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

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

Independent systems!

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

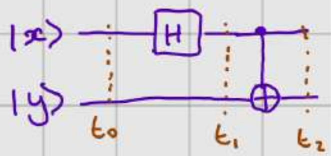
Bell-States

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:



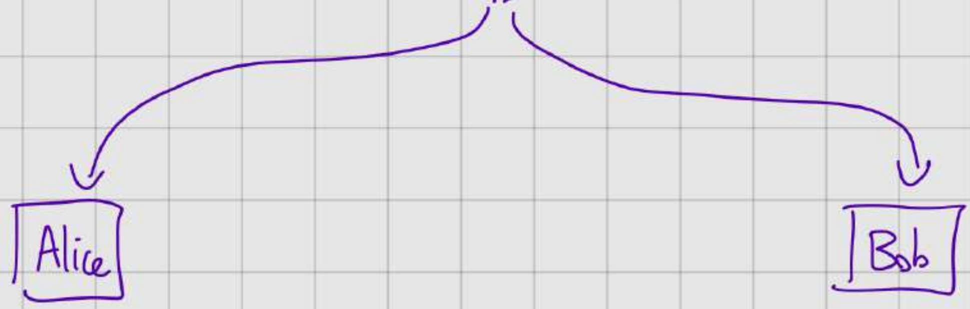
$\longrightarrow |\Phi_{xy}\rangle$

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

The EPR Paradox

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 state after measurement is

$$|11\rangle.$$

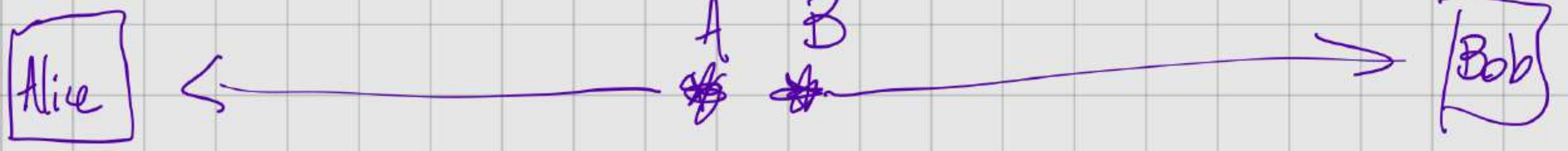
After measurement Alice can predict with <u>certainty</u> what Bob will measure if he measures in Z basis also.

Bob's state somehow 'knows' the outcome of Alice's measurement

This property also holds for all possible measurement choices!
<u>If</u> Alice and Bob both measure in a basis $\{|v_0\rangle, |v_1\rangle\}$ then the will have a distribution

$$\mathbb{P}[A=a, B=b] = \begin{cases} \frac{1}{2} & \text{if } a,b = 0,0 \\ 0 & \text{if } a,b = 0,1 \\ 0 & \text{if } a,b = 1,0 \\ \frac{1}{2} & \text{if } a,b = 1,1 \end{cases}$$

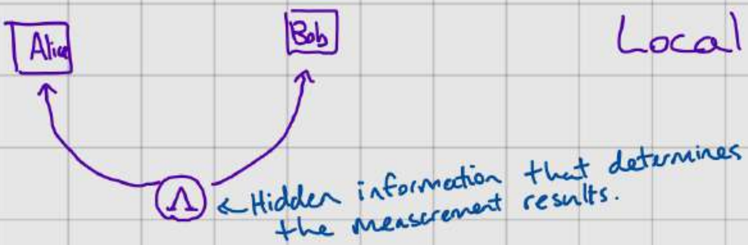
This will work even if Alice and Bob are spacelike/caus
separated.



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.

