13

Quantum Resources

> In my life, I have prayed but one prayer: oh Lord, make my enemies ridiculous. And God granted it.
>
> – *Voltaire, letter to Étienne Noël Damilaville, 1767*

Although bankers on Wall Street can have pretty much whatever they want in whatever quantity they want, this chapter is for the rest of us cheapskates. Throughout this book, we have assumed that we, like quantum bankers, have had access to whatever processes we need in whatever quantity. For instance, in teleportation, we assumed we could obtain Bell states at will and do joint measurements on pairs of systems. For non-locality, we assumed we had lots of GHZ states around, so we could make enough measurements to see our assumptions about locality cave in. And for MBQC, we assumed that we had huge graph states around to implement universal quantum computation.

As you might expect, these things ain't cheap! Quantum processes involving multiple systems typically take some very special equipment and many hours to implement. So, when it comes to such *resources*, it behooves one to think about doing as much as possible with as little as possible. This is of course true not just for quantum states, but for any kind of resource: coal, oil, nuclear, wind, and solar energy; certain chemicals; or just a bit of affection.

What is important about all resources is what we can do with them. If we think of the benefits of resources (e.g. warm, comfy houses or secure communication) as being resources themselves, we see that pretty much all questions about resources boil down to the following two:

1. Can a given resource be converted into some other resource?
2. How much of resource X to do we need to obtain resource Y?

These are exactly the questions a *resource theory* aims to answer.

One place this idea of 'conversion of resources' appears very explicitly is in the study of chemical reactions, where one finds expressions like these:

$$\begin{aligned} 6\mathrm{CO}_2 + 6\mathrm{H}_2\mathrm{O} + \text{light} &\longrightarrow \mathrm{C}_6\mathrm{H}_{12}\mathrm{O}_6 + 6\mathrm{O}_2 \\ \mathrm{C}_6\mathrm{H}_{12}\mathrm{O}_6 &\longrightarrow 2\mathrm{C}_2\mathrm{H}_5\mathrm{OH} + 2\mathrm{CO}_2 \end{aligned}$$

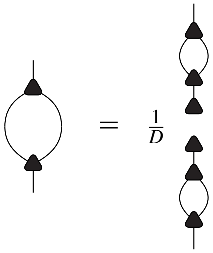
Such an expression tells us that we can convert the stuff on the LHS to the stuff on the RHS. Even though the expression doesn't provide any details about how this conversion is actually done, it does provide us with two very useful pieces of information. First, it specifies how much we need of one resource to get a certain amount of another, and second, it tells us all the resources a given resource can be converted into. Clearly, the more things it can be converted into, the more desirable it is.

This is true for any kind of resource, including the quantum examples we gave above. We listed several entangled states that were good for various tasks, but if some entangled state can be easily converted into any other entangled state, then clearly it should be at the top of the food chain. This idea is captured by the *resource theory of entanglement*.

Of course, entanglement is not the only quantum resource one may care about. Given that real-world devices tend to implement quantum processes in fairly noisy and unreliable ways, it is very natural to study *purity* of quantum states as a resource theory. Other resources are even more subtle. For instance, when doing quantum key distribution, sharing a reference frame, i.e. agreeing on what the Z- and the X-spiders are, is a key resource.

But what exactly is a resource theory? It's a process theory, of course! More specifically, it's a process theory with a very special interpretation: the types of the process theory represent resources and the processes represent conversions. From a process theory, we can derive a *convertibility relation*, which in turn tells us about the *conversion rates* of resources, what good (cost) *measures* should be, whether a theory has *catalysts*, etc.

Along the way, we'll make two interesting observations. When we study the resource theories of purity and entanglement, we'll see that, even though the conversion relations of these theories seem to be 'quantitative', we can still prove strong characterisation theorems diagrammatically. Moreover, when we study entanglement of three qubits, we'll see that each of the maximal *entanglement classes* is captured by some kind of spider. One of these spiders is very familiar by now, since it's been the main character of the past five chapters. However, the other kind of spider is quite different. Rather than happily fusing with its neighbours, it explodes:



13.1 Resource Theories

A resource theory is really just a process theory, except for the wording.

