Module II, Part 2

Entropy, information and entanglement

PH 534 QIC

Himadri Shekhar Dhar
himadri.dhar@iitb.ac.in

B. Entanglement, majorization and Nielsen’s theorem

In this section we begin by briefly discussing the origin story of entanglement (and quantum correlations in general) before going on to ask the more fundamental question about what is entanglement. We then try to come up with a more operational approach to define the all-conquering physical entity in quantum physics.

i) Background

The first instance of confrontation with the classical viewpoint of physics, was raised by Einstein, Podolsky and Rosen (EPR), who were troubled by the violation of the conjunction of “objective reality” and “locality” in the quantum description of a physical system with spatially separated subsystems, as mentioned in their seminal paper of 1935[1]. The main contention was the presence of weird and spooky quantum correlations, and in general they proposed that quantum mechanics was incomplete.

Schrödinger often discussed the weirdness of quantum theory and quantum correlations in general with a very philosophical tone. In different texts, he touched upon different aspects of nonclassicality:

In this statement, “…like a scholar in an examination, cannot possibly know which of the two questions I am going to ask first: it so seems that our scholar is prepared to give the right answer to the first question… Therefore, he must know both answers; which is an amazing knowledge,” he touches upon the notion of nonlocality.

In another, “It is rather discomforting that the theory should allow a system to be steered or piloted into one or the other type of state at the experimenter's mercy in spite of his having no access to it,” he hints at what would later be termed as the phenomena of quantum steering.

[1] A. Einstein, B. Podolsky, and N. Rosen, *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?* Phys. Rev. **47**, 777 (1935).

And finally, “When two systems… enter into temporary physical interaction due to known forces between them… they can no longer be described … by endowing each of them with a representative of its own. I would not call that one but rather the characteristic trait of quantum mechanics,” where he finally calls upon entanglement.

To reiterate, Schrödinger called the “characteristic trait of quantum mechanics” being the complete description of a composite system without providing all the information about its subsystems, and originally referred to this “Verschränkung” or entanglement

The signature of nonlocal quantum correlations was first quantified through the seminal derivation of Bell inequalities. In 1964, John Bell showed that for all theoretical description of quantum mechanics, which additionally account for “objective reality and locality” by means of some “hidden variable”, all bipartite correlations must be statistically constrained by a set of inequalities. Further, he pointed out that certain quantum states did not satisfy these inequalities. In the following years, experiments demonstrated that quantum states can violate these Bell inequalities, thus confirming the impossibility of using only “objectively real and local” or local hidden-variable description of quantum phenomena[2]. Over the years, important theoretical and experimental results have supported and enriched the quantum viewpoint of the physical world and established quantum theory as one of the foundational cornerstones of modern physics. Significantly, the enigmatic trait of the world arising due to quantum correlations is at the heart of major technological developments in the 21st Century and is the fundamental resource for quantum information processing.

The violation of Bell inequalities led to a critical interest in quantum correlations for future development of concepts such as quantum communication and the possibility of developing computational devices with no classical analogue. However, it was not until the late 20th Century, that the quantum correlation, in its quintessential form of entanglement, was established in terms of local quantum operations and classical

[2] The notion of nonlocal hidden variables to describe quantum mechanics was first proposed by David Bohm in his now seminal work. But by invoking nonlocality it essentially violates EPR’s original argument against the lack of “objective reality” and “locality” in quantum mechanics.

operations. In subsequent years, various theoretical approaches for studying entanglement, such as inequalities derived from asymptotic rates of information compression, distillation of entangled states, majorization conditions, witnesses and resource theories were introduced and studied[3].

ii) Entanglement

The fundamental basis of what constitutes nonclassicality or how quantum correlations are conceptually formulated is not limited to a single theoretical framework. In a broad sense, nonclassicality arises when composite physical systems or degrees of freedom are correlated in ways that are inaccessible to classical objects. The earliest forms of quantifiable nonclassicality in two-party or bipartite quantum states (bipartite quantum states) arose from the violation of Bell inequality. The conceptualization of quantum correlation has evolved over the years. The fundamental idea that violation of Bell inequality was the key principle of defining quantum correlation suffered a setback when it was shown that there exist certain entangled states that do not violate the Bell inequalities and hence, violation of Bell inequality is a sufficient but not necessary condition for entanglement. This led to the realization that states without entanglement are those which can be prepared using *local quantum operations and classical communication* (LOCC). The set of states that cannot be prepared using LOCC are then called entangled. Consequently the set of separable states is smaller than the set of states that do not violate Bell inequalities.

