

Resource theory of local operations and shared randomness - a primer

quantUM seminars, 17 feb 2023

Andrea D'Urbano



Index

- Preliminary examples and motivations;
- Resource theory framework;
- Application to EPR scenario;
- Ideas, future work and discussion.



Introduction

An active area of research in quantum foundations is the study of nonclassicality. The first example of such nonclassicality was given by Einstein, Podolsky and Rosen in their famous scenario.

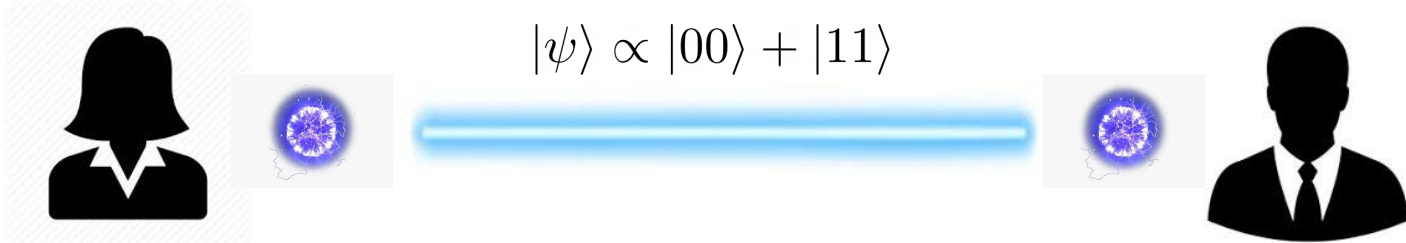
In experiments where space-like separated subsystems share a common goal, the separation between classical and quantum effects is particularly evident: quantum theory allow for correlations unobtainable by classical means.

As a first step, let's recall two examples: EPR and Bell experiments.



EPR paradox

This thought experiment was used to argue the incompleteness of quantum theory description of reality.



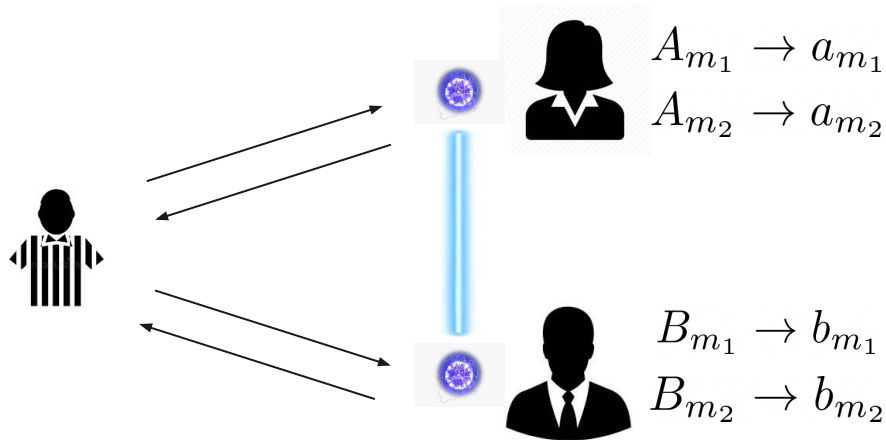


EPR steering

The Alice's measurement on her half on the bipartite entangled state, following the rules of quantum mechanics, determines the outcome of Bob's measurement *instantaneously*. This phenomenon, often referred as "steering", gave rise to a lot of discussion on the superluminal influence that the 2 subsystems seem to have on each other. The key points are:

- No information is vehicolated through this phenomenon;
- After the measurement the knowledge of the other system is updated: there is no causal influence;
- Alice and Bob share a common cause (as discussed later).

Bell experiment



A similar discussion can be made for a Bell experiment.

By sharing an entangled state (a quantum resource) and a common classical cause, Alice and Bob are able to outperform any classical strategy, demonstrating a quantum advantage.

$$\langle A_{m_1} B_{m_1} \rangle + \langle A_{m_1} B_{m_2} \rangle + \langle A_{m_2} B_{m_1} \rangle - \langle A_{m_2} B_{m_2} \rangle \not\leq 2$$



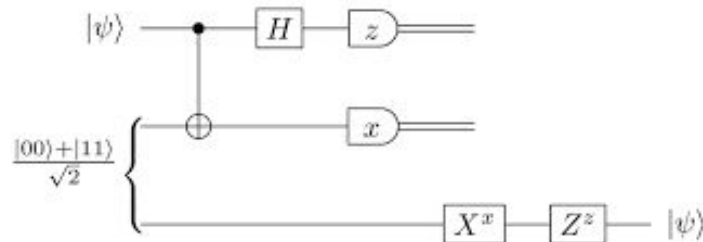
LOSR

- We would like a framework, where the description of such nonsignalling resources, games and experiments to probe them are unified.
- This framework was introduced in [1] and it is called: local operations and shared randomness (LOSR).
- This formalism was applied in [2] and [3] to describe respectively Bell scenarios and EPR experiments.