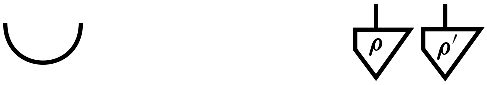
Definition 13.1 A *resource theory* is a process theory where the types are called *resources*, and the processes are called *resource conversions*.

This actually makes it very different!

For example, we could define a resource theory called **food**, where the systems are ingredients and the processes are ways to prepare food, i.e. convert one food into an other food. A raw carrot can be converted into a boiled carrot, or a boiled carrot and a cup of broth can be converted into soup. Another example is **energy**, whose resources are forms of energy and whose resource conversions turn one form of energy into another: coal into heat, heat into electricity, electricity into work, etc.

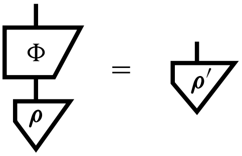
13.1.1 Free Processes

For process theories such as **quantum processes**, all states of a given type have been treated on equal footing. However, clearly there is a big difference between the following two states in terms of what one can do with them:



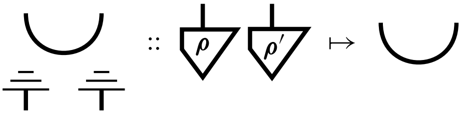
For example, the first one allows one to do teleportation, while the second one doesn't. To capture this difference within a process theory we will treat the states themselves as different types. So, states in a process theory like **quantum processes** will become types in the resource theory we construct. Hence, we get some types (i.e. resources) that are useful for teleportation and others that are totally useless for teleportation.

They will be related by means of the processes (i.e. resource conversions) in our theory. But what should these be? One choice would be to take the conversions from a resource ρ to another resource ρ' to be all those processes in the original process theory that transform ρ into ρ':



(13.1)

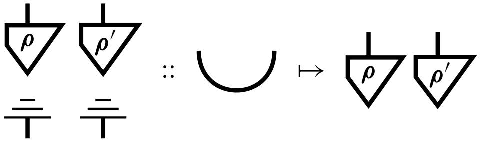
However, that wouldn't give us anything useful. For example, if we care about entanglement, we want to be able to learn from the structure of the resource theory **entanglement** that the Bell state is a much more valuable resource than any separable state. But if we include all processes as resource conversions, we could just use this process:



(13.2)

to turn any state, including the separable ones, into a Bell state!

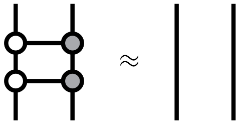
So, we should distinguish between those processes that allow us to 'create' more of our resource (in this case, entanglement) and those that do not. For example the quantum process:



should be allowed, since it can only destroy entanglement, while the quantum process (13.2) should not be allowed, since it can create entanglement where there was none before.

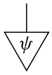
A process that only decreases (or preserves) the resource of interest is called a *free process*, which is meant to suggest that the other processes are 'expensive', so we want to avoid using them. If two processes are free, then their compositions should also be free, so free processes always form a subtheory of a resource theory.

Remark 13.2 On the other hand, non-free processes typically do not form a process theory. For instance, the CNOT gate can introduce new entanglement, so it should not be free, but doing a CNOT-gate twice:



is just the same as doing nothing, which is always free!

Note that *free states* are processes in **F**:



that convert 'nothing' into that state itself. This perfectly matches the idea that 'free' means getting something for nothing.

We can capture all of this by specialising Definition 13.1 to those resource theories that arise from an underlying process theory.

Definition 13.3 Given a process theory **P** together with a subtheory **F** of *free processes*, we define the corresponding resource theory:

$$\textbf{P-states/F}$$

to be the process theory that has:

- the states of **P** as its types, and
- the processes in **F** that convert ρ into ρ' as its processes.

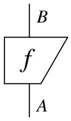
The beauty of such resource theories is that one never has to say exactly what it means for a state to have 'X amount of a resource'. For instance, as we'll see later, asking 'how much' entanglement a state has is not really a well-defined question, because states can be entangled in different, inequivalent ways. On the other hand, once we say what our free processes are, we can immediately start comparing resources.

