Monogamy of Entanglement

For classical correlations, we can have

$$I(A;B_1)=1 \quad I(A;B_2)=1, \quad I(A;B_3)=1, \dots, \quad I(A;B_N)=1$$

While $I(A;B_1B_2B_3\dots B_N)=1$ so

$$I(A;B_1)+I(A;B_2)+\dots \gg I(A;B_1B_2B_3\dots B_N)$$

So the correlation that A has with B1, it can also have with B2, and arbitrarily many other systems

For entanglement, this is not the case. Given a suitable entanglement measure $\mathcal{E}$

$$\mathcal{E}(\rho_{A,B_1})+\mathcal{E}(\rho_{A,B_2})+\mathcal{E}(\rho_{A,B_3})+\cdots \leq \mathcal{E}(\rho_{A,B_1\dots B_N})$$

If A is maximally entangled with B1, it cannot be entangled with anything else

IF $\rho_{AB_1}=|\phi^+\rangle\langle\phi^+|$ THEN $\rho_{AB_1B_2\dots}=|\phi^+\rangle\langle\phi^+|\otimes\rho_{B_1B_2\dots}$ $\therefore$ $\mathcal{E}(\rho_{AB_2B_3\dots})=\mathcal{E}(\rho_{B_1B_2B_3\dots})=0$

$\mathcal{E}(\rho_{AB})=1$

Creating Entanglement

LOCC cannot create entanglement, but what can?
Two types of non-local operation

1) Entangling Measurements: Measure in entangled basis

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \qquad |\psi^+\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right) \qquad |\psi^-\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$$

For initial product state

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

The measurment results in

$$\left.\begin{array}{ll} |\phi^+\rangle & \text{with prob. } \frac{1}{2} \\ |\phi^-\rangle & \text{with prob. } \frac{1}{2} \end{array}\right\} \text{ENTANGLED}$$

2) Entangling unitary

Prime example: controlled operations

$$U = \sum_i |\alpha_i\rangle\langle\alpha_i| \otimes U_i \qquad \langle\alpha_i|\alpha_j\rangle = 0$$

This applies an operation U_i to system B that depends on the state $|\alpha_i\rangle$ of system A

Examples:

CNOT $\quad \Lambda^x = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes \sigma_x$

$$\Lambda^x |+0\rangle = \Lambda^x \frac{1}{\sqrt{2}}\left(|00\rangle + |10\rangle\right) = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) = |\phi^+\rangle$$

CPHASE $\quad \Lambda^z = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes \sigma_z$

$$\Lambda^z |++\rangle = \Lambda^z \frac{1}{\sqrt{2}}\left(|0+\rangle + |1+\rangle\right) = \frac{1}{\sqrt{2}}\left(|0+\rangle + |1-\rangle\right) = \mathbb{1} \otimes H |\phi^+\rangle$$

$$\text{Hadamard} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

What kinds of interactions do these require? For the CPHASE

$$\Lambda^z = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes \sigma_z$$

Use $|0\rangle\langle 0| = \frac{1}{2}(\mathbb{1} + \sigma_z)$ $|1\rangle\langle 1| = \frac{1}{2}(\mathbb{1} - \sigma_z)$

$$\Lambda^z = \frac{1}{2}\left(\mathbb{1}\otimes\mathbb{1} + \sigma_z\otimes\mathbb{1} + \mathbb{1}\otimes\sigma_z - \sigma_z\otimes\sigma_z\right)$$

If $U^2 = \mathbb{1}$ note that $U = U^\dagger$ and so is a valid Hamiltonian

Since eigenvalues are ±1 $e^{iUt} = \mathbb{1}\cos(t) + iU\sin(t)$

$$\therefore e^{iU\pi/2} = iU \quad \therefore e^{i(U-\mathbb{1})\pi/2} = U$$

Since $\left(\Lambda^z\right)^2 = \mathbb{1}$

$$iU_{CPHASE} = e^{iH\pi/2}, \qquad H = \frac{1}{2}\left(\mathbb{1}\otimes\mathbb{1} + \sigma_z\otimes\mathbb{1} + \mathbb{1}\otimes\sigma_z - \sigma_z\otimes\sigma_z\right)$$

So 2-body z-z interactions and a z field can be used

The z-z interactions on their own can also entangle

$$H = \sigma_z \otimes \sigma_z = \begin{pmatrix} 1 &&& \\ & -1 && \\ && -1 & \\ &&& 1 \end{pmatrix}$$