Resources

Many field of science use the notion of *resource* to describe processes and states (physical or logical). Talking about resources allow to address problems as the conversion among them under specific conditions.

For example suppose that Alice and Bob do not share a quantum channel, but they can communicate classically and can also perform some local operations on quantum states. This set of operations is commonly referred to as local operations and classical communication (LOCC). The quantum teleportation protocol can be recasted in resource theory using LOCC: an entangled state is transformed into a quantum channel.





Mathematical description

A resource theory, is mathematically described by a *symmetric monoidal category* where the objects are resources and the morphisms are transformations among them [5].

A category is a collection of “objects” linked by maps, also called “morphisms”. The maps must be composable by associativity and it must always exist an identity map for each object.

A symmetric monoidal category, without the proper rigor, is a category equipped with an associative and commutative operator:

$$\otimes : \mathcal{C} \times \mathcal{C} \rightarrow \mathcal{C}$$



Type of resources

Here a resource is represented as a completely positive, trace-preserving, nonsignaling quantum channel (i.e. a linear map between Hilbert spaces). Depending on the input and output space of a resource, we can define:

- Trivial resources, represented pictorially with no lines;
- Classical resources, represented pictorially with one line;
- Quantum resources, represented pictorially with two lines.



Partition and global Type

A resource in general is shared among various parties. The type of a single party's share of a resource, is called partition-type of the i -th party :

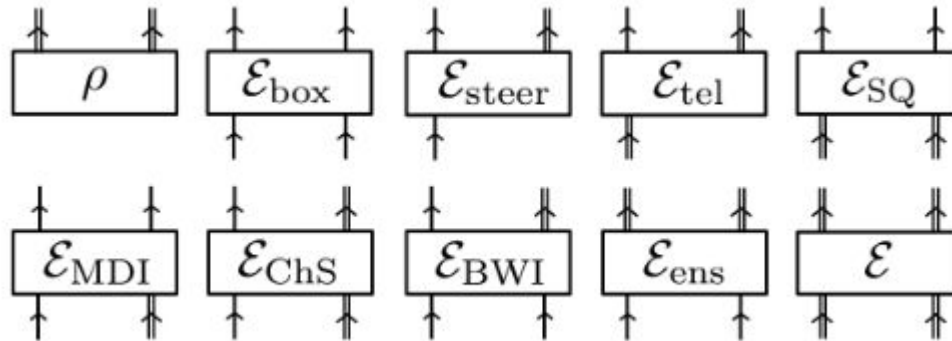
$$T_i := X_i \rightarrow Y_i \quad X, Y \in \{I, C, Q\}$$

Similarly, the global type will be:

$$T := X_1 X_2 \cdots X_n \rightarrow Y_1 Y_2 \cdots Y_n$$

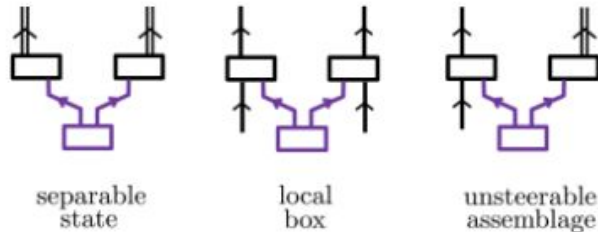


Resources for 2 party system



Free vs Non-free resources

A resource is said to be free with respect to a specific set of operations, if the parties can generate it freely using the restrictions imposed. For example a LOSR free resource can be generated using only local operations and shared randomness.



Any other resource is non-free and is a source of nonclassicality in that set of operations.



Type-independent theory

The purpose of the type-independent resource theory presented in [1] is to quantitatively characterize non-free resources of arbitrary types.

Here we will follow their discussion, specific to LOSR, to understand the techniques adopted by this theory.

Transforming resources

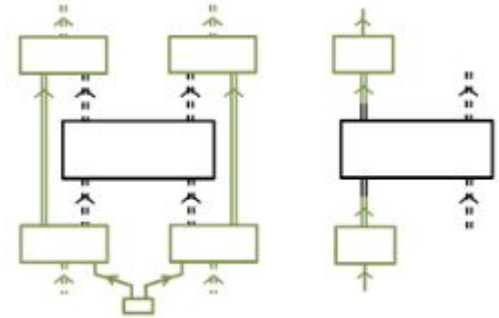
Using free operations, resources can be transformed one into another (morphisms). The set of free operations induces a preorder (reflexivity + transitivity) over the set of all resources.

$$R \succcurlyeq_{LOS_R} R' \quad \text{iff} \quad R' = \tau \circ R$$

If the following hold:

$$R \succcurlyeq_{LOS_R} R' \quad \wedge \quad R' \succcurlyeq_{LOS_R} R$$

Then the two resources are in the same equivalence class.





Encoding nonclassicality

Reasoning in terms of global types and not in terms of resources themselves, is useful to encode and compare, using the preorder structure, the different manifestations of nonclassicality. If for every resource of a type T' , there exist a resource of type T in the same equivalence class, then T encode the nonclassicality of T' .

