}}\left(\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)\right)$$

Time t_2

Alice applies $\boxed{H}$ to 1st qubit

$$\frac{1}{\sqrt{2}}\Big(\alpha|+\rangle(|00\rangle+|11\rangle) + \beta|-\rangle(|10\rangle+|01\rangle)\Big)$$

$$= \frac{1}{2}\Big(\alpha(|0\rangle+|1\rangle)(|00\rangle+|11\rangle) + \beta(|0\rangle-|1\rangle)(|10\rangle+|01\rangle)\Big)$$

$$= \frac{1}{2}\Big(\alpha(|000\rangle+|100\rangle+|011\rangle+|111\rangle) + \beta(|010\rangle+|001\rangle-|110\rangle-|101\rangle)\Big)$$

$$= \frac{1}{2}\Big(|00\rangle(\alpha|0\rangle+\beta|1\rangle) + |01\rangle(\alpha|1\rangle+\beta|0\rangle) + |10\rangle(\alpha|0\rangle-\beta|1\rangle) + |11\rangle(\alpha|1\rangle-\beta|0\rangle)\Big)$$

Time t_3

Alice measures first two qubits.

Outcome	Prob	PMS
00	$\frac{1}{4}$	$\lvert 00\rangle(\alpha\lvert 0\rangle+\beta\lvert 1\rangle)$
01	$\frac{1}{4}$	$\lvert 01\rangle(\alpha\lvert 1\rangle+\beta\lvert 0\rangle)$
10	$\frac{1}{4}$	$\lvert 10\rangle(\alpha\lvert 0\rangle-\beta\lvert 1\rangle)$
11	$\frac{1}{4}$	$\lvert 11\rangle(\alpha\lvert 1\rangle-\beta\lvert 0\rangle)$

Time t_4

Alice sends Bob results of measurement and he corrects his qubit!

What corrects should he make?

* Why is this not violating SR?
* Why does this not violate No cloning?

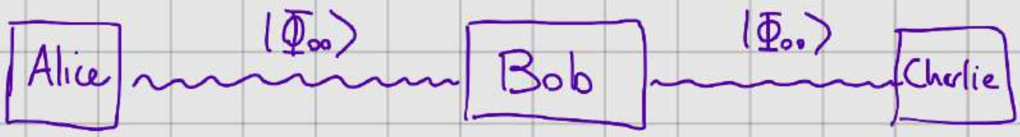
Teleportation shows that different resources can be combined to create a new resource. Entanglement + Classical Communication $\longrightarrow$ Quantum Channel.

Teleportation can also be used to build useful gates and to aid error correction.

Remark: The first 3 timesteps can be also viewed as Alice measuring her two qubits in the $\{|\Phi_{xy}\rangle\}_{xy}$ Bell-basis.

Entanglement Swapping

It is possible to entangle two particles that have never interacted before.



State of whole system is $\quad |\Phi_{00}\rangle_{AB_1} \otimes |\Phi_{00}\rangle_{B_2C}$

Alice and charlie's particles have never interacted, at the moment they are completely independent systems. Bob can use his two systems to transfer entanglement to Alice and Charlie...

He performs a measurement in the Bell basis on his two qubits
$\{|\Phi_{ij}\rangle\}_{ij}$

State at beginning $\quad \frac{1}{2}\left(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle\right)$

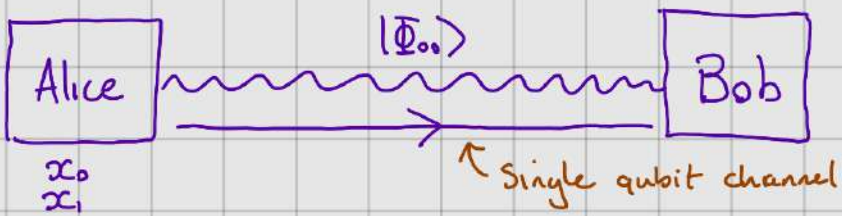
Outcome	Prob	PMS
00	1/4	$\frac{1}{\sqrt{2}}\left(|0\rangle|\Phi_{00}\rangle|0\rangle + |1\rangle|\Phi_{00}\rangle|1\rangle\right)$
01	1/4	$\frac{1}{\sqrt{2}}\left(|0\rangle|\Phi_{01}\rangle|1\rangle + |1\rangle|\Phi_{01}\rangle|0\rangle\right)$
10	1/4	$\frac{1}{\sqrt{2}}\left(|0\rangle|\Phi_{10}\rangle|0\rangle - |1\rangle|\Phi_{10}\rangle|1\rangle\right)$
11	1/4	$\frac{1}{\sqrt{2}}\left(|0\rangle|\Phi_{11}\rangle|1\rangle - |1\rangle|\Phi_{11}\rangle|0\rangle\right)$