iii) Local operations and classical communication (LOCC)

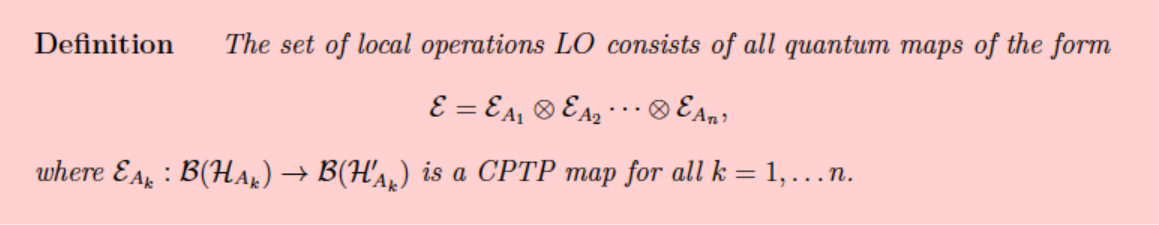
Note: This subsection is not necessary for exams.

a) Local operations (LO):

Let us consider the bipartite case, with Aditi and Bharat sharing a state located at two spatially distant points. The joint system is described by the composite Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, and the class of possible local operations are described by $\mathcal{E} = \mathcal{E}_A \otimes \mathcal{E}_B$,

[3] Although we will not cover all these topics in the course, I will provide additional material for those who are interested in learning a bit more. Of course, excellent books and papers exist on the Internet.

where $\mathcal{E}_A$ is a CPTP map applied by Aditi locally on her system, and $\mathcal{E}_B$ is a CPTP operator applied by Bharat locally on his state. Here, we note that addition of an ancilla state or tracing out of a state are valid CPTP maps that can be applied locally by both Aditi and Bharat.



Definition *The set of local operations LO consists of all quantum maps of the form*

$$\mathcal{E} = \mathcal{E}_{A_1} \otimes \mathcal{E}_{A_2} \cdots \otimes \mathcal{E}_{A_n},$$

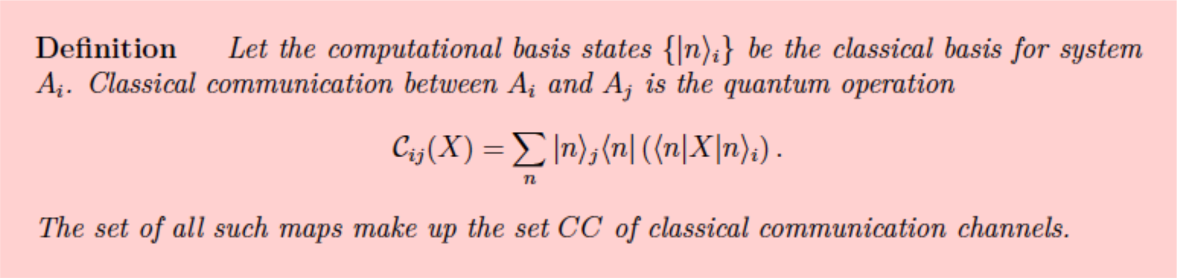
where $\mathcal{E}_{A_k} : \mathcal{B}(\mathcal{H}_{A_k}) \to \mathcal{B}(\mathcal{H}'_{A_k})$ *is a CPTP map for all* $k = 1, \ldots n$.

b) Classical communication (CC):