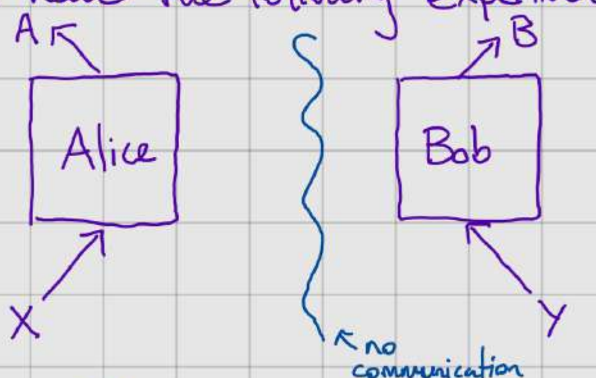
They wanted something like:



Local hidden variable model

The CHSH game

Suppose we have the following experiment



uniformly

1) Alice and Bob receive independent/random binary inputs X, Y

2) They must respond with binary outputs A, B.

3) They win the game if $A \oplus B = X \cdot Y$

X,Y	Winning Answers
(0,0)	(0,0) or (1,1)
(0,1)	(0,0) or (1,1)
(1,0)	(0,0) or (1,1)
(1,1)	(0,1) or (1,0)

A=B if $X,Y \in \{(0,0),(0,1)$ or $(1,0)\}$

otherwise

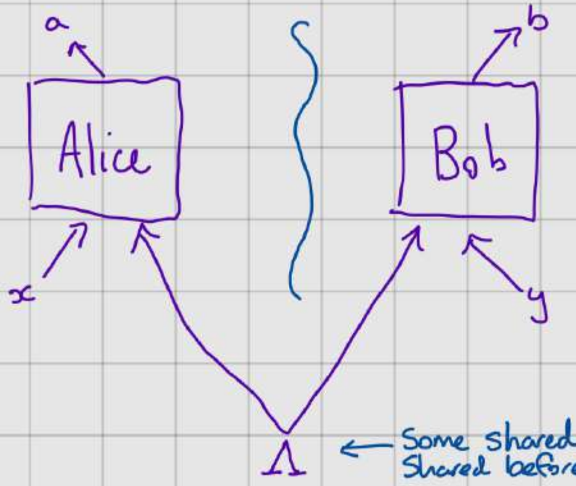
$A \neq B$ if $X,Y = (1,1)$

What's probability Alice & Bob win?

$$P_{win} = \underbrace{\frac{1}{4}}_{p(xy)} \sum_{a \oplus b = xy} p(ab|xy)$$

P_{win} depends on how they react to their inputs.

Local Hidden Variable model



Classical (non-quantum) Strategy

Some shared random variable
Shared before they were separated (before inputs given)

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. $\mathcal{L}$ - set of local distributions

Derivation (Bonus)

We make two assumptions 1) $p(\lambda|xy) = p(\lambda)$ (x,y) chosen independently of everything (including Λ)

2) A is independent of B,Y given Λ
B is independent of X,A given Λ } Causal structure of the problem

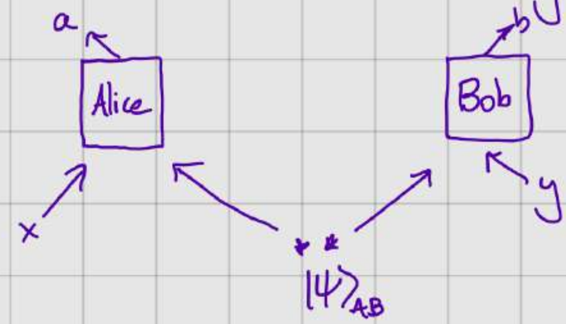
Then

$$p(ab|xy) = \sum_{\lambda} p(ab|xy\lambda)\, p(\lambda|xy) = \sum_{\lambda} p(\lambda)\, p(ab|xy\lambda)$$

$$= \sum_\lambda p(\lambda)\, p(a|bxy\lambda)\, p(b|xy\lambda) \leftarrow p(a|bxy\lambda) = p(a|x\lambda)$$
$$p(b|xy\lambda) = p(b|y\lambda)$$
$$= \sum_\lambda p(\lambda)\, p(a|x\lambda)\, p(b|y\lambda)$$

Quantum Explanation

Instead imagine Alice and Bob share an entangled state $|\psi\rangle_{AB}$



If $X=x$ Alice performs measurement $\{M_{0|x}, M_{1|x}\}$ on her particle.
If $Y=y$ Bob performs measurement $\{N_{0|y}, N_{1|y}\}$ on his particle

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

Let Q be the set of all such distributions.