Can also view this as a teleportation protocol Bob teleports 1 of his qubits through the other entangled pair to one of the parties.

* Useful for sharing entanglement in networks
* Crytographic applications
* Both swapping and teleportation have been implemented experimentally.

Superdense Coding

Preshared 2-qubit entanglement + single qubit channel
$\Longrightarrow$ 2 bits of communication.



Alice wants to send a random two bit message x_0x_1 to Bob.
She can do this by sending just a single qubit of information

* Holevo's th^{m} (later in course) - at most one classical bit of information can be transmitted via a qubit.

$$X \xrightarrow{\text{encode}} |\psi\rangle \xrightarrow[\text{measure}]{\text{decode}} Y \qquad I(X:Y) \text{ - mutual information}$$

$$I(X:Y) \leq 1$$

Using preshared entanglement we can break this bound. Entanglement acts as a potential bit of communication.

Message	Action	State
00	$\mathbb{1} \otimes \mathbb{1}$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$
01	$Z \otimes \mathbb{1}$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$
10	$X \otimes \mathbb{1}$	$\frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$
11	$ZX \otimes \mathbb{1}$	$\frac{1}{\sqrt{2}}(-\|10\rangle + \|01\rangle)$

What do now?
Bell basis
|
Orthogonal
|
Perfectly distinguishable!

Measurement for Bob recovers the values x_0x_1!

Lemma

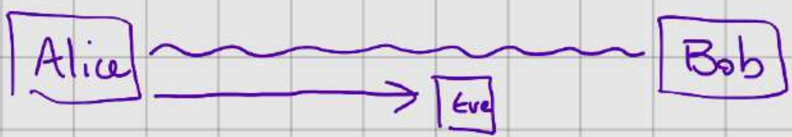
Let $\{P, \mathbb{1} - P\}$ be a qubit projective measurement (not $\{\mathbb{1}, 0\}$). Then

$$\langle \Phi_{ij} | (P \otimes \mathbb{1}) | \Phi_{ij} \rangle = \frac{1}{2}$$

Proof Exercise....

What does the above lemma say about a Bell-state resource?

* Locally a source of randomness
* Local information provides no information about the global state!



Suppose Alice and Bob are executing the superdense coding protocol to send information. Eve intercepts the qubit Alice sends to Bob. Is the message secure?

Yes - if Eve can only measure one part of the system then she can't learn anything. The message is encoded as a global property!

Communication Complexity Advantages

How much communication is needed to compute $f(a,b,c)$ when a,b,c are held by separate parties?

Example

Alice	Bob	Charlie
$a_0 a_1$	$b_0 b_1$	$c_0 c_1$

$a \vee b = \begin{cases} 0 & a=b=0 \\ 1 & \text{otherwise} \end{cases}$

Each party has 2bit input. Want to compute

PROMISED $\boxed{a_0 \oplus b_0 \oplus c_0 = 0}$

$$f(a,b,c) = a_1 \oplus b_1 \oplus c_1 \oplus (a_0 \vee b_0 \vee c_0)$$

* 4 bits of communication is sufficient
  - Alice announces $a_0 a_1$
  - If $a_0 = 1$ then announce b_1 and c_1
  - If $a_0 = 0$ then Bob announces $b_0 \oplus b_1$, Charlie announces c_1

$b_0 = 1 \Rightarrow$ RHS $= 1$
$b_0 = 0 \Rightarrow$ RHS $= 0$
by promise.