- $QQ \rightarrow QQ$ Encode every other bipartite global type;
- Ordering over global types can be deduced from the ordering over partition types.

Pairings of partition-types

Does type T encode the nonclassicality of type T' ?

$T' \backslash T$	$I \rightarrow C$	$I \rightarrow Q$	$C \rightarrow C$	$C \rightarrow Q$	$Q \rightarrow C$	$Q \rightarrow Q$
$I \rightarrow C$	✓ embed	✓ embed	✓ embed	✓ embed	✓ embed	✓ embed
$I \rightarrow Q$	✗ trans.	✓ embed	✗ Werner states	✓ embed	✓ semi-quantum games	✓ embed
$C \rightarrow C$	✗ trans.	✗ LOSR cannot entangle	✓ embed	✓ embed	✓ embed	✓ embed
$C \rightarrow Q$	✗ trans.	✗ trans.	✗ trans.	✓ embed	✓ Thm 3	✓ embed
$Q \rightarrow C$	✗ trans.	✗ trans.	✗ trans.	?	✓ embed	✓ embed
$Q \rightarrow Q$	✗ trans.	✗ trans.	✗ trans.	?	✓ Thm 3	✓ embed



Applications

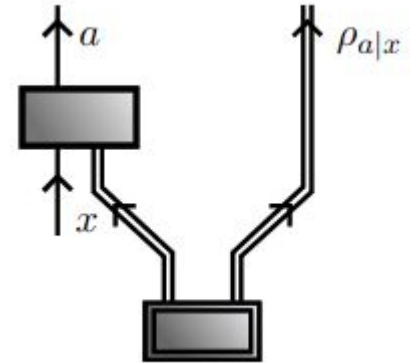
The resource-theoretic approach presented, was applied in literature in Bell experiments [2] and in EPR scenarios [3]. Our goal is to build on these examples to apply this approach on a quantum multiparty protocol, such as quantum secret sharing [4], or some similar and simpler examples.

We are going to present the applications of this approach to the EPR scenarios.

EPR scenarios

Alice and Bob share a physical system and performs local operations on it, possibly sharing a common cause. The chosen measurement setting is denoted by x , and the outcome by a . By measuring her system, Alice refines her knowledge of Bob's system, which is now described by a conditional marginal state. The ensemble of ensembles of quantum states is called an *assemblage*:

$$\Sigma_{A|X} := \left\{ \left\{ p(a|x) \rho_{a|x} \right\}_{a \in A} \right\}_{x \in X}$$





Enveloping theory

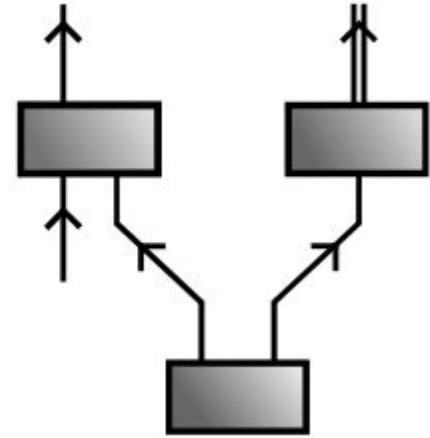
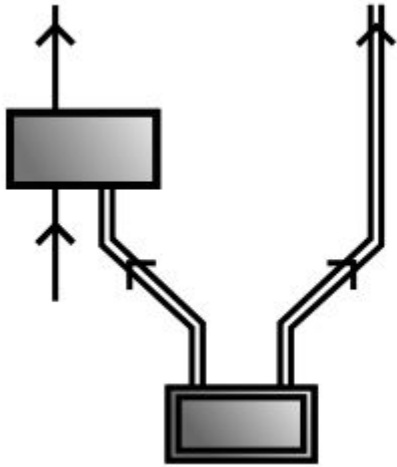
In order to quantify the resourcefulness of given processes, it must be distinguished the set of all possible resources that can be produced in the setup, called *enveloping theory*, by the set of free operation, the *free subtheory*. Then, using the notion of preorder previously introduced, the relative value of any pair of resources can be determined.

Assemblages can be studied as processes in and of themselves, since these contain all the relevant information for characterizing an EPR scenario. Therefore in this instance of resource theory, the resources are taken to be assemblages:

$$\Sigma_{A|X} := \left\{ \left\{ \sigma_{a|x} \right\}_{a \in A} \right\}_{x \in X}$$



Causality structure and LORS operations





Quantumly-realizable assemblage

In quantum theory, the state of the shared system can be described by a density matrix and Alice implements generalised measurements, i.e., positive operator-valued measures (POVMs), $\{\{M_{a|x}\}_{a \in A}\}_{x \in X}$

An assemblage has a quantum realization iff there exist an Alice Hilbert space where the measurements take place, and a density matrix such that for all x and a :

$$\sigma_{a|x} = \text{tr}_A\{(M_{a|x} \otimes \mathbb{I})\rho\}$$



Assemblage with classical common cause

These are all and only those that can be constructed freely from LOSR operations. We can consider:

- a probability distribution describing the common cause $p(\lambda)$
- a conditional probability distribution for the Alice's box $p(a|x, \lambda)$
- a normalized quantum state for Bob's state ρ_λ

Hence, the elements of an LOSR-free assemblage (“unsteerable”) can be written as

$$\sigma_{a|x} = \sum_{\lambda} p(\lambda) p(a|x, \lambda) \rho_{\lambda}$$

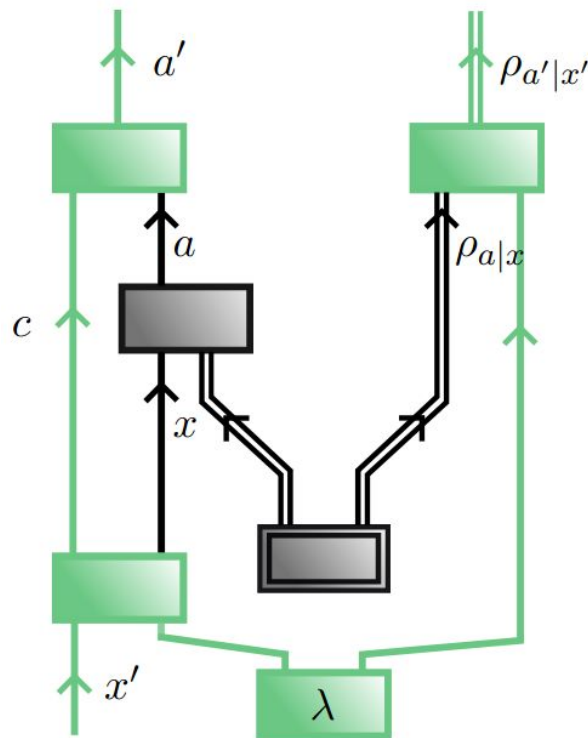
LOSR transformations

$p(c, x|x', \lambda)$ encodes the classical pre-processing of Alice's input;

$p(a'|a, c)$ encodes the classical post-processing of Alice's output

$\mathcal{E}_\lambda[\cdot]$ completely positive trace preserving (CPTP) map which post-processes Bob's quantum system.

$$\sigma'_{a'|x'} = \sum_{\lambda, c} \sum_{a, x} p(\lambda) p(c, x|x', \lambda) p(a|x) p(a'|a, c) \mathcal{E}_\lambda(\rho_{a|x})$$



LOSR transformations

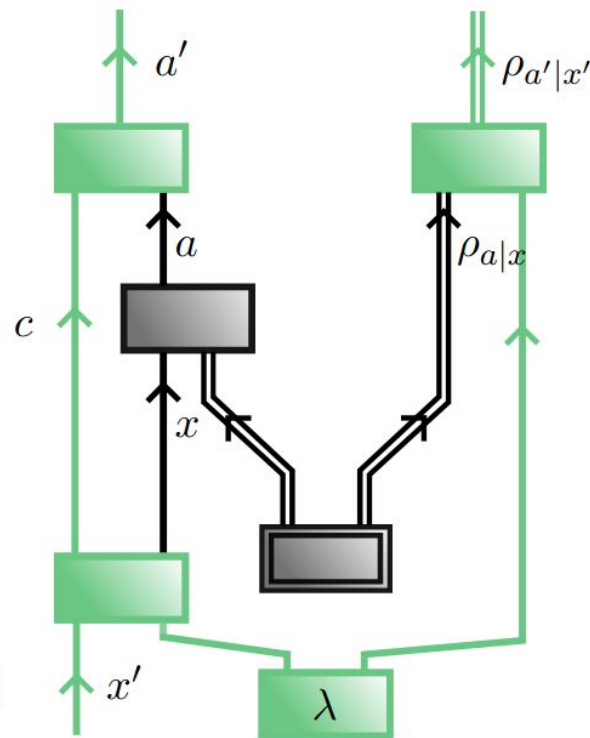
$p(c, x|x', \lambda)$ encodes the classical pre-processing of Alice's input;

$p(a'|a, c)$ encodes the classical post-processing of Alice's output

$\mathcal{E}_\lambda[\cdot]$ completely positive trace preserving (CPTP) map which post-processes Bob's quantum system.

$$\sigma'_{a'|x'} = \sum_{\lambda, c} \sum_{a, x} p(\lambda) p(c, x|x', \lambda) p(a|x) p(a'|a, c) \mathcal{E}_\lambda(\rho_{a|x})$$

$$\sigma'_{a'|x'} = \sum_{\lambda} \sum_{a, x} p(\lambda) p(a'|a, x', \lambda) p(x|x', \lambda) p(a|x) \mathcal{E}_\lambda(\rho_{a|x})$$