13.1.2 Comparing Resources

Definition 13.4 For a resource theory **R**, resource A can be *converted* into resource B, which we write as follows:

$$A \succeq B$$

if and only if there exists a process in **R** from A to B:

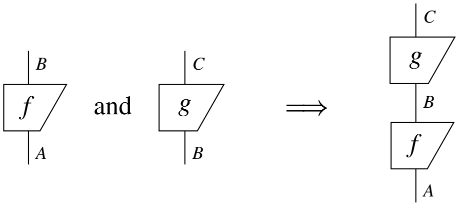


Two resources A and B are *equivalent* if $A \succeq B$ and $B \succeq A$, in which case we write:

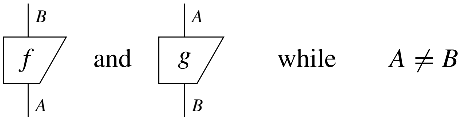
$$A \simeq B$$

This definition has three immediate consequences. First, that $\succeq$ is *reflexive*, i.e. $A \succeq A$, since the identity process always converts A to itself:

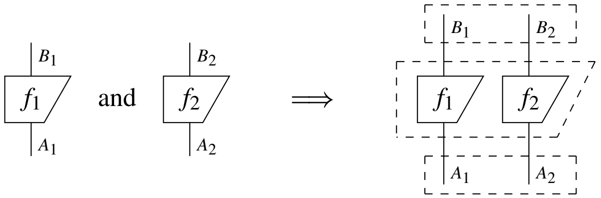
It is also *transitive*, i.e. if $A \succeq B$ and $B \succeq C$, then $A \succeq C$, by $\circ$-composition:



These two conditions make the relation $\succeq$ into a *preorder*. However, $\succeq$ does not need to be a *partial order*, which is a preorder that is additionally *anti-symmetric*, i.e. if $A \succeq B$ and $B \succeq A$ then $A = B$, because it's perfectly reasonable to have resources that are interconvertible but not equal. That is, there can exist:



In addition to being a preorder, $\succeq$ plays well with $\otimes$:



So in summary we have the following theorem.

Theorem 13.5 For R the set of resources in a resource theory:

$$(R, \succeq, \otimes, I)$$

forms a *preordered monoid*. That is, $(R, \otimes, I)$ forms a monoid:

$$(A \otimes B) \otimes C = A \otimes (B \otimes C) \qquad\qquad A \otimes I = A = I \otimes A$$

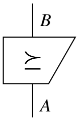
$(R, \succeq)$ forms a preorder:

$$A \succeq A \qquad\qquad A \succeq B \text{ and } B \succeq C \implies A \succeq C$$

and these two structures are compatible:

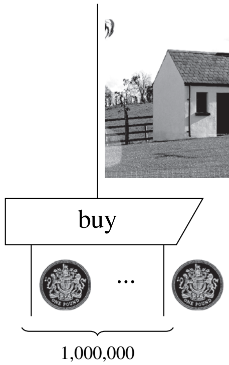
$$A_1 \succeq B_1 \text{ and } A_2 \succeq B_2 \implies A_1 \otimes A_2 \succeq B_1 \otimes B_2$$

Remark 13.6 Equivalently, a preordered monoid can be defined as a process theory where there exists at most one process of any given type, which we could write like this:



The presence of such a process then simply witnesses the fact that $A \succeq B$. So, the passage from a resource theory to a preordered monoid $(R, \succeq, \otimes)$ can be seen as passing from a big process theory, with lots of different processes, to a much smaller one, where we only remember whether there were any processes of a given type or not.

Very early on in this book we saw that process theories put $\circ$-composition and $\otimes$-composition of processes on the same footing. Similarly, convertibility of resources is tightly intertwined with $\otimes$-composition of systems. While one may not be able to convert a single pound coin into a home in Oxford, one million or so of those would get you something:



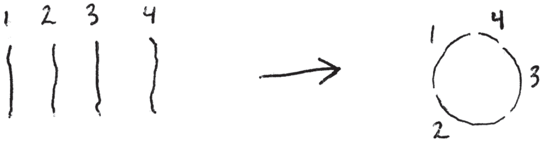
Hence, the addition of ⊗ gives us the ability to trade quantities of one resource for quantities of another. In other words, we can express the rate at which one resource can be converted into another.