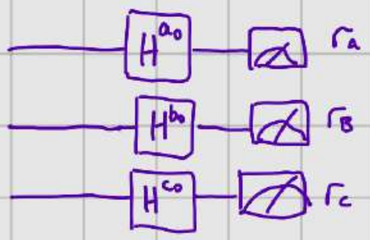
* 4 bits necessary is more involved (see Buhrman et al. Quantum entanglement and communication complexity 2001)

A quantum strategy

The parties share the state

$$|\Psi_{ABC}\rangle = \frac{1}{2}\left(|000\rangle - |011\rangle - |101\rangle - |110\rangle\right)$$

We use the circuit



Communicate $a_1 \oplus r_A$
$b_1 \oplus r_B$
$c_1 \oplus r_C$

Claim $r_A \oplus r_B \oplus r_C = a_0 \vee b_0 \vee c_0$

Suppose $a_0 = b_0 = c_0 = 0$

Then we get

Outcome	Prob
000	1/4
011	1/4
101	1/4
110	1/4

$r_A \oplus r_B \oplus r_C = 0$ ✓

Suppose $a_0 = b_0 = 1$ $c_0 = 0$ then state is

$$\frac{1}{2}\left(|{+}{+}0\rangle - |{+}{-}1\rangle - |{-}{+}1\rangle - |{-}{-}0\rangle \right)$$

$$= \frac{1}{4}\big(|000\rangle + |010\rangle + |100\rangle + |110\rangle - |001\rangle + |011\rangle - |101\rangle + |111\rangle$$
$$- |001\rangle - |011\rangle + |101\rangle + |111\rangle - |000\rangle + |010\rangle + |100\rangle - |110\rangle \big)$$

$$= \frac{1}{4}\left(2|010\rangle + 2|100\rangle - 2|001\rangle + 2|111\rangle \right)$$

Outcome	Prob
010	1/4
100	1/4
001	1/4
111	1/4

$r_A \oplus r_B \oplus r_C = 1$ ✓

By symmetry of the state the other cases must work also!

Density Operators

With the introduced formalism it is cumbersome to describe probabilistic mixtures of quantum states

$$\{(p_i, |\psi_i\rangle)\}_i$$

Density operators offer a convenient method to encode this. Suppose I prepare a system $\mathcal{H}$ in state $|\psi_i\rangle$ with probability p_i. We can describe the state of that system using a density operator

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

As we'll see below measurement probabilities are computed as

$$\mathbb{P}(i) = \mathrm{Tr}(\rho P_i)$$

where $\{P_i\}$ is a projective measurement. This is consistent with the interpretation of ρ as a probabilistic mixture of preparations.

Eg.

$$\mathbb{P}(i) = \mathrm{Tr}(\rho P_i) = \sum_j p_j \mathrm{Tr}(P_i |\psi_j\rangle\langle\psi_j|)$$

$$= \sum_j p_j \langle\psi_j|P_i|\psi_j\rangle = \sum_j p_j \mathbb{P}(i \mid |\psi_j\rangle)$$

What we expect from such an experiment.

ρ is a linear operator $\mathcal{H} \to \mathcal{H}$.

Def^n (Density Operator)

Given a Hilbert space $\mathcal{H}$, a density operator $\rho : \mathcal{H} \to \mathcal{H}$ is a linear operator satisfying

1) $\rho \geq 0$ (positive semidefinite)
2) $\mathrm{Tr}(\rho) = 1$ (unit trace)

Remark (Trace)

Given a square matrix $M = (m_{ij})_{ij}$ we can define its trace as

$$\mathrm{Tr}(M) := \sum_i m_{ii} = \sum_i \langle i|M|i\rangle$$

computational basis.