The unitary $\sigma_z \otimes \sigma_z$ is not entangling, but

$$\therefore U(t) = e^{-iHt} = \begin{pmatrix} e^{-it} &&& \\ & e^{it} && \\ && e^{it} & \\ &&& e^{-it} \end{pmatrix} \quad \therefore U\left(\frac{\pi}{4}\right) = \begin{pmatrix} \sqrt{-i} &&& \\ & i\sqrt{-i} && \\ && i\sqrt{-i} & \\ &&& \sqrt{-i} \end{pmatrix} = \sqrt{-i} \begin{pmatrix} 1 &&& \\ & i && \\ && i & \\ &&& 1 \end{pmatrix}$$

$$|\psi\rangle = U\left(\frac{\pi}{4}\right)|++\rangle = \begin{pmatrix} 1 &&& \\ & i && \\ && i & \\ &&& 1 \end{pmatrix} \times \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 \\ i \\ i \\ 1 \end{pmatrix} = \frac{1}{2}\Big(|00\rangle + i|01\rangle + i|10\rangle + |11\rangle\Big)$$

$$\begin{aligned} |\psi\rangle\langle\psi| = \frac{1}{4}\Big(& |00\rangle\langle 00| \cancel{- i|00\rangle\langle 01|} - i|00\rangle\langle 10| \cancel{+ |00\rangle\langle 11|} \\ & \cancel{+ i|01\rangle\langle 00|} + |01\rangle\langle 01| \cancel{+ |01\rangle\langle 10|} + i|01\rangle\langle 11| \\ & + i|10\rangle\langle 00| \cancel{+ |10\rangle\langle 01|} + |10\rangle\langle 10| \cancel{+ i|10\rangle\langle 11|} \\ & \cancel{+ |11\rangle\langle 00|} - i|11\rangle\langle 01| \cancel{+ |11\rangle\langle 10|} + |11\rangle\langle 11|\Big) \end{aligned}$$

$$\begin{aligned} \therefore \rho_A = tr_B(|\psi\rangle\langle\psi|) = \frac{1}{4}\Big(& |0\rangle\langle 0| \cancel{- i|0\rangle\langle 1|} \\ & + |0\rangle\langle 0| \cancel{+ i|0\rangle\langle 1|} \\ & \cancel{+ i|1\rangle\langle 0|} + |1\rangle\langle 1| \\ & \cancel{- i|1\rangle\langle 0|} + |1\rangle\langle 1| \Big) \\ = \mathbb{1} \end{aligned}$$

Maximally Entangled

State Purification

Schmidt decomposition implies a way to represent n dimensional mixed states as n^2 dimensional pure states

Useful because pure states can be easier than mixed.

Schmidt decomposition:

$$|\psi\rangle = \sum_{i=1}^{n}\sum_{j=1}^{m} c_{ij}\,|\alpha_i\,\beta_j\rangle \qquad\qquad |\psi\rangle = \sum_{i=1}^{n} \sqrt{p_i}\,|a_i\,\tilde{a}_i\rangle$$

$$\hookrightarrow \rho_A = \sum_i p_i\,|a_i\rangle\langle a_i|\,,\quad \rho_B = \sum_i p_i\,|\tilde{a}_i\rangle\langle\tilde{a}_i| \hookleftarrow$$

So given a mixed state $\rho_A = \sum_{i=1}^{n} p_i\,|a_i\rangle\langle a_i|$

We can invent a ficticious system with which we suppose it is entangled, and give that a consistent mixed state. The dimension must be at least n, and we can choose the basis states to suit us $\rho_B = \sum_{i=1}^{n} p_i\,|i\rangle\langle i|$

We can then construct the entangled state for which ρ_A is the partial density matrix $|\psi_{AB}\rangle = \sum_{i=1}^{n} \sqrt{p_i}\,|\alpha_i\; i\rangle$

No cloning theorem

If we have a qubit (or any other system) in a known state $|\psi\rangle$ we can copy it simply by preparing another qubit in the same state (same for classical copying)

But what if we don't know the state?

If we know that it belongs to a certain set of orthogonal states $\langle\sigma_j|\sigma_k\rangle = \delta_{jk}$ then we can copy it by one of two possible methods

Method 1: Measure with basis $\{P_j = |\sigma_j\rangle\langle\sigma_j|\}$ to determine which state the system is in, then copy as above

Method 2: Apply an appropriate unitary to copy the state to a 'blank' qubit (one prepared in a known state)

$$U(|\sigma_j\rangle\otimes|0\rangle) = |\sigma_j\rangle\otimes|\sigma_j\rangle \qquad U = \sum_j |\sigma_j\sigma_j\rangle\langle\sigma_j 0| + \dots$$

terms that act on states with second qubit in state $|1\rangle$, required for unitarity but not otherwise specified

This method is required if the copy needs to be reversed at some later time (not possible for method 1)

What if the state is completely unknown? We do not even know a basis in which it belongs?