What is
$$\omega_L = \max_{p\in\mathcal{L}} \frac{1}{4} \sum_{a\oplus b = xy} p(ab|xy)$$
$$\omega_Q = \max_{p\in Q} \frac{1}{4} \sum_{a\oplus b = xy} p(ab|xy)$$
?

(best winning probabilities for classical and quantum strategies)

The best local strategy

Simple: Always output 0

$$p(a|x\lambda) = \begin{cases} 1 & \text{if } a=0 \\ 0 & \text{otherwise} \end{cases}$$

$$p(b|yx) = \begin{cases} 1 & \text{if } b=0 \\ 0 & \end{cases}$$

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

wins with prob 3/4

With a bit more work you can show this is optimal i.e.

$$\omega_L = 3/4.$$

A quantum strategy

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

Alice measures

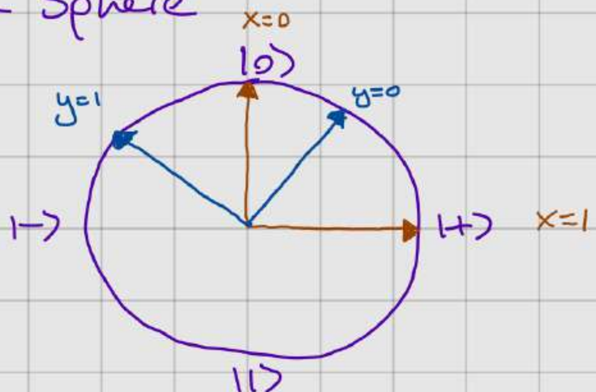
$x=0$	$\{|0\rangle, |1\rangle\}$ basis	Z
$x=1$	$\{|+\rangle, |-\rangle\}$ basis	X

Bob measures

observables

$\frac{X+Z}{\sqrt{2}}$	$y=0$	$\{\cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle,\ \cos(\frac{5\pi}{8})|0\rangle + \sin(\frac{5\pi}{8})|1\rangle\}$
$\frac{X-Z}{\sqrt{2}}$	$y=1$	$\{\cos(-\pi/8)|0\rangle + \sin(-\pi/8)|1\rangle,\ \cos(\frac{3\pi}{8})|0\rangle + \sin(\frac{3\pi}{8})|1\rangle\}$

In the Bloch sphere



One can compute the distribution $p(ab|xy)$ and find

$$p_{win} = \cos(\pi/8)^2 \approx 0.85$$

So this quantum strategy achieves a better winning probability than any classical strategy which is bounded by 3/4.

Remarks

* This rules out the possibility of a local hidden variable model of quantum theory (like EPR) wanted.
  We say quantum theory is <u>nonlocal</u> and the above is called a <u>nonlocal game</u>.

Remark (Tsirelson Bound)

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

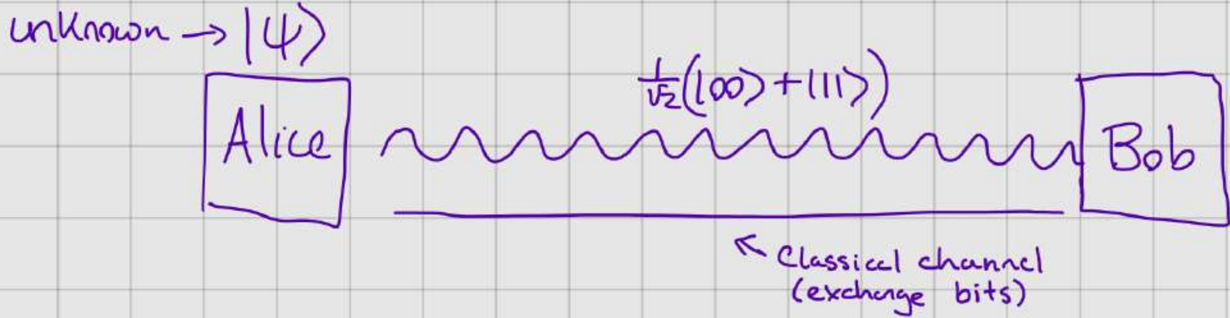
Loopholes

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.