It satisfies some properties

- (linear) $\mathrm{Tr}(\alpha A + \beta B) = \alpha \mathrm{Tr}(A) + \beta \mathrm{Tr}(B)$, $\alpha, \beta \in \mathbb{C}$

- (Cyclic) $\mathrm{Tr}[AB] = \mathrm{Tr}[BA]$

* (Inner product) On $M_{n\times n}(\mathbb{C})$, vector space of $n\times n$ matrices with entries in $\mathbb{C}$, forms an inner-product

$$\langle A, B\rangle = Tr[A^{+}B]$$

* (Tensor Product) $Tr(A\otimes B) = Tr(A)\otimes Tr(B)$

By spectral theorem all density operators can be expressed in the form

$$\rho = \sum \lambda_i |\psi_i\rangle\langle\psi_i|$$

where $|\psi_i\rangle$ form an orthonormal basis for the space. Furthermore $\sum_i \lambda_i = 1$ with $\lambda_i \in [0,1] \Rightarrow$ we have an operational meaning for density operators.

<u>Postulate (States - extended)</u>

A quantum state is represented by a density operator acting on the systems associated Hilbert space.

<u>Examples</u>

* $\rho = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$ is the maximally mixed state for a qubit system.

* $\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|+\rangle\langle +| = \begin{pmatrix} \frac{3}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} \end{pmatrix}$

* If $|\psi\rangle = e^{it}|\phi\rangle$ then they correspond to the same density operator $|\psi\rangle\langle\psi| = e^{it}e^{-it}|\phi\rangle\langle\phi| = |\phi\rangle\langle\phi|$

* $\rho = |\psi\rangle\langle\psi|$ - <u>pure</u> state
  - otherwise we say it is <u>mixed</u>.

Bloch Sphere Representation

Qubit

$$\rho = \begin{pmatrix} \alpha & \beta \\ \beta^* & 1-\alpha \end{pmatrix}$$

Can decompose ρ in operator basis $\{\frac{1}{2}\mathbb{1}, \frac{1}{2}X, \frac{1}{2}Y, \frac{1}{2}Z\}$.
This is an orthonormal basis for $M_{2\times 2}(\mathbb{C})$ - respect to $\langle A, B\rangle = \mathrm{Tr}(A^\dagger B)$

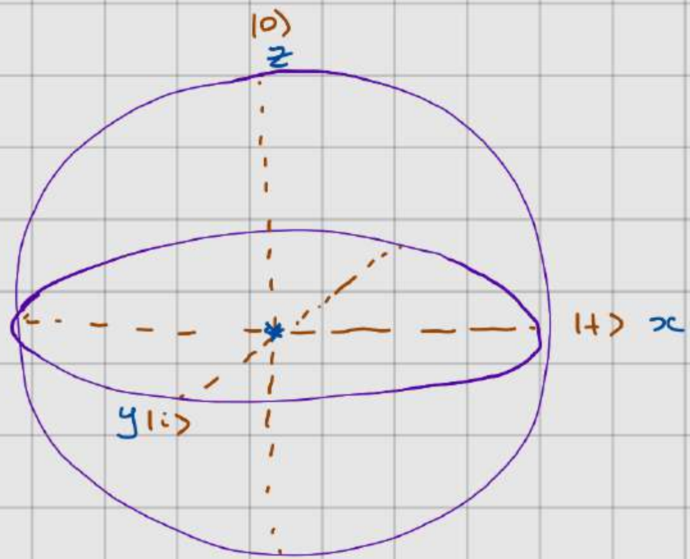
$$\rho = \frac{n_0 \mathbb{1} + n_x X + n_y Y + n_z Z}{2}$$

$\mathrm{Tr}[\rho] = 1 \Rightarrow n_0 = 1$

$\rho = \rho^\dagger \Rightarrow (n_x, n_y, n_z) \in \mathbb{R}^3$

$\rho \geq 0 \Rightarrow n_x^2 + n_y^2 + n_z^2 \leq 1$

$n_x^2 + n_y^2 + n_z^2 = 1$ when ρ is pure.