Classical communication is a bit more subtle. What we term as classical information is essentially any information that can be encoded in some orthonormal basis (say the computation basis) with no superpositions. In the density matrix language, this looks like a diagonal matrix in an orthonormal basis or the eigenbasis. This is deemed classical because the orthogonality of states gives information a strong classical flavour. For instance, we know that information communicated using orthogonal states are perfectly distinguishable. Take the example of qubits: in the absence of coherent superpositions (or off-diagonal terms), the states $|0\rangle$ and $|1\rangle$, behave for all purposes like classical bits 0 and 1, even if they represent the spin of a single atom. This is a very different perspective than how we think of quantumness in other disciplines of physics, say condensed matter or many-body physics. What is termed as classical or quasi-classical in quantum information theory are quantities that have clear classical analogue, even though the systems on which they are encoded can be microscopic and quantum in nature. On the other hand, quantum features, such as coherence and entanglement, have no classical analogue but may in principle arise in large macroscopic quantum systems.[4]

[4] One may argue that coherence surely arises in classical theory of waves, say electromagnetic (EM) theory. To place a simplified argument here, quantum mechanics actually puts the classical EM theory and the first quantization due to Schrodinger's equation on an equal footing, giving us the first step of the famous but often misunderstood "wave-particle" duality. So quantum mechanics in first quantization forces you to think of everything as waves and coherence. In the second step, EM fields are quantized to get the notion of photons, and you now have the second quantization in quantum field theory, which gives rise to the interaction of relativistic particles. Now everything is described in some sort of particle-like objects.

So, getting back to classical communication, we can think of it as a kind of re-labelling of who owns the information stored in an orthonormal basis. Say, Aditi has a classical information stored in her register or orthogonal state $|k\rangle\langle k|_A$, which she simply communicates to Bharat, who then owns $|k\rangle\langle k|_B$. In an operational sense, classical communication typically implies that Bharat can coordinate any local operation on his state conditioned on some local operation done by Aditi.



Definition *Let the computational basis states $\{|n\rangle_i\}$ be the classical basis for system A_i. Classical communication between A_i and A_j is the quantum operation*

$$\mathcal{C}_{ij}(X) = \sum_n |n\rangle_j\langle n| \left(\langle n|X|n\rangle_i\right).$$

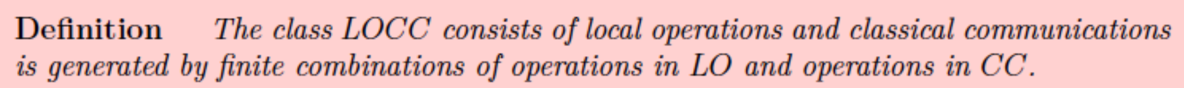
The set of all such maps make up the set CC of classical communication channels.

c) LOCC:

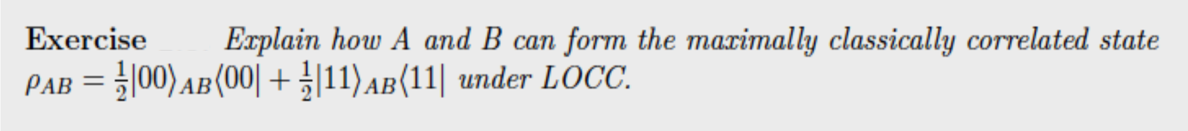
So LOCC operations typically combine and coordinate all local operations with some classical communication. The standard LOCC for bipartite pure systems can be reduced to the following: Aditi does some measurement $\mathcal{M} = \{M_i\}$ on her system, with outcomes $\{m_i\}$. She communicates the value of m_i to Bharat, who then performs a unitary transformation U_i on his system. Mathematically we can write this as:

$$\rho_{AB} \to \sum_i M_i \otimes \mathbb{I}\, \rho_{AB}\, M_i^\dagger \otimes \mathbb{I} \to \sum_i (\mathbb{I} \otimes U_i)\,(M_i \otimes \mathbb{I})\rho_{AB}\,(M_i^\dagger \otimes \mathbb{I})\,(\mathbb{I} \otimes U_i^\dagger)$$

$$= \sum_i (M_i \otimes U_i)\, \rho_{AB}\, (M_i^\dagger \otimes U_i^\dagger)$$



Definition *The class LOCC consists of local operations and classical communications is generated by finite combinations of operations in LO and operations in CC.*