LOSR transformations

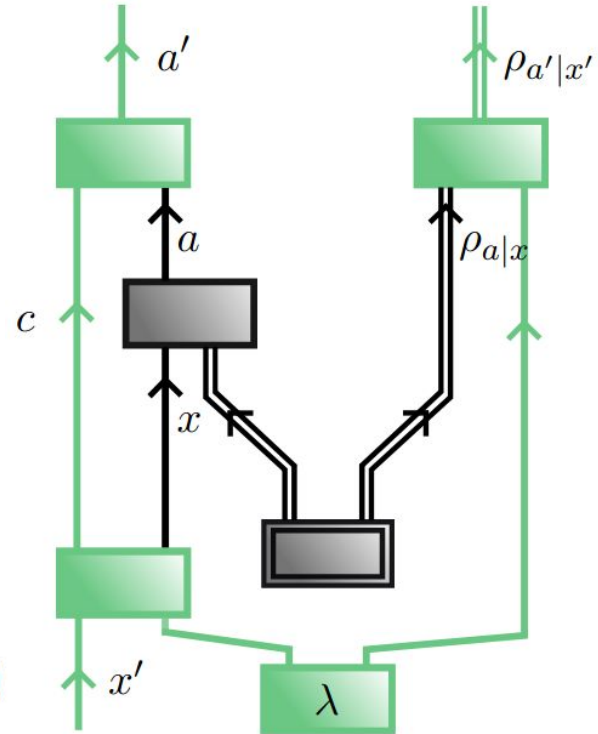
$p(c, x|x', \lambda)$ encodes the classical pre-processing of Alice's input;

$p(a'|a, c)$ encodes the classical post-processing of Alice's output

$\mathcal{E}_\lambda[\cdot]$ completely positive trace preserving (CPTP) map which post-processes Bob's quantum system.

$$\sigma'_{a'|x'} = \sum_{\lambda, c} \sum_{a, x} p(\lambda) p(c, x|x', \lambda) p(a|x) p(a'|a, c) \mathcal{E}_\lambda(\rho_{a|x})$$

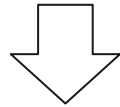
$$\sigma'_{a'|x'} = \sum_{\lambda} \sum_{a, x} p(\lambda) p(a'|a, x', \lambda) p(x|x', \lambda) p(a|x) \mathcal{E}_\lambda(\rho_{a|x})$$





Convexity

The set of free operations is convex, its extremal elements are deterministic, and enumerable for fixed type of the source and of the target resource.



This implies that the set of free operations mapping from a given source resource type to a given target resource type is a polytope.



Convexity

$$\begin{cases} \tau_0 \in LOSR \\ \tau_1 \in LOSR \end{cases} \implies \omega\tau_0 + (1 - \omega) \in LOSR, \omega \in [0, 1]$$

It is demonstrable showing that the resources required to achieve such a mixing are achievable using LOSR. In fact it is sufficient to sample a binary variable that decides what operation will be implemented, and add it to the shared randomness.



Decomposition of Alice's processing

Alice's pre- and post-processing can be decomposed as a convex combination of deterministic operations:


$$p(a'|a, x', \lambda) p(x|x', \lambda) = \sum_{\tilde{\lambda}} p(\tilde{\lambda}|\lambda) D(a'|a, x', \tilde{\lambda}) D(x|x', \tilde{\lambda})$$




Decomposition of Alice's processing

Alice's pre- and post-processing can be decomposed as a convex combination of deterministic operations:

$$p(a'|a, x', \lambda) p(x|x', \lambda) = \sum_{\tilde{\lambda}} p(\tilde{\lambda}|\lambda) D(a'|a, x', \tilde{\lambda}) D(x|x', \tilde{\lambda})$$


$$D(a'|a, x', \tilde{\lambda}) = \delta_{a', f_{\tilde{\lambda}}(a, x')}$$



$$D(x|x', \tilde{\lambda}) = \delta_{x, g_{\tilde{\lambda}}(x')}$$



Simplified LOSR transformation

$$\sigma'_{a'|x'} = \sum_{\tilde{\lambda}} \sum_{a,x} D(a'|a, x', \tilde{\lambda}) D(x|x', \tilde{\lambda}) \tilde{\mathcal{E}}_{\tilde{\lambda}}(\sigma_{a|x})$$

The deterministic operations simply select a fixed outcome for each possible choice of the parameters. This simplified characterisation of a generic LOSR transformation is useful computationally.


$$\tilde{\mathcal{E}}_{\tilde{\lambda}}(\sigma_{a|x}) = \sum_{\lambda} p(\lambda) p(\tilde{\lambda}|\lambda) \mathcal{E}_{\lambda}(p(a|x) \rho_{a|x})$$



Deciding resource conversions

$$\sigma'_{a'|x'} = \sum_{\tilde{\lambda}} \sum_{a,x} D(a'|a, x', \tilde{\lambda}) D(x|x', \tilde{\lambda}) \tilde{\mathcal{E}}_{\tilde{\lambda}}(\sigma_{a|x})$$

An assemblage can be converted into another under LOSR operations if and only if there exist a collection of completely positive and trace non-increasing (CPTNI) maps $\tilde{\mathcal{E}}_{\tilde{\lambda}}$ such that the decomposition is feasible: this is a decision problem.