$* \ \mathbb{1}/2$

$|0\rangle\langle 0|$ corresponds to $(0, 0, 1)$

$$\rho = \frac{\mathbb{1}}{2} + \frac{Z}{2} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \checkmark$$

$|+\rangle\langle +| \longrightarrow (1, 0, 0)$

$$|+\rangle\langle +| = \frac{\mathbb{1}}{2} + \frac{X}{2} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} \checkmark$$

Postulate (Unitary evolution)

A closed systems evolution corresponds to a unitary transformation,

$$\rho \longmapsto U \rho U^{\dagger}$$

Postulate (Measurement)

Measuring a system in state ρ with a measurement $\{P_i\}_i$, the probability of obtaining outcome i is

$$\mathbb{P}(i) = \mathrm{Tr}[\rho P_i]$$

If $P_i = |v\rangle\langle v|$ then $\mathrm{Tr}[\rho |v\rangle\langle v|] = \mathrm{Tr}[\langle v|\rho|v\rangle] = \langle v|\rho|v\rangle$

and afterwards the state updates to

$$\frac{P_i \rho P_i}{\mathrm{Tr}(\rho P_i)} .$$

Multiple systems

Suppose ρ is a state on a joint system AB. We say ρ is <u>separable</u> if $\exists$ states $\{\tau_i\}$ on system A and states $\{\sigma_i\}_i$ on system B and a probability distribution $p(i)$ such that

$$\rho = \sum_i p(i)\, \tau_i \otimes \sigma_i$$

Otherwise we say ρ is entangled.

Def^n (Partial Trace)

Let M be a square matrix acting on a Hilbert space $A \otimes B$. Then we define the partial trace over system A as

$$\mathrm{Tr}_A[M] = \sum_i (\langle i| \otimes \mathbb{1})\, M\, (|i\rangle \otimes \mathbb{1})$$

where $\{|i\rangle\}_i$ is any orthonormal basis for A.

(Similar definition for B).

Let $M = \sum_{\substack{ij \\ kl}} M_{ijkl} \, |i\rangle\langle j| \otimes |k\rangle\langle l|$ (any matrix on $A \otimes B$ can be written like this)

then can define partial trace by the action

$$\mathrm{Tr}_A\left[|i\rangle\langle j| \otimes |k\rangle\langle l|\right] = \mathrm{Tr}\left[|i\rangle\langle j|\right] \otimes |k\rangle\langle l|$$
$$= \delta_{ij} \, |k\rangle\langle l|$$

and extend linearly. Kronecker Delta

Partial trace (Properties)

* (Linear)
* (Partially Cyclic)
$$\mathrm{Tr}_A\left[(M_1 \otimes \mathbb{1}) X (M_2 \otimes \mathbb{1})\right] = \mathrm{Tr}_A\left[(M_2 M_1 \otimes \mathbb{1}) X\right]$$
* $\mathrm{Tr}[X] = \mathrm{Tr}_A\left[\mathrm{Tr}_B[X]\right] = \mathrm{Tr}_B\left[\mathrm{Tr}_A(X)\right]$
* $\mathrm{Tr}_A\left[(\mathbb{1} \otimes X) Z (\mathbb{1} \otimes Y)\right] = X \, \mathrm{Tr}_A(Z) \, Y$

Defining Marginal States

Consider a joint system $A \otimes B$. If we have a state ρ on the whole system can we define states on the subsystems?

Yes! $\rho_A = \mathrm{Tr}_B[\rho]$ $\rho_B = \mathrm{Tr}_A[\rho]$

ρ_A, ρ_B are the states of knowledge of systems A and B (resp) if you ignore the other system.

[Operational justification for partial trace]

Operationally Bob measures his system in any basis $\{|i\rangle\}$

After measurement state on output i is

$$\underbrace{(\mathbb{1}\otimes|i\rangle\langle i|)\rho_{AB}(\mathbb{1}\otimes|i\rangle\langle i|)}_{\rho(i)} = \underbrace{\overbrace{(\mathbb{1}\otimes\langle i|)\rho_{AB}(\mathbb{1}\otimes|i\rangle)}^{p(i)}}_{\text{operator on } \mathcal{H}_A \text{ only}} \otimes|i\rangle\langle i|$$

Now for each i we have a product state. With probability $p(i)$ Alice's state is $(\mathbb{1}\otimes\langle i|)\rho_{AB}(\mathbb{1}\otimes|i\rangle)/p(i)$.