Definition 13.7 For resources A and B in a resource theory, the *conversion rate* is given by:

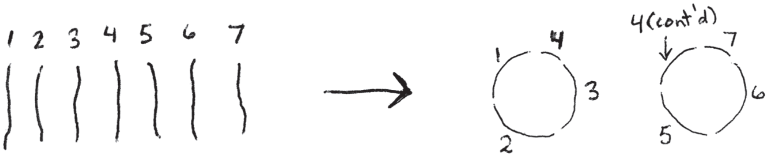
$$r(A \succeq B) \ := \ \text{supremum}\left\{ \frac{N}{M} \ \middle| \ \underbrace{A \otimes \cdots \otimes A}_{M} \ \succeq \ \underbrace{B \otimes \cdots \otimes B}_{N} \right\}$$

If we consider a resource theory just containing the process above, the conversion rate from pounds to Oxford houses is $\frac{1}{1{,}000{,}000}$. So, a pound can be converted into one one-millionth of an Oxford house. What a bargain!

Remark* 13.8 Since the conversion rate is computed as a supremum, this can in general be irrational. Take, for example, a theory where resources are little strings that we can cut and arrange into shapes. Then, we need 4 strings of length 1 to make a circle of diameter 1:



but only 7 strings to make 2 circles:



and 10 strings to make 3 circles, 13 to make 4, and so on. If we carry on to infinity, we approach the optimal rate, which is given by the supremum:

$$\text{supremum}\left\{\frac{1}{4},\frac{2}{7},\frac{3}{10},\frac{4}{13},\ldots\right\} = \frac{1}{\pi}$$

So, we can optimally produce one circle for every π strings.

The convertibility relation totally forgets what the processes in a resource theory are and remembers only if such a process exists. Nevertheless, it already contains a great deal of information about the structure of a resource theory. For example, it tells us whether our resource theory has *catalysts*, that is, resources C for which:

$$A \otimes C \succeq B \otimes C \quad \text{while} \quad A \not\succeq B$$

It also tells us if resources are *quantity-like*:

$$\left.\begin{array}{c} A_1 \otimes A_2 \simeq B_1 \otimes B_2 \\ A_1 \succeq B_1 \end{array}\right\} \implies B_2 \succeq A_2$$

i.e. resources behave like ‘quantities of stuff’, where the whole is just the sum of the parts. Similarly, it tells us if resources are *non-interacting*:

$$A \succeq B_1 \otimes B_2 \implies \exists A_1, A_2 : \left\{\begin{array}{l} A \simeq A_1 \otimes A_2 \\ A_1 \succeq B_1 \\ A_2 \succeq B_2 \end{array}\right.$$

which means that whenever a resource gives us multiple things, we can ‘cut it up’ and produce each of those things independently.

Exercise 13.9 Prove that if a resource theory is quantity-like and non-interacting, then it is also *catalysis-free*:

$$A \otimes C \succeq B \otimes C \implies A \succeq B$$

13.1.3 Measuring Resources

Physicist like real numbers, and so do many others. There is nothing wrong with that, as long as it doesn’t become an obsession. When it comes to gauging the value of a resource, numbers might be part of the story, but they can never be the whole story, because they often miss vital information. This stems from the fact that real numbers form not only a partial order, but in fact a *total order*. That is, for any two real numbers a and b we have either:

$$a \geq b \qquad\qquad \text{or} \qquad\qquad b \geq a$$

Hence, if we want to compare two resources by assigning them real numbers, it will always be the case that:

$$A \succeq B \qquad\qquad \text{or} \qquad\qquad B \succeq A$$

But what if neither of these things is true?

A key example comes from entanglement. While using numbers to measure entanglement works okay for a pair of qubits, we'll see in Section 13.3.2 that as soon as we have a slightly more complicated system (e.g. three qubits), this breaks down precisely because incomparable states start to appear. Rather than giving us 'more' or 'less' entanglement, these states give us different kinds of entanglement. However, this didn't stop people from coming up with a whole zoo of ways to measure entanglement with real numbers, which work well for comparing some states, but not others.

On the other hand, when it comes to measuring impurity of quantum states, there is a very famous number called *entropy*, which does a pretty good job of telling us how pure a state is.