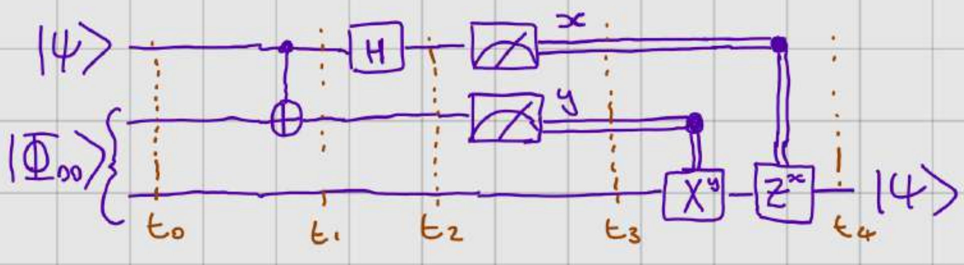


* Share a state $|\Phi_{00}\rangle$
* Can communicate classically

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

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

Time t_1

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

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

Time t_2

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

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

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

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

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

Time t_3

Alice measures first two qubits.

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

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? $\rightarrow$ Classical communication required
- Why does this not violate No cloning? $\rightarrow$ Not copied - original state destroyed in the process

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 $|\Phi_{00}\rangle_{AB_1} \otimes |\Phi_{00}\rangle_{B_2C}$

Alice and Charlie's particles have <u>never</u> 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
$\{|\Phi_{ij}\rangle\}_{ij}$ ← entangled measurement

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

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	$\frac{1}{\sqrt{2}}\left(|0\rangle|\Phi_{11}\rangle|1\rangle - |1\rangle|\Phi_{11}\rangle|0\rangle\right)$

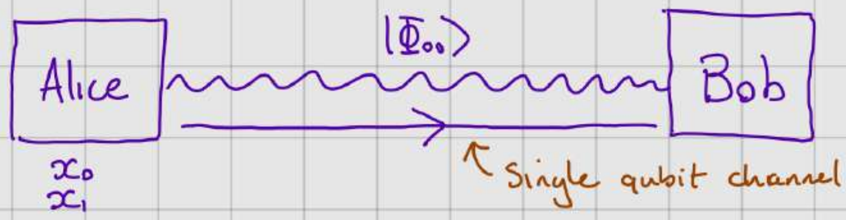
Can also view this as a teleportation protocol Bob teleports 1 of his qubits through the other entangled pair to one of the parties.

* 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
$\implies$ 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

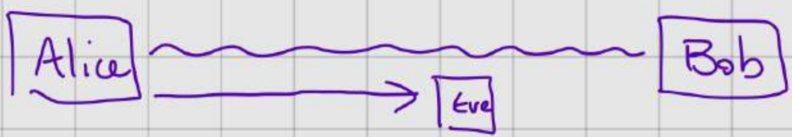
Let $\{P, \mathbb{1}-P\}$ be a qubit projective measurement. Then
(not $\{\mathbb{1}, 0\}$)

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

<u>Proof</u>. Exercise...

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

* Locally a source of randomness
* Local information provides <u>no</u> 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 different parties?