Averaging over i as Alice doesn't learn this her state is then

$$\sum_i (\mathbb{1}\otimes\langle i|)\rho_{AB}(\mathbb{1}\otimes|i\rangle) = Tr_B[\rho_{AB}]$$

(Alice's system should not depend on what operation Bob does locally to his system. Unless she learns some new information).

Not surprising

2 dependent coins

HH or TT

locally look random but if Bob informs Alice of the value of his coin then her local state will change.

Th^m (Partial trace) [Mathematical justification for Partial trace]

$Tr_A : \mathcal{L}(\mathcal{H}_A\otimes\mathcal{H}_B)\to\mathcal{L}(\mathcal{H}_B)$ is the unique linear map satisfying

$$Tr_B(X\otimes Y) = X\,Tr(Y)$$

Proof

Suppose another linear map f existed. $(f(X\otimes Y) = X\,Tr(Y))$

Let $Z\in\mathcal{L}(\mathcal{H}_A\otimes\mathcal{H}_B)$ Then

$$\begin{aligned} f(Z) &= f\Big(\sum_{ijkl} z_{ijkl}\, |i\rangle\langle j|\otimes|k\rangle\langle l|\Big) \\ &= \sum_{ijkl} z_{ijkl}\, f(|i\rangle\langle j|\otimes|k\rangle\langle l|) \\ &= \sum_{ijkl} z_{ijkl}\, |i\rangle\langle j|\, Tr(|k\rangle\langle l|) \\ &= \sum_{ijk} z_{ijkk}\, |i\rangle\langle j| \equiv Tr_B(Z) \end{aligned}$$

⊠

Examples

* $Tr_A[\,|\psi\rangle\langle\psi|_A\otimes|\phi\rangle\langle\phi|_B] = |\phi\rangle\langle\phi|_B$

Makes sense as product systems are independent so our local states should just be the different tensor factors.

- $|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

Then $\rho_A = \rho_B = \mathbb{1}/2 = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$

Consistent with our observation before that $|\psi\rangle$ produces uniform randomness from a local measurement. [See earlier lemma]

Recall proof that $\langle \Phi_{ij}|(P \otimes \mathbb{1})|\Phi_{ij}\rangle$ we can now prove this much easier

Define marginal state $\rho_A = \mathbb{1}/2$
then measure $\mathrm{Tr}[\rho_A P] = \frac{1}{2}\mathrm{Tr}[P] = \frac{1}{2}$

If Bob locally transforms this system with some unitary U, this does not change Alice's local state!

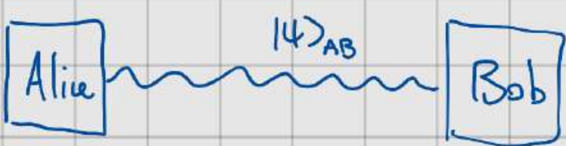
Also consistent with relativity
$\rho_A = \mathrm{Tr}_B[\rho_{AB}] = \mathrm{Tr}_B[(\mathbb{1} \otimes U^\dagger U)\rho_{AB}]$
$= \mathrm{Tr}_B[(\mathbb{1} \otimes U)\rho_{AB}(\mathbb{1} \otimes U^\dagger)]$

- We can use density operators to embed probability theory into quantum. For a discrete probability distribution $\{p(i)\}_i$ we can define a 'classical basis' $\{|i\rangle\}$ (just take computational always) and then

$$\rho = \sum_i p(i)\,|i\rangle\langle i| \equiv \begin{pmatrix} p(0) & 0 & & 0 \\ 0 & p(1) & & \\ & & p(2) & \\ 0 & & & \ddots \end{pmatrix}$$

is called a <u>classical</u> state.