Exercise *Explain how A and B can form the maximally classically correlated state $\rho_{AB} = \frac{1}{2}|00\rangle_{AB}\langle 00| + \frac{1}{2}|11\rangle_{AB}\langle 11|$ under LOCC.*

iv) Transforming entangled states using LOCC

Now that we have discussed what is LOCC and briefly touched upon its connection to entanglement, we look at how quantum states can be transformed using LOCC protocols. In particular, we seek to delve deeper into the connection between LOCC and entanglement. A general study of LOCC protocols in entangled states is a very difficult proposition, so we stick to the simple case of bipartite pure quantum states shared between Aditi and Bharat (say, $|\psi\rangle_{AB}$), and we ask under what conditions can one use LOCC to transform, $|\psi\rangle_{AB} \to |\phi\rangle_{AB}$.

Look at the following example (please check the calculations):

Note: Calculations related to LOCC transformation of the type below are not necessary for exams.

Example: Suppose we want to convert the state,

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

to the state, $|\phi\rangle_{AB} = \cos\theta\,|00\rangle + \sin\theta\,|11\rangle$, using LOCC in a deterministic manner.

Let, Aditi perform measurement, $\mathcal{M} = \left\{M_1 = \begin{pmatrix} \cos\theta & 0 \\ 0 & \sin\theta \end{pmatrix};\ M_1 = \begin{pmatrix} 0 & \cos\theta \\ \sin\theta & 0 \end{pmatrix}\right\}$. Depending on her measurement, she classically communicates her outcome to Bharat classically, who action is conditioned upon inputs from Aditi.

If Aditi performs: $(M_1 \otimes \mathbb{I})|\psi\rangle_{AB} \to |\tilde{\psi}\rangle_{AB} = \begin{pmatrix} \cos\theta & 0 & 0 & 0 \\ 0 & \cos\theta & 0 & 0 \\ 0 & 0 & \sin\theta & 0 \\ 0 & 0 & 0 & \sin\theta \end{pmatrix} |\psi\rangle_{AB},$

$$= \frac{1}{\sqrt{2}}(\cos\theta\,|00\rangle + \sin\theta\,|11\rangle) = \frac{1}{\sqrt{2}}|\phi\rangle_{AB}$$

So, for outcome m_1, Bharat does nothing (or applies the identity operator) to get the state $|\phi\rangle_{AB}$, thus completing the LOCC protocol.

If Aditi performs: $(M_2 \otimes \mathbb{I})|\psi\rangle_{AB} \to |\tilde{\psi}\rangle_{AB} = \begin{pmatrix} 0 & 0 & \cos\theta & 0 \\ 0 & 0 & 0 & \cos\theta \\ \sin\theta & 0 & 0 & 0 \\ 0 & \sin\theta & 0 & 0 \end{pmatrix} |\psi\rangle_{AB},$

$$= \frac{1}{\sqrt{2}}(\cos\theta\,|01\rangle + \sin\theta\,|10\rangle)\,.$$

For outcome m_2, Bharat applies the Pauli σ_x operator on his qubit to get $|\phi\rangle_{AB}$,

$$(\mathbb{I} \otimes \sigma_x)|\tilde{\psi}\rangle_{AB} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} |\tilde{\psi}\rangle_{AB} = \frac{1}{\sqrt{2}}(\cos\theta\,|00\rangle + \sin\theta\,|11\rangle) = \frac{1}{\sqrt{2}}|\phi\rangle_{AB}.$$

The factor $\frac{1}{\sqrt{2}}$ simply tells us that each occur with probability $\left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$.

Exercise: Show that the state $|\psi^-\rangle_{AB} \to |\phi\rangle_{AB}$ is possible under LOCC, where $|\psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$, is the singlet and $|\phi\rangle_{AB}$ is any two-qubit state?

The question that now arises is whether we can always do such a thing. Can we transform any two-qubit state to another state? Is $|\psi\rangle_{AB} \to |\phi\rangle_{AB}$ under LOCC for any $|\psi\rangle_{AB}$ and $|\phi\rangle_{AB}$?