Can we still define a copying unitary as before? Which will work on any arbitrary pure state?

$$U\big(|\psi\rangle\otimes|0\rangle\big)=|\psi\rangle\otimes|\psi\rangle \qquad \forall\,|\psi\rangle$$

Consider a unitary that can copy both the states $|\psi\rangle$ and $|\varphi\rangle$

$$U\big(|\psi\rangle\otimes|0\rangle\big)=|\psi\rangle\otimes|\psi\rangle \qquad\qquad U\big(|\varphi\rangle\otimes|0\rangle\big)=|\varphi\rangle\otimes|\varphi\rangle$$

Now consider the following inner products

$$\big(\langle\psi|\otimes\langle 0|\big)\big(|\varphi\rangle\otimes|0\rangle\big)=\langle\psi|\varphi\rangle \quad , \quad \big(\langle\psi|\otimes\langle\psi|\big)\big(|\varphi\rangle\otimes|\varphi\rangle\big)=\langle\psi|\varphi\rangle^2$$

Assuming that U exists and using the property $U^\dagger U=\mathbb{1}$

$$\big(\langle\psi|\otimes\langle 0|\big)\big(|\varphi\rangle\otimes|0\rangle\big)=\big(\langle\psi|\otimes\langle 0|\big)U^\dagger U\big(|\varphi\rangle\otimes|0\rangle\big)=\big(\langle\psi|\otimes\langle\psi|\big)\big(|\varphi\rangle\otimes|\varphi\rangle\big)$$

$$\therefore\ \langle\psi|\varphi\rangle=\langle\psi|\varphi\rangle^2 \qquad \therefore\ \langle\psi|\varphi\rangle=0 \text{ or } 1$$

So it only works when the states are part of the same orthonormal basis. There is no way to copy an arbitrary unknown state: No cloning theorem

Conditional Entropy

Classically we can define the conditional entropy

$$H(X|Y) = \underbrace{\sum_y p(x) \Big(\underbrace{- \sum_x p(x|y) \log p(x|y)}_{\text{entropy of } X \text{ after } Y \text{ is measured as } y} \Big)}_{\text{averaged over all } y} = H(XY) - H(Y)$$

With this we can define the MI in a different (but equivalent) way

$$I(X;Y) = H(X) - H(X|Y)$$

The MI is the information in X that is not left unknown once Y is measured

No clear quantum definition of CI, since there is not a unique measurement basis

Maybe we can just replace Shannon with Von Neumann in the end result?

$$S(A|B) = S(\rho_{AB}) - S(\rho_B)$$

Let's try applying this to a Bell basis state

$\rho_A = \rho_B = \frac{1}{2}\mathbb{1}$ $\therefore$ $S(\rho_A) = S(\rho_B) = 1$ but $S(\rho_{AB}) = 0$ So $S(A|B) = -1$!

Doesn't seem to make sense, but actually it does

This is the most widely used definition of quantum conditional entropy

State Merging

Alice, Bob and Charlie share a 3 qubit state $|\psi\rangle_{ABC}$

They share no other quantum correlations

They can communicate classically

They can also send qubits to each other using a 'quantum channel'. But this costs, so they use it as little as possible

Alice wants to send her share of the state to Bob

How many times does she need to use the quantum channel to do this?

Example 1: $|\psi\rangle_{ABC} = |\phi^+\rangle_{AC} \otimes |0\rangle_B$ $S(A|B) = 1$

Bob and Charlie initially unentangled, but maximally entangled at the end

Can't be done by LOCC alone. Alice must use the channel to send her qubit: 1 use needed

Example 2: $|\psi\rangle_{ABC} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ $S(A|B) = 0$

Note that, for this state

$$|\psi_{ABC}\rangle = \frac{1}{2}\left(|{+}00\rangle + |{-}00\rangle + |{+}11\rangle - |{-}11\rangle\right) = \frac{1}{\sqrt{2}}\left(|+\rangle_A \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{BC} + |-\rangle_A \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{BC}\right)$$

If Alice measures in the X basis, B and C's state will be projected to $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{BC}$ or $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{BC}$

If she gets $|-\rangle$ she tell tell Bob to apply σ^z, then B and C's state will be $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{BC}$

Bob can then take a blank qubit $|0\rangle_B \otimes \frac{1}{\sqrt{2}}(|00\rangle_{BC} + |11\rangle_{BC})$

And entangle it to his other qubit with a CNOT

U_{CNOT}: $|00\rangle \to |00\rangle$ $\therefore$ $|0\rangle_B \otimes \frac{1}{\sqrt{2}}(|00\rangle_{BC} + |11\rangle_{BC}) \longrightarrow \frac{1}{\sqrt{2}}(|00\rangle_B \otimes |0\rangle_C + |11\rangle_B \otimes |1\rangle_C) = |\psi\rangle_{BBC}$

$|01\rangle \to |11\rangle$

...

Now Bob has Alice's share and Alice does not

Zero uses of quantum channel needed!