Choi-Jamiolkowski isomorphism

This is an isomorphism between channels and states. Every CPTP map $\mathcal{E} : \mathcal{H}_B \rightarrow \mathcal{H}_{B'}$ can be associated with an operator W on $\mathcal{H}_B \otimes \mathcal{H}_{B'}$ such that:

$$\mathcal{E}(\rho_B) = d_B \operatorname{tr}_B \left\{ W (\mathbb{I}_{B'} \otimes \rho_B^T) \right\}$$

Conversely, the operator can be written as:

$$W = (\mathcal{E} \otimes \mathbb{I}_{B'}) |\Omega\rangle \langle \Omega|, \quad |\Omega\rangle = \frac{1}{\sqrt{d_B}} \sum_{i=1}^{d_B} |ii\rangle$$



Semidefinite program (SDP)

With the previous correspondence, the decision problem can be formulated as a semidefinite program.
Rewriting the map in the composition:

$$\sigma'_{a'|x'} = \sum_{\lambda} \sum_{a,x} D(a'|a, x', \lambda) D(x|x', \lambda) d_B \operatorname{tr}_B \left\{ W_{\lambda} (\mathbb{I}_{B'} \otimes \sigma_{a|x}^T) \right\}$$

Where W_{λ} is the Choi state, i.e. a $(d_B \times d_{B'})$ by $(d_B \times d_{B'})$ matrix.

Semidefinite program (SDP)

With the previous correspondence, the decision problem can be formulated as a semidefinite program.
Rewriting the map in the decomposition:

$$\sigma'_{a'|x'} = \sum_{\lambda} \sum_{a,x} D(a'|a, x', \lambda) D(x|x', \lambda) d_B \operatorname{tr}_B \left\{ W_{\lambda} (\mathbb{I}_{B'} \otimes \sigma_{a|x}^T) \right\}$$

Where $\mathbb{I}_{B'}$ is the Choi state, i.e. a $(d_B \times d_{B'})$ by $(d_B \times d_{B'})$ matrix.

Enumeration of
deterministic
distributions

$$|\mathbb{A}'|^{|\mathbb{A}| \times |\mathbb{X}'|} \times |\mathbb{X}|^{|\mathbb{X}'|}$$

Semidefinite program (SDP)

The assemblage $\Sigma_{\mathbb{A}|\mathbb{X}}$ can be converted into the assemblage $\Sigma'_{\mathbb{A}'|\mathbb{X}'}$ under LOSR operations, denoted by $\Sigma_{\mathbb{A}|\mathbb{X}} \xrightarrow{\text{LOSR}} \Sigma'_{\mathbb{A}'|\mathbb{X}'}$, if and only if the following SDP is feasible:

$$\begin{aligned}
 & \text{given } \{ \{ \sigma_{a|x} \}_a \}_x, \{ \{ \sigma'_{a'|x'} \}_{a'} \}_{x'}, \{ D(a'|a, x', \lambda) \}_{\lambda, a', a, x'}, \{ D(x|x', \lambda) \}_{\lambda, x, x'} \\
 & \text{find } \{ (W_\lambda)_{BB'} \}_\lambda \\
 & \text{s.t. } \begin{cases} W_\lambda \geq 0, \\ \text{tr}_{B'} \{ W_\lambda \} \propto \frac{1}{d} \mathbb{I}_B \quad \forall \lambda, \\ \sum_\lambda \text{tr}_{B'} \{ W_\lambda \} = \frac{1}{d} \mathbb{I}_B, \\ \sigma'_{a'|x'} = \sum_\lambda \sum_{a,x} D(a'|a, x', \lambda) D(x|x', \lambda) d_B \text{tr}_B \left\{ W_\lambda (\mathbb{I}_{B'} \otimes \sigma_{a|x}^T) \right\}. \end{cases}
 \end{aligned}$$

When the conversion is not possible, we denote it by $\Sigma_{\mathbb{A}|\mathbb{X}} \not\xrightarrow{\text{LOSR}} \Sigma'_{\mathbb{A}'|\mathbb{X}'}$.



Resource monotones

Using the SDP, it is possible to study the preorder among resources numerically. It exist however, also an analytical methods called *resource monotones*: functions which are monotonic under the free operations in the resource theory. Using monotones it is possible to find equivalence classes and conversion relations among resources.

$$M : Res \rightarrow \mathbb{R}, \text{ if } M(R_1) < M(R_2) \implies R_1 \not\rightarrow R_2$$

Reals numbers could be seem as a partial quantification of the “nonfreeness” of the resources.