Example Alice, Bob and charlie are each given a 2 bit input

Alice $a_0 a_1$ Bob $b_0 b_1$

They are promised that $a_0 \oplus b_0 \oplus c_0 = 0$

Charlie $c_0 c_1$

How much information do they need to communicate to compute

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

$x \vee y = \begin{cases} 0 & \text{if } 0,0 \\ 1 & \text{otherwise} \end{cases}$

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

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

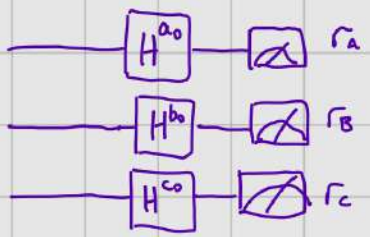
* 4 bits necessary is more involved (see Buhrman et al. Quantum entanglement and communication complexity 2001)

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 $\begin{matrix} a_1 \oplus r_A \\ b_1 \oplus r_B \\ c_1 \oplus r_C \end{matrix}$

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	$\frac{1}{4}$
011	$\frac{1}{4}$
101	$\frac{1}{4}$
110	$\frac{1}{4}$

$r_A \oplus r_B \oplus r_C = 0$ ✓

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	$\frac{1}{4}$
100	$\frac{1}{4}$
001	$\frac{1}{4}$
111	$\frac{1}{4}$

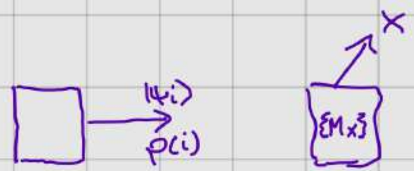
$r_A \oplus r_B \oplus r_C = 1$ ✓

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

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



A source produces $|\psi_i\rangle$ with probability $p(i)$ what's the probability we get outcome x when we perform measurement $\{M_x\}_x$?

$$\mathbb{P}[X=x] = \sum_i \mathbb{P}[X=x \mid \text{State was } |\psi_i\rangle]\, \mathbb{P}[\text{State was } |\psi_i\rangle]$$

$$= \sum_i \langle\psi_i| M_x |\psi_i\rangle\, p(i)$$

$$= \sum_i \langle\psi_i| \underbrace{\Big(\sum_j |j\rangle\langle j|\Big)}_{=\mathbb{1}} M_x |\psi_i\rangle\, p(i)$$

$$= \sum_{ij} \underbrace{\langle\psi_i|j\rangle}_{\in\mathbb{C}} \underbrace{\langle j| M_x |\psi_i\rangle}_{\in\mathbb{C}}\, p(i)$$

$$= \sum_{ij} \langle j| M_x |\psi_i\rangle\langle\psi_i| j\rangle\, p(i)$$

$$= \sum_j \langle j| M_x \underbrace{\Big(\sum_i p(i) |\psi_i\rangle\langle\psi_i|\Big)}_{\rho} |j\rangle \qquad \text{(linearity of matrix multiplication)}$$

$$= \sum_j \langle j| M_x \rho |j\rangle = \mathrm{Tr}[M_x \rho] \qquad \Big(\mathrm{Tr}[Y] := \sum_i \langle i|Y|i\rangle\Big)$$

Given an ensemble $\{p(i), |\psi_i\rangle\}$ we have introduced a new matrix

$$\rho = \sum_i p(i) |\psi_i\rangle\langle\psi_i|$$

It is a convenient way of dealing with such sources and the probability we receive outcome x when measuring $\{M_x\}_x$ has a particularly simple form

$$\mathbb{P}[X=x] = \mathrm{Tr}[M_x \rho]$$

Quick recap of trace

For a square matrix X the trace of X is defined as

$$\mathrm{Tr}[X] := \sum_i \langle i | X | i \rangle = \sum_i X_{ii}$$

Standard basis

diagonal elements

It satisfies numerous properties:

1) Cyclicity: $\mathrm{Tr}[XY] = \mathrm{Tr}[YX]$

2) Linearity: $\mathrm{Tr}[\alpha X + \beta Y] = \alpha \mathrm{Tr}[X] + \beta \mathrm{Tr}[Y]$ $\quad \alpha, \beta \in \mathbb{C}$

3) Tensor Product: $\mathrm{Tr}[X \otimes Y] = \mathrm{Tr}[X]\mathrm{Tr}[Y]$

4) Inner Product: For the vector space of $m \times n$ matrices with entries in $\mathbb{C}$ (i.e. $\mathbb{C}^{m \times n}$) we have an inner product $\langle X, Y \rangle = \mathrm{Tr}[X^\dagger Y]$.