As you may have guessed, the answer is resoundingly NO!! We know that LOCC cannot create entanglement, so you cannot transform a separable state to an entangled state. It so happens that LOCC defines a partial order on set of pure bipartite quantum states, depending on whether we can reach certain states from a given initial entangled state. This also gives us the tool to define entanglement measures. But before that, to fully describe the interconversion of pure, bipartite quantum states we need to introduce the important concept of majorization, which captures the notion of order and disorder in a range of areas that involve some kind of irreversibility.

v) Majorization theory

Majorization is a relation defined between vectors $\boldsymbol{x} = \{x_1, x_2, x_3, \ldots, x_n\}$ and $\boldsymbol{y} = \{y_1, y_2,\ y_3,\ \ldots\ ,\ y_N\}$. The ordering of the components does not matter, but just the distribution of the values and in particular the deviation of these components from being uniform. Since the ordering doesn't matter it is convenient to define the sorted vector $\boldsymbol{x}^{\downarrow} = \{x_1^{\downarrow}, x_2^{\downarrow},\ x_3^{\downarrow}, \ldots,\ x_N^{\downarrow}\}$, where $\boldsymbol{x}^{\downarrow} :=$ re-order components of $\boldsymbol{x}$ so elements decrease in size. For example: $\boldsymbol{x} = \{2, 3, 9, 5, 0, 1\}$ and $\boldsymbol{x}^{\downarrow} = \{9, 5, 3, 2, 1, 0\}$. The majorization relation between two vectors is then related by the following statement:

For two vectors x and y, x is majorized by y, which is written as $x \prec y$, if and only if:

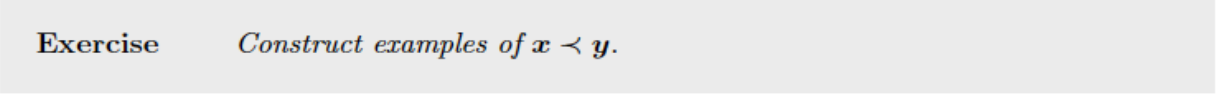
$$\text{I)}\ \sum_{i=1}^{j} x_i^{\downarrow} \leq \sum_{i=1}^{j} y_i^{\downarrow} \text{ for all } j = 1,\ 2,\ \ldots, N-1.$$

$$\text{II)}\ \sum_{i=1}^{N} x_i^{\downarrow} = \sum_{i=1}^{N} y_i^{\downarrow}$$

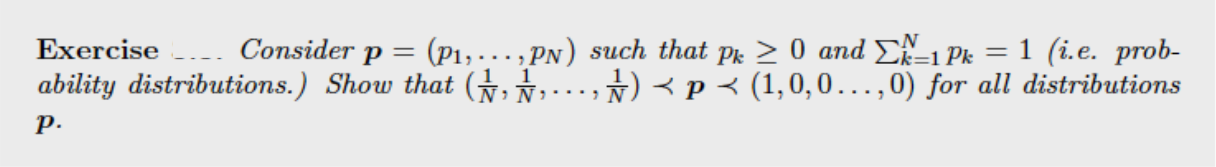
These conditions can be rewritten as:

$$\begin{gathered} x_1^{\downarrow} \leq y_1^{\downarrow} \\ x_1^{\downarrow} + x_2^{\downarrow} \leq y_1^{\downarrow} + y_2^{\downarrow} \\ x_1^{\downarrow} + x_2^{\downarrow} + x_3^{\downarrow} \leq y_1^{\downarrow} + y_2^{\downarrow} + y_3^{\downarrow} \\ . \\ . \\ x_1^{\downarrow} + x_2^{\downarrow} + x_3^{\downarrow} + \cdots + x_N^{\downarrow} = y_1^{\downarrow} + y_2^{\downarrow} + y_3^{\downarrow} + \cdots + y_N^{\downarrow} \end{gathered} \tag{5}$$

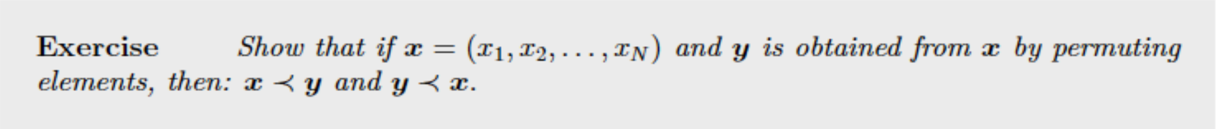
The condition $x \prec y$, implies that x is more disordered than y, or "x is more uniform than y".