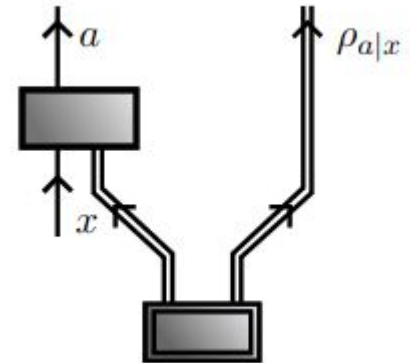
Example EPR

Consider an EPR scenario with $\mathbb{A} = \mathbb{X} = \{0, 1\}$ and Bob's dimension is 2. Alice and Bob shared an entangled state:

$$|\theta\rangle = \cos \theta |00\rangle + \sin \theta |11\rangle$$

The assemblage is:

$$\sigma_{a|x}^\theta = \text{tr}_A \left\{ \widetilde{M}_{a|x} \otimes \mathbb{I} |\theta\rangle \langle \theta| \right\}$$



Example EPR

Consider an EPR scenario with $\mathbb{A} = \mathbb{X} = \{0, 1\}$ and Bob's dimension is 2.
Alice and Bob shared an entangled state:

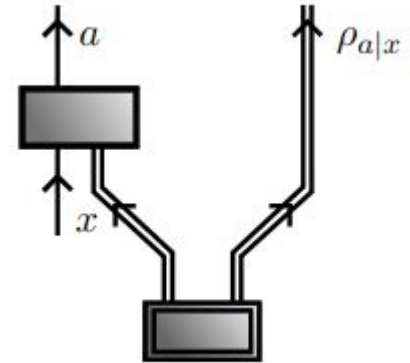
$$|\theta\rangle = \cos\theta |00\rangle + \sin\theta |11\rangle$$

The assemblage is:

$$\sigma_{a|x}^\theta = \text{tr}_A \left\{ \widetilde{M}_{a|x} \otimes \mathbb{I} |\theta\rangle \langle \theta| \right\}$$

$$\widetilde{M}_{a|0} = \frac{1}{2} \{ \mathbb{I} + (-1)^a \sigma_z \}$$

$$\widetilde{M}_{a|1} = \frac{1}{2} \{ \mathbb{I} + (-1)^a \sigma_x \}$$





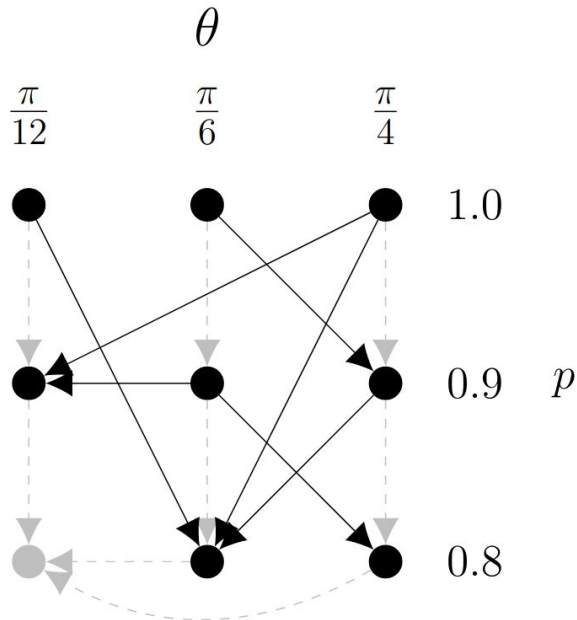
Example EPR

Let's also add another parameter responsible for mixing the assemblage elements with noise.

$$\Sigma_{\mathbb{A}|\mathbb{X}}^{\theta,p} = \left\{ \left\{ p \sigma_{a|x}^{\theta} + (1-p) \frac{\mathbb{I}}{4} \right\}_{a \in \mathbb{A}} \right\}_{x \in \mathbb{X}}$$

The family of assemblages is parametrized by 2 parameters and its preorder structure can be studied using monotones or numerically, as discussed before.

Example: numerical analysis



The black dots correspond to nonfree assemblages, and the grey dot represents a free assemblage. The arrows represent possible conversions.

Using monotones the numerical results are confirmed. Furthermore, providing a complete set of monotone completely characterize the preorder.

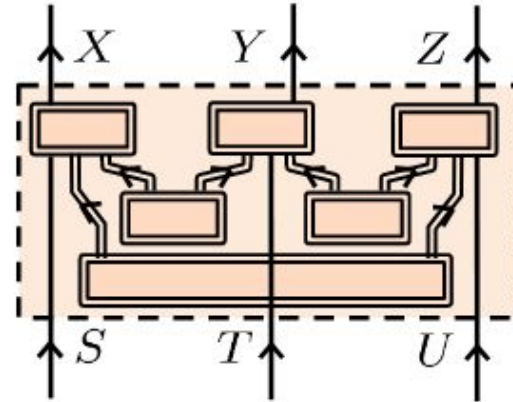
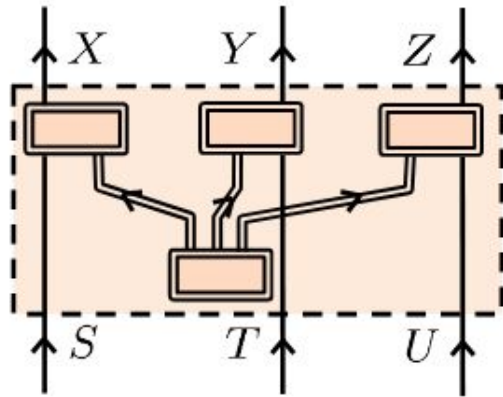


Causal structure

A resource theory, as we have seen, must be coupled with a set of allowed (free) operations, for example LOSR or LOCC. There is however another fundamental component which until now we gave for granted: the *causal structure*. Its description is based on generalized probability theories GPT, which imply 2 possible causal influences:

- GPT channel among parties, describing cause-effect relation;
- GPT states, describing common-cause relations.