But before we get there, how do we go about assigning numbers to resources in a consistent way? We begin by making the positive real numbers $\mathbb{R}_{\geq 0}$ into a preordered monoid. We always let $\succeq$ be the usual ordering on positive real numbers, but then for $\otimes$, we have many choices. For instance, we can take $\otimes$ to be the sum of two positive real numbers. Then clearly:

$$a \geq a' \text{ and } b \geq b' \quad\Longrightarrow\quad a+b \geq a'+b'$$

But we can also use:

$$\max(a,b) \;:=\; \begin{cases} a & \text{if } a \geq b \\ b & \text{if } b \geq a \end{cases}$$

Exercise 13.10 Show that max is associative:

$$\max(a, \max(b,c)) \;=\; \max(\max(a,b)c)$$

and compatible with $\geq$, that is:

$$a \geq a' \text{ and } b \geq b' \quad\Longrightarrow\quad \max(a,b) \geq \max(a',b')$$

These two choices give us two different preordered monoids:

$$\mathcal{R}^{+} := (\mathbb{R}_{\geq 0}\,,\,\geq\,,\,+\,,\,0) \qquad\qquad \mathcal{R}^{\max} := (\mathbb{R}_{\geq 0}\,,\,\geq\,,\,\max\,,\,0)$$

and two corresponding kinds of measures.

Definition 13.11 Given a resource theory, an *additive measure* is a function:

$$M : (R, \succeq, \otimes) \to \mathcal{R}^{+}$$

where:

$$A \succeq B \implies M(A) \geq M(B) \qquad M(A \otimes B) = M(A) + M(B)$$

Similarly, a *supremal measure* is a function:

$$M : (R, \succeq, \otimes) \to \mathcal{R}^{\max}$$

where:

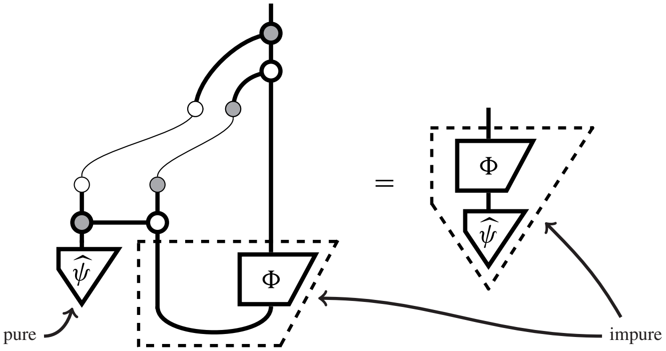
$$A \succeq B \implies M(A) \geq M(B) \qquad M(A \otimes B) = \max(M(A), M(B))$$

A measure gives us only partial information about a resource theory and its convertibility relation $\succeq$. Notably, measures can be used to prove that a given resource cannot be converted into another, for if $M(A) < M(B)$, then it must not be the case that $A \succeq B$. However, the converse isn't true. It could still be the case that $M(A) \geq M(B)$ even when no conversion $A \succeq B$ exists.

On the other hand, numbers are (usually) a lot easier to compare than the resources they came from, so in the rare cases that a measure does in fact totally capture $\succeq$, we are happy.

13.2 Purity Theory

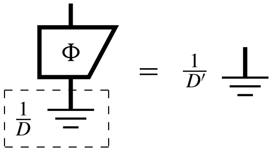
Most of the time in quantum theory, we value states and processes that are as pure as possible. For example, the Bell state in quantum teleportation is valuable not just because it is entangled, but also because it is pure. If instead we use an impure state in teleportation, then also the resulting state will inherit that impurity:



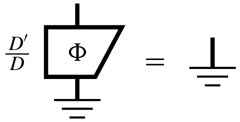
Introducing a bit of impurity like this is okay, and in fact unavoidable, since pure states represent an ideal that is impossible to achieve in practice. However, if we introduce too much impurity like this, pretty soon we'll just have garbage, e.g. a maximally mixed state. Hence purity is a vital resource. In this section, we will define a resource theory for purity and show how the purity of states can be compared and quantified.

13.2.1 Comparing Purity

If it is purity that we cherish, then the free processes should be precisely those that cannot create new purity. In particular, they should preserve maximal impurity:



or equivalently:



(13.3)

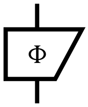
where D is the dimension of Φ's input and D' the dimension of its output.

Definition 13.12