Usual inner product with columns of matrix stacked on top of each other.

We call such a matrix ρ a <u>density matrix</u> and they have 2 defining properties:

1) Unit trace: $\quad \mathrm{Tr}[\rho] = 1$
2) Positive semidefinite: $\quad \rho = \rho^\dagger$ and $\langle x|\rho|x\rangle \geq 0 \;\; \forall |x\rangle \in \mathcal{H}$.

By the spectral theorem we have $\rho = \sum_i \lambda_i |v_i\rangle\langle v_i|$ for some orthonormal basis $\{|v_i\rangle\}$. Property (2) implies $\lambda_i \geq 0$ and property (1) implies $\sum_i \lambda_i = 1$. I.e. $\{\lambda_i\}_i$ form a probability distribution and $\{|v_i\rangle\}_i$ are quantum states so any matrix satisfying (1) and (2) describes a probabilistic state preparation. We arrive at a new (more general) postulate for states.

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

Let A be a quantum system with associated Hilbert space $\mathcal{H}_A$. Then the possible states of the system are described by density matrices acting on $\mathcal{H}_A$. I.e. Hermitian matrices ρ acting on $\mathcal{H}_A$ and satisfying

1) $\mathrm{Tr}[\rho] = 1$
2) $\langle x|\rho|x\rangle \geq 0 \quad \forall |x\rangle \in \mathcal{H}_A$.

<u>Examples</u>

1) If the state of the system is $|\psi\rangle$ then the associated density matrix is

$$\rho = |\psi\rangle\langle\psi|.$$

otherwise we say

This matrix has rank 1 and we call it a <u>pure state</u>.

2) $$\rho = \tfrac{1}{2}|0\rangle\langle 0| + \tfrac{1}{2}|1\rangle\langle 1| = \mathbb{1}/2 = \begin{pmatrix} \tfrac{1}{2} & 0 \\ 0 & \tfrac{1}{2} \end{pmatrix}$$

This results from preparing $|0\rangle$ with prob $\tfrac{1}{2}$ and $|1\rangle$ with prob $\tfrac{1}{2}$ (Maximally mixed state - least amount of knowledge about system).

3) $$\rho = \tfrac{3}{4}|0\rangle\langle 0| + \tfrac{1}{4}|+\rangle\langle +| = \begin{pmatrix} 7/8 & \tfrac{1}{8} \\ 1/8 & \tfrac{1}{8} \end{pmatrix}$$

4) If $|\psi\rangle = e^{i\theta}|\phi\rangle$ (Global phase difference)
then
$$|\psi\rangle\langle\psi| = e^{i\theta}|\phi\rangle\langle\phi|e^{-i\theta} = |\phi\rangle\langle\phi|$$
Same density matrices!

The Bloch ball

A qubit state can in general be written as

$$\rho = \begin{pmatrix} a & \beta \\ \bar{\beta} & 1-a \end{pmatrix}$$

$a \in [0,1]$
$\beta \in \mathbb{C}$ $|\beta| \leq \sqrt{a(1-a)}$

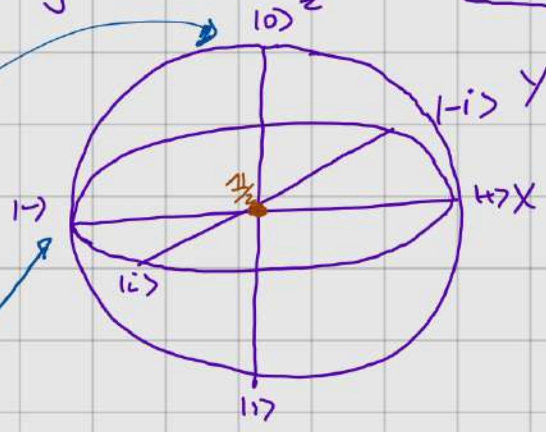
It is also possible to write this as

$$\rho = \frac{\mathbb{1} + r_x X + r_y Y + r_z Z}{2}$$

with X, Y, Z the Pauli matrices.