<u>Usage example</u> [Bonus - advanced]



Alice measures $\{P_i\}$ on her part of the state.
After outcome i the state becomes $(P_i \otimes \mathbb{1})|\psi\rangle\langle\psi|(P_i \otimes \mathbb{1}) / \mathrm{Tr}(\ldots)$
Bob's local state is $\rho_B^i = \mathrm{Tr}_A[(P_i \otimes \mathbb{1})|\psi\rangle\langle\psi|(P_i \otimes \mathbb{1})] / \mathrm{Tr}(\ldots)$
Encode information about Alice's outcome and Bob's information in a state

$$\sum_i p(i)\,|i\rangle\langle i| \otimes \rho_B^i$$

cq state
classical-quantum state.
Represents correlation between Alice's outcome and Bob's quantum system.

Crypto / Communication applications, Classical system is some secret / message
Want to know if Bob (potentially an adversary) can learn the value of the system A.

Trace out first system $\rho_B = \sum_i p(i)\rho_B^i$

Becomes a distinguishability problem!

(Solution known in the case of a binary secret.)

$$\boxed{\text{Alice}} \xrightarrow{\quad \rho_x \quad} \boxed{\text{Bob}}$$

$x \in \{0,1\}$ $\qquad\qquad$ $x = ?$

$\underline{\text{Th}^m \text{ (Helstrom)}}$

Let ρ_0, ρ_1 be states on a Hilbert space H.
Then for any $\lambda \in [0,1]$ we have

$$\max_{\{P_0, P_1\}} \lambda \operatorname{Tr}[\rho_0 P_0] + (1-\lambda)\operatorname{Tr}[\rho_1 P_1] = \frac{1}{2} + \frac{1}{2}\|\lambda\rho_0 - (1-\lambda)\rho_1\|_1$$

Probability of successfully distinguishing ρ_0 and ρ_1 when they are sent with a distribution $\{\lambda, 1-\lambda\}$.

$\|X\|_1 := \operatorname{Tr}[(X^\dagger X)^{\frac{1}{2}}]$
(trace norm)

Generalization of p-norm $\|x\|_p = \left(\sum_i |x_i|^p\right)^{\frac{1}{p}}$ for vectors.

$\|X\|_1 = \sum_i |\lambda_i|$

$\underline{\text{Proof}}$

$\underline{\text{Upper bound}}$

Let $\rho = \lambda\rho_0 + (1-\lambda)\rho_1$ and $X = \lambda\rho_0 - (1-\lambda)\rho_1$ $\qquad$ $\lambda\rho_0 = \frac{\rho+X}{2}$ $\quad$ $(1-\lambda)\rho_1 = \frac{\rho - X}{2}$

$$\begin{aligned}
\text{Then } \lambda\operatorname{Tr}(\rho_0 P_0) + (1-\lambda)\operatorname{Tr}(\rho_1 P_1) &= \operatorname{Tr}\left(\frac{\rho+X}{2}P_0\right) + \operatorname{Tr}\left(\frac{\rho-X}{2}P_1\right) \\
&= \frac{1}{2}\operatorname{Tr}(\rho(P_0+P_1)) + \frac{1}{2}\operatorname{Tr}(X(P_0-P_1)) \\
&= \frac{1}{2} + \frac{1}{2}\operatorname{Tr}(X(P_0-P_1)) \\
&\le \frac{1}{2} + \frac{1}{2}\|X\|_1 \|P_0 - P_1\|_\infty \\
&\le \frac{1}{2} + \frac{1}{2}\|X\|_1
\end{aligned}$$

(Hölder's inequality)

$\|Y\|_\infty = \sup_{\|v\rangle} \|Y|v\rangle\|$
$=$ largest absolute eigenvalue (for normal matrices)

Achievability: Take measurement $P_0 =$ projector onto eigenspaces of X with positive eigenvalue

$P_1 = \mathbb{1} - P_0$ (proj onto non-positive eigenspaces)

Use fact that $\|Y\|_1 = \sum_i |\lambda_i|$ λ_i eigenvalues of Y.