Exercise *Construct examples of* $\boldsymbol{x} \prec \boldsymbol{y}$.



Exercise *Consider* $\boldsymbol{p} = (p_1, \ldots, p_N)$ *such that* $p_k \geq 0$ *and* $\sum_{k=1}^{N} p_k = 1$ *(i.e. probability distributions.) Show that* $(\frac{1}{N}, \frac{1}{N}, \ldots, \frac{1}{N}) \prec \boldsymbol{p} \prec (1, 0, 0 \ldots, 0)$ *for all distributions* $\boldsymbol{p}$.



Exercise *Show that if* $\boldsymbol{x} = (x_1, x_2, \ldots, x_N)$ *and* $\boldsymbol{y}$ *is obtained from* $\boldsymbol{x}$ *by permuting elements, then:* $\boldsymbol{x} \prec \boldsymbol{y}$ *and* $\boldsymbol{y} \prec \boldsymbol{x}$.

vi) Nielsen's theorem

Now that we have the majorization theorem, we can now make a strong statement about the central result for pure, bipartite state conversions using the LOCC protocol. The following theorem by Nielsen gives the necessary and sufficient condition for all such possible LOCC conversions.

Consider the state, $|\phi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_A$, where

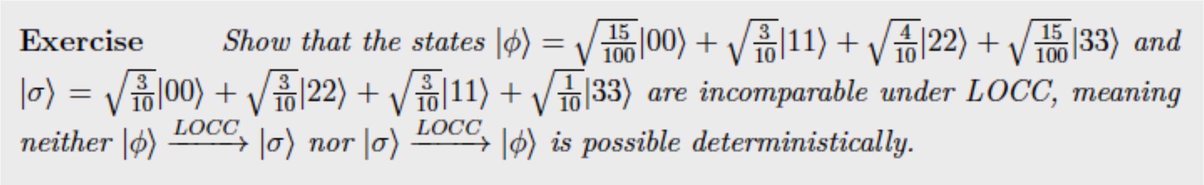
$$\lambda(\phi) := \left\{\text{eigenvalues of } \rho_A = \mathrm{Tr}_B\left[|\phi\rangle\langle\phi|_{AB}\right]\right\}$$

then the transformation, $|\phi\rangle_{AB} \xrightarrow{LOCC} |\psi\rangle_{AB}$ is possible deterministically, if and only if,

$$\lambda(\phi) \prec \lambda(\psi).$$

In other words, the partial order induced by LOCC on the set of pure bipartite states coincides with the partial order from majorization theory for the marginal spectra $\boldsymbol{\lambda}(\phi)$ of the pure states.

For a given pure state there will exist states which can be reached in a reversible way under LOCC, and states that can be reached (or can be arrived from) in an irreversible way, and then there are states that are incomparable under LOCC.



Exercise *Show that the states* $|\phi\rangle = \sqrt{\frac{15}{100}}|00\rangle + \sqrt{\frac{3}{10}}|11\rangle + \sqrt{\frac{4}{10}}|22\rangle + \sqrt{\frac{15}{100}}|33\rangle$ *and* $|\sigma\rangle = \sqrt{\frac{3}{10}}|00\rangle + \sqrt{\frac{3}{10}}|22\rangle + \sqrt{\frac{3}{10}}|11\rangle + \sqrt{\frac{1}{10}}|33\rangle$ *are incomparable under LOCC, meaning neither* $|\phi\rangle \xrightarrow{LOCC} |\sigma\rangle$ *nor* $|\sigma\rangle \xrightarrow{LOCC} |\phi\rangle$ *is possible deterministically.*

Now one can attach a measure of entanglement E for pure bipartite quantum states under LOCC, by at the very least demanding that if $|\psi\rangle_{AB} \to |\phi\rangle_{AB}$, we have the relation, $E(|\psi\rangle_{AB}) \geq E(|\phi\rangle_{AB})$. This condition demands that the measure is an entanglement monotone under LOCC, meaning its value can never increase under local operations and classical communications. This makes sense as we know LOCC cannot create nor increase entanglement.