Example 3: $|\psi\rangle_{ABC} = |\phi^+\rangle_{AB} \otimes |0\rangle_C$ $S(A|B) = -1$

Alice and Bob share a known state, unentangled with Charlie

End result is for Bob to have a Bell pair of his own

He can just make one, Alice needn't do anything!

She doesn't even need to destroy her half of the Bell pair

This can be used in future to teleport a qubit to Bob, without needing to use the quantum channel

So she uses the channel -1 times!

In general, for N copies of $|\psi\rangle_{ABC}$:

If $S(A|B) > 0$, $-S(A|B)N$ QUBITS MUST BE SENT

If $S(A|B) < 0$, - NO QUBITS NEED TO BE SENT

- REMAINING ENTANGLEMENT CAN BE TURNED INTO $S(A|B)N$ BELL PAIRS $\therefore$ $S(A|B)N$ QUBITS CAN BE SENT WITHOUT THE CHANNEL

Anonymous Broadcast

Suppose there are N people, one of whom wishes to send a bit to the rest

The sender wishes to be anonymous, and the receivers are happy to respect that anonymity

One way to achieve this: they sit around a table and flip a coin with each of their neighbours

Each receiver then broadcasts the sum (mod 2) of the flips to the rest: $f_{j,j-1} + f_{j,j+1} \mod 2$

results of flip with neighbour to the:

left ($f_{j,j-1}$)	right ($f_{j,j+1}$)	bit value to broadcast
heads (0)	heads (0)	0
heads (0)	tails (1)	1
tails (1)	heads (0)	1
tails (1)	tails (1)	0

The sender also adds the bit value in: $f_{j,j-1} + f_{j,j+1} + b \mod 2$

Everyone then adds up all the broadcast bits (mod 2)

$$\left(f_{s,s-1} + f_{s,s+1} + b \mod 2\right) + \sum_{j \neq s} \left(f_{j,j-1} + f_{j,j+1} \mod 2\right) = b + \sum_{j} f_{j,j-1} + f_{j,j+1} \mod 2$$

Note that each flip appears twice (it's a round table) and

$$f + f \mod 2 = 0 \qquad \therefore \sum_{j} f_{j,j-1} + f_{j,j+1} \mod 2 = 0$$

So the sum of all broadcast bits is b

The bit has been sent without revealing the sender!

Another method: Get a trusted referee to prepare a set of N bits $\{B_j\}$, one for each player, whose values are completely random except that $\sum_j B_j \mod 2 = 0$

All then broadcast their bit value, except the sender who broadcasts $B_j + b \mod 2$

Again, all broadcast bits add up to b. The message is revealed without identifying the sender

All such classical protocols have a flaw. By comparing the data given to the sender to the bit they broadcast, their identity can be determined

This requires stealing their stuff, or compromising trusted people. Hard, but not impossible

With shared entanglement, we can make it impossible(r)

Consider the states

$$|GHZ^+\rangle = \frac{1}{\sqrt{2}}\left(|+\rangle^{\otimes N} + |-\rangle^{\otimes N}\right) \qquad |GHZ^-\rangle = \frac{1}{\sqrt{2}}\left(|+\rangle^{\otimes N} - |-\rangle^{\otimes N}\right)$$

These are orthogonal

$$\langle GHZ^+|GHZ^-\rangle = \frac{1}{2}\left(\langle +|+\rangle^N - \langle +|-\rangle^N + \langle -|+\rangle^N - \langle -|-\rangle^N\right) = 0$$

And distingishable by LOCC

$$|GHZ^+\rangle = \frac{1}{2^{N-1}}\sum_{b\in E}|b\rangle \qquad |GHZ\ \rangle = \frac{1}{2^{N-1}}\sum_{b\in O}|b\rangle$$

where E = Set of all N bit strings with even # of 1's

O = " odd "

measure in Z basis on each qubit.

$\therefore$ Add up results mod 2

$0 \Rightarrow |GHZ^+\rangle$, $1 \Rightarrow |GHZ^-\rangle$

When shared between N participants, it is possible for any one of them to rotate between the two states

$$\sigma_x^j |GHZ^+\rangle = |GHZ^-\rangle \quad \sigma_x^j |GHZ^-\rangle = |GHZ^+\rangle \quad \forall j$$

No trace of who did it is left

$$\sigma_x^j |GHZ^+\rangle = \sigma_x^k |GHZ^+\rangle = |GHZ^-\rangle \quad \forall jk$$

We can then start by sharing $|GHZ^+\rangle$ between N players

The sender does nothing to send b=0 and applies a σ_x to send b=1

Everyone then measures in the Z basis to determine whether the state was $|GHZ^+\rangle$ or $|GHZ^-\rangle$, and so determine b

No incriminating resources left to steal! Broadcast is completely traceless

Entanglement replaces the need for a trusted referee in for the second classical method