Condition of ρ being a state becomes $\boxed{r_x^2 + r_y^2 + r_z^2 = 1}$

Equation of a Ball



(r_x, r_y, r_z) Cartesian coordinates

Example
$$(0,0,1) \mapsto \rho = \frac{\mathbb{1}+Z}{2} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = |0\rangle\langle 0|$$
$$(-1,0,0) \mapsto \rho = \frac{\mathbb{1}-X}{2} = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} = |-\rangle\langle -|$$
$$(0,0,0) \mapsto \rho = \mathbb{1}/2 = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$$

Closer to centre the more noisy/mixed the state is.

$$r_x^2 + r_y^2 + r_z^2 = 1 \iff \text{Pure state } \rho = |\psi\rangle\langle\psi| \text{ for some } |\psi\rangle.$$

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

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

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

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

Can create the state without systems interacting quantumly.

Otherwise we say ρ is entangled.

A small problem

Given two random variables X, Y and their joint distribution $\mathbb{P}[X=x, Y=y]$ how do we compute the distribution $\mathbb{P}[X=x]$?

Like state of 2 particles

Ans: We marginalise $\mathbb{P}[X=x] = \sum_y \mathbb{P}[X=x, Y=y]$ ← Want to recover 1 particle state.

Forgetting information about Y

We can ask the analogous question for quantum systems

Suppose we have a bipartite system AB in a state $|\psi\rangle_{AB}$ what is the state of system A?

If $|\psi\rangle_{AB} = |w\rangle_A \otimes |v\rangle_B$ then easy (just $|w\rangle_A$)

If $|\psi\rangle_{AB} = \sum_{ij} \alpha_{ij} |i\rangle|j\rangle$ is entangled then it is less clear.

Suppose B measures in $\{|j\rangle\}$ basis, with probability $p(j) = \sum_i |\alpha_{ij}|^2$ they recieve outcome j and the state becomes

$$\frac{\sum_i \alpha_{ij} |i\rangle |j\rangle}{\sum_i |\alpha_{ij}|^2} \leftarrow \text{no longer entangled}$$

so state on A upon outcome j is

$$|\phi_j\rangle_A = \frac{\sum_i \alpha_{ij} |i\rangle}{\sum_i |\alpha_{ij}|^2}$$

Forgetting outcome of measurement

If we think about this as a probabilistic preparation of system A we should have

$$\rho_A = \sum_j p(j) |\phi_j\rangle\langle\phi_j| = \sum_{ik} \alpha_{ij} \overline{\alpha_{kj}} |i\rangle\langle k|$$

This form is invariant under choice of measurement basis.

We can express this procedure more comprehensively using partial trace.

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 B as

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

where $\{|i\rangle\}_i$ is <u>any</u> 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

$$Tr_B[M] = \sum_{ijkl} m_{ijkl} \, |i\rangle\langle j| \cdot \underbrace{Tr[|k\rangle\langle l|]}_{\delta_{kl} = \begin{cases} 1 & \text{if } k=l \\ 0 & \text{otherwise} \end{cases}}$$

Partial trace (Properties)

* (Linear)
* (Partially Cyclic)
  $$Tr_A[(M_1 \otimes \mathbb{1}) X (M_2 \otimes \mathbb{1})] = Tr_A[(M_2 M_1 \otimes \mathbb{1}) X]$$
* $Tr[X] = Tr_A[Tr_B[X]] = Tr_B[Tr_A(X)]$
* $Tr_A[(\mathbb{1} \otimes X) Z (\mathbb{1} \otimes Y)] = X \, Tr_A(Z) \, Y$

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! $\rho_A = Tr_B[\rho]$ $\qquad \rho_B = Tr_A[\rho]$