For such an entanglement monotone we also demand that if the reversible transformation $|\phi\rangle_{AB} \to |\psi\rangle_{AB}$ is permissible, then $E\left(|\psi\rangle_{AB}\right) = E(|\phi\rangle_{AB})$, and the states must be equally entangled with respect to any measure. If $|\phi\rangle_{AB}$ and $|\psi\rangle_{AB}$ are incomparable then there is, a priori, no constraint on the measure of entanglement.

vii) Catalysis

Consider the situation where Aditi and Bharat share a quantum state consisting by a pair of qudits ($d \ = \ 4$), given by

$$|\psi\rangle_{AB} = \sqrt{{}^{2}/_{5}}\,|00\rangle + \sqrt{{}^{2}/_{5}}\,|11\rangle + \sqrt{{}^{1}/_{10}}\,|22\rangle + \sqrt{{}^{1}/_{10}}\,|33\rangle.$$

Using Nielsen's theorem, it is clear to see that Aditi and Bharat cannot use LOCC to deterministically transform $|\psi\rangle_{AB}$ to the state below:

$$|\phi\rangle_{AB} = \sqrt{{}^{1}/_{2}}\,|00\rangle + \sqrt{{}^{1}/_{4}}\,|11\rangle + \sqrt{{}^{1}/_{4}}\,|22\rangle.$$

Let, $\lambda(\phi) := \{\text{eigenvalues of}\, \rho_A = \mathrm{Tr}_B\big[|\phi\rangle\langle\phi|_{AB}\big]\}$ (similarly for $\lambda(\psi)$). Since, both $|\psi\rangle_{AB}$ and $|\phi\rangle_{AB}$ are written in their Schmidt representation, it is straightforward to estimate both $\lambda(\psi)$ and $\lambda(\phi)$:

$$\lambda(\psi) = \{x\} = \{{}^{2}/_{5}, {}^{2}/_{5}, {}^{1}/_{10}, {}^{1}/_{10}\};\ \lambda(\phi) = \{y\} = \{{}^{1}/_{2}, {}^{1}/_{4}, {}^{1}/_{4}, 0\}.$$

Applying the majorization criteria we have;

$$x_1 \le y_1;\ x_1 + x_2 \ge y_1 + y_2.$$

Therefore, $\lambda(\psi) \nprec \lambda(\phi)$ and $\lambda(\phi) \nprec \lambda(\psi)$.

But if they can find an ancilla state somewhere:

$$|\zeta\rangle_{A'B'} = \sqrt{{}^{3}/_{5}}\,|00\rangle + \sqrt{{}^{2}/_{5}}\,|11\rangle.$$

it can be shown that $|\psi\rangle_{AB} \otimes |\zeta\rangle_{A'B'} \xrightarrow{LOCC} |\phi\rangle_{AB} \otimes |\zeta\rangle_{A'B'}$. Therefore the state $|\zeta\rangle_{A'B'}$ acts like a catalyst.

Let, $\lambda(\psi) := \{\text{eigenvalues of}\, \rho_{AA'} = \mathrm{Tr}_{BB'}\big[|\psi\rangle\langle\psi|_{AB} \otimes |\zeta\rangle\langle\zeta|_{A'B'}\big]\}$. The same for $\lambda(\phi)$. The eigenvalues are obtained by simply multiplying and squaring the Schmidt coefficients:

$$\lambda(\psi) = \{{}^{6}/_{25}, {}^{6}/_{25}, {}^{4}/_{25}, {}^{4}/_{25}, {}^{3}/_{50}, {}^{3}/_{50}, {}^{2}/_{50}, {}^{2}/_{50}\};$$

$$\lambda(\phi) = \{{}^{3}/_{10}, {}^{2}/_{10}, {}^{3}/_{20}, {}^{3}/_{20}, {}^{2}/_{20}, {}^{2}/_{20}, 0, 0\}.$$

It is easy to verify that now, $\lambda(\psi) \prec \lambda(\phi)$, which implies that

$$|\boldsymbol{\psi}\rangle_{AB} \otimes |\boldsymbol{\zeta}\rangle_{A'B'} \xrightarrow{\boldsymbol{LOCC}} |\boldsymbol{\phi}\rangle_{AB} \otimes |\boldsymbol{\zeta}\rangle_{A'B'}.$$

viii) Majorization, the notion of disorder and its connection to LOCC

Note: This subsection is not necessary for exams.