Effects of causal structures



The causal structure specifies how randomness is shared among the parties, and consequently specifies whether or not convexity holds.



Ideas

- Apply this framework to quantify the advantage of quantum protocols;
- Problems and limitations (ex, multi-stage processes, different free operations at each step);
- Nonconvexity induced by adversary (discussion on causal structure).



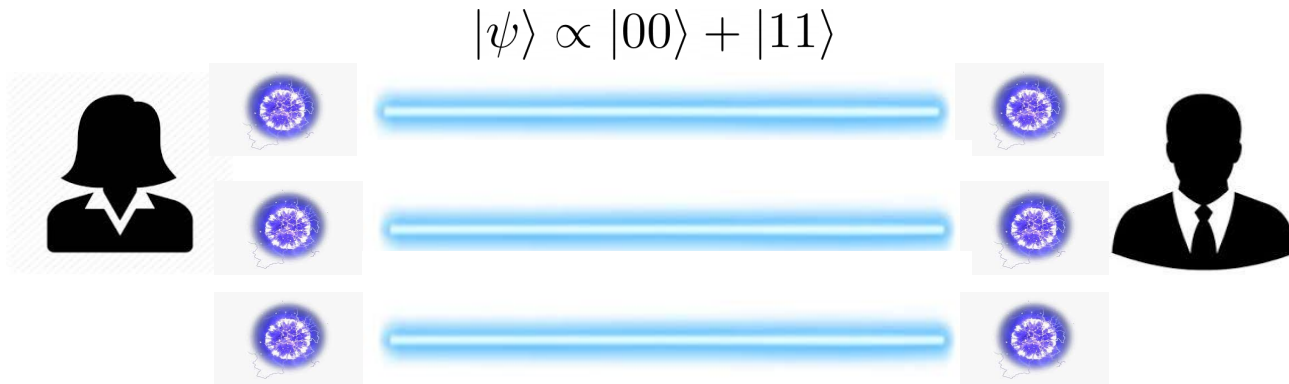
Quantum secret sharing

To the best of my knowledge, the simplest quantum multiparty computation protocol is quantum secret sharing [4]. It works by sharing among the participants multiple entangled states (usually generalized GHZ states), and measuring them in one of two possible bases. The outcome of the measurement must not be revealed. After this stage, the participants share the choice of basis, and therefore can deduce some informations about other participants' measurements.

Let's see a simple version of the protocol, involving only two participants and producing a shared key.

Insecure quantum key distribution

Suppose we have Alice and Bob, sharing lots of numbered entangled pairs of qubits. Using this resources their common goal is to establish a secret key, i.e. gain shared randomness.



Insecure quantum key distribution

This protocol is not secure because it cannot distinguish between a truthfully entangled state and a state prepared by a malicious adversary, Eve.

$$|\psi\rangle \propto (|00\rangle + |11\rangle)|e\rangle$$



$$|\phi\rangle \propto |00\rangle|e_0\rangle + |11\rangle|e_1\rangle$$



Secure qkd

The two previous cases could be distinguished by checking the correlations between measurement in different bases. For example, choosing X and Z as measuring bases, the expected correlations in the good state are:

$$\langle Z \otimes Z \rangle = 1$$

$$\langle X \otimes X \rangle = 1$$

While in the bad state:

$$\langle Z \otimes Z \rangle = 1$$

$$\langle X \otimes X \rangle = 0$$

By choosing randomly a subset of entangled states as tests for eavesdropping, the protocol is secure.



Discussion on quantum secret sharing

The approach presented for the generation of a shared key and the one used for quantum secret sharing are very similar:

- It is possible to apply LOSR formalism to this type of settings?
- What game can be created to study such scenario?
- What happen to the resources when Eve is introduced?



Obrigado pela atenção!

References

- [1] Schmid, David, Denis Rosset, and Francesco Buscemi. "The type-independent resource theory of local operations and shared randomness." *Quantum* 4 (2020): 262.
- [2] Wolfe, Elie, et al. "Quantifying Bell: The resource theory of nonclassicality of common-cause boxes." *Quantum* 4 (2020): 280.
- [3] Zjawin, Beata, et al. "Quantifying EPR: the resource theory of nonclassicality of common-cause assemblages." *arXiv preprint arXiv:2111.10244* (2021).
- [4] Hillery, Mark, Vladimír Bužek, and André Berthiaume. "Quantum secret sharing." *Physical Review A* 59.3 (1999): 1829.
- [5] Coecke, Bob, Tobias Fritz, and Robert W. Spekkens. "A mathematical theory of resources." *Information and Computation* 250 (2016): 59-86.