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

Examples

1) Suppose $|\psi\rangle_{AB} = |v\rangle_A \otimes |w\rangle_B$

then $\rho_{AB} = |\psi\rangle\langle\psi| = |v\rangle\langle v| \otimes |w\rangle\langle w|$

$$\rho_A = \mathrm{Tr}_B[\rho_{AB}] = |v\rangle\langle v| \cdot \mathrm{Tr}[|\omega\rangle\langle\omega|]$$
$$= |v\rangle\langle v| \qquad \text{(as expected)}$$

$$\rho_B = |\omega\rangle\langle\omega| \qquad \text{(as expected)}$$

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

$$\rho_{AB} = |\psi\rangle\langle\psi| = \frac{|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|}{2}$$

$$\rho_A = \mathrm{Tr}_B[\rho_{AB}] = \sum_i (\mathbb{1} \otimes \langle i|)\, |\psi\rangle\langle\psi|\, (\mathbb{1} \otimes |i\rangle)$$
$$= \tfrac{1}{2}|0\rangle\langle 0| + \tfrac{1}{2}|1\rangle\langle 1| = \mathbb{1}/2$$

local state of knowledge is full noise.

Agrees with earlier lemma that $\langle\Phi_{ij}|(P\otimes\mathbb{1})|\Phi_{ij}\rangle = \frac{1}{2}$

3) We can now embed probability theory into quantum theory. For a distribution $p(x)$ we define a corresponding density matrix that is diagonal

$$\rho_X = \sum_x p(x)\,|x\rangle\langle x| = \begin{pmatrix} p(0) & & & 0 \\ & p(1) & & \\ & & p(2) & \\ 0 & & & \ddots \end{pmatrix}$$

If we have a joint distribution $p(x,y)$ then we define it analogously (one system for each random variable)

$$\rho_{XY} = \sum_{xy} p(x,y)\,|x\rangle\langle x| \otimes |y\rangle\langle y| = \begin{pmatrix} p(0,0) & & & & & 0 \\ & p(0,1) & & & & \\ & & p(0,2) & & & \\ & & & \ddots & & \\ & & & & p(1,0) & \\ & & 0 & & & \ddots \\ & & & & & p(n,m) \end{pmatrix}$$

Now partial trace over X we get

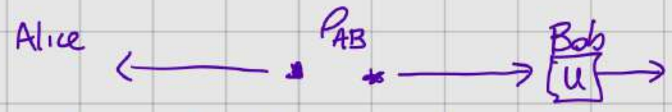
$$\rho_Y = \mathrm{Tr}_X[\rho_{XY}] = \sum_{xy} p(x,y)\, \mathrm{Tr}[|x\rangle\langle x|]\, |y\rangle\langle y|$$
$$= \sum_{xy} p(x,y)\, |y\rangle\langle y|$$
$$= \sum_y \Big(\sum_x p(x,y)\Big) |y\rangle\langle y|$$
$$= \sum_y \mathbb{P}[Y=y]\, |y\rangle\langle y|$$

Exactly the marginal distribution

Quantum theory generalizes probability theory. Embed information theory into quantum theory.

Partial trace properties are consistent with what we expect operationally.

* Local transformations



If Bob performs a local transformation it should <u>not</u> affect the state of Alice's system $\rho_A = \mathrm{Tr}_B(\rho_{AB}]$

$$\rho_{AB} \longmapsto (\mathbb{1}\otimes U)\rho_{AB}(\mathbb{1}\otimes U^{\dagger})$$

$$\rho_A^{U} = \mathrm{Tr}_B[(\mathbb{1}\otimes U)\rho_{AB}(\mathbb{1}\otimes U^{\dagger})] \overset{\text{partial cyclicity}}{=} \mathrm{Tr}_B[(\mathbb{1}\otimes U^{\dagger}U)\rho_{AB}]$$

$$= \mathrm{Tr}_B[\rho_{AB}] = \underset{\text{Unchanged}}{\rho_A}$$

* Local measurements: If Alice measures system A with $\{M_x\}$

We have $\mathrm{Tr}[M_x\,\rho_A] = \mathrm{Tr}((M_x\otimes\mathbb{1}_B)(\rho_{AB})]$