As stated earlier the notion that $x \prec y$, implies that x is more disordered than y, is because $x \prec y$, if and only if $x = \sum_i q_i P_i y$, where P_i are permutation matrices. In other words, x is more disordered then y as it can always be represented as a convex mixture of vectors obtained after permuting the elements of y.

Interestingly, a doubly stochastic matrix D (with non-negative elements, and each row and column sum equal to 1) can always be written as $D = \sum_i q_i P_i$. Therefore, for $x \prec y$, we have $x = Dy$, for some doubly-stochastic matrix.

Now, Horn's lemma[5] connects these double stochastic matrices to unitary matrices and majorization. For instance, if U is a unitary matrix with elements u_{ij}, then the matrix $D_{ij} \equiv |u_{ij}|^2$ is a doubly stochastic. So, for $x \prec y$, we have $x = Dy$, where D is a unitary-stochastic matrix.

Uhlmann's theorem connects the Horn's lemma to the eigenvalues of Hermitian operators, X and Y, given by say $\lambda(X)$ and $\lambda(Y)$, by stating that $\lambda(X) \prec \lambda(Y)$, if and only if, $X = \sum_i q_i U_i Y U_i^\dagger$, where U_i are unitary matrices. This shows that operator X (reduced density matrices in Nielsen's theorem) is more disordered that Y, as X can be obtained by the convex mixing of Y acted upon by unitaries.

So, all that remains is to connect LOCC to Uhlmann's lemma. As shown earlier in the example on LOCC, for bipartite pure states shared between two parties, the LOCC protocol can be described in terms of measurement $\mathcal{M} = \{M_i\}$ performed by Aditi and a set of conditioned unitaries $\{U_i\}$ performed by Bharat locally on his system. Again, consider the transformation, $|\psi\rangle_{AB} \rightarrow |\phi\rangle_{AB}$.

[5] Please see the paper: *Majorization and the interconversion of bipartite states*, by Nielsen and Vidal, Quantum Information & Computation 1, 76 (2001). Also see: Chapter 12 of Nielsen and Chuang.

At Aditi's end she starts with a reduced system be ρ_ψ and ends up with ρ_ϕ after measurements on her subsystem, i.e., $M_i \rho_\psi {M_i}^\dagger = p_i \rho_\phi$, where p_i is the probability of the measurement outcome, m_i.

Now, $M_i \rho_\psi {M_i}^\dagger = \sqrt{M_i \rho_\psi {M_i}^\dagger}\sqrt{M_i \rho_\psi {M_i}^\dagger} = \sqrt{M_i \rho_\psi {M_i}^\dagger}\, U_i {U_i}^\dagger \sqrt{M_i \rho_\psi {M_i}^\dagger}$ and $M_i \rho_\psi {M_i}^\dagger = M_i \sqrt{\rho_\psi}\sqrt{\rho_\psi} {M_i}^\dagger$, which gives us the polar decomposition: $M_i \sqrt{\rho_\psi} = \sqrt{M_i \rho_\psi {M_i}^\dagger} U_i = \sqrt{p_i \rho_\phi}\, U_i$. Multiplying with the adjoint gives us:

$$\sqrt{\rho_\psi} {M_i}^\dagger M_i \sqrt{\rho_\psi} = p_i\, {U_i}^\dagger \rho_\phi U_i.$$

Summing, we have: $\rho_\psi = \sum_i p_i\, {U_i}^\dagger \rho_\phi U_i$, which gives us the Uhlmann's theorem for convex mixing and thus connects LOCC with majorization.