Bonus Topics

Schmidt Decomposition & purifications

(Two extremely useful tools)

Th^{m} (Schmidt Decomposition)

Suppose $|\psi\rangle_{AB}$ is a pure state on a bipartite system AB. Then $\exists$ orthonormal bases $\{|v_i\rangle\}_i$ for A and $\{|w_i\rangle\}_i$ for B such that

$$|\psi\rangle = \sum_i \lambda_i |v_i\rangle|w_i\rangle$$

where $\lambda_i \geq 0$ and $\sum_i \lambda_i^2 = 1$. λ_i - Schmidt coefficients.

Proof We can write $|\psi\rangle = \sum_{ij} a_{ij} |i\rangle|j\rangle$ for $a_{ij} \in \mathbb{C}$.
Let $A = (a_{ij})_{ij}$. By singular value decomposition $\exists$ unitary matrices U, V and a non-negative diagonal matrix D such that $A = UDV$
$a_{ij} = \sum_{ijk} u_{ik} d_{kk} v_{kj}$. So,

$$\begin{aligned}|\psi\rangle &= \sum_{ijk} u_{ik} d_{kk} v_{kj} |i\rangle|j\rangle \\ &= \sum_k d_{kk} \left(\sum_i u_{ik}|i\rangle\right)\left(\sum_j v_{kj}|j\rangle\right) \\ &= \sum_k d_{kk} \underbrace{|v_k\rangle |w_k\rangle}_{\text{ONB}}\end{aligned}$$

$$\begin{aligned}\langle v_k|v_j\rangle &= \sum_i \overline{u_{ik}} u_{ij} \langle k|j\rangle \\ &= \sum_i \overline{u_{ij}} u_{ij} = 1 \text{ as } u \text{ is Unitary}\end{aligned}$$

$\boxtimes$

Example: $\rho_{AB} = |\psi\rangle\langle\psi|_{AB}$ then
$$\left.\begin{aligned}\rho_A &= \sum_k \lambda_k^2 |v_k\rangle\langle v_k| \\ \rho_B &= \sum_k \lambda_k^2 |w_k\rangle\langle w_k|\end{aligned}\right\} \text{same spectrum}$$

Schmidt Rank: - # of nonzero λ_i in schmidt decomposition
- Measure of entanglement for pure states

Exercise: Prove $|\psi\rangle$ is a product state $\iff$ ρ_A, ρ_B are pure.

Purification

Suppose we have a system A in a mixed state $\rho_A = \sum_i p_i |v_i\rangle\langle v_i|$

Can we find a system B and a state $|\psi\rangle_{AB}$ such that

$$\rho_A = \mathrm{Tr}_B [|\psi\rangle\langle\psi|] \; ?$$

Yes $$|\psi\rangle_{AB} = \sum_i \sqrt{p_i}\, |v_i\rangle |w_i\rangle$$

Then $$\rho_A = \sum_i p_i |v_i\rangle\langle v_i|$$

Th^m (Uhlman)

Purifications are unique up to unitary transformations on the purifying system. For two purifications $|\psi\rangle_{AB}$ $|\phi\rangle_{AB}$ $\exists$ a unitary U such that

$$|\psi\rangle_{AB} = (\mathbb{1} \otimes U) |\phi\rangle_{AB} .$$

Def^n (POVM measurement)

POVMs represent a more general class of measurements than projective ones. Typically, we do not associate a post-measurement state to a POVM measurement.

A POVM is a collection of positive operators $\{M_x\}_x$, $M_x \geq 0$. (No longer have to be projective.)

The probability of obtaining outcome x when in the state ρ is

$$\mathbb{P}(x) = \mathrm{Tr}[\rho M_x] .$$

Examples

* $M_0 = \begin{pmatrix} 3/4 & 0 \\ 0 & 1/4 \end{pmatrix}$ $M_1 = \begin{pmatrix} 1/4 & 0 \\ 0 & 3/4 \end{pmatrix}$ (non-projective measurement)
* Mix measurements $\{P_i\}_i$ $\{Q_i\}_i$ define $\{R_i\}$

  $$R_i = \lambda P_i + (1-\lambda) Q_i \qquad \lambda \in [0,1].$$

  valid POVM

  Captures adding classical randomness to the measurement choice.

* Coin flip $\{p\mathbb{1} , (1-p)\mathbb{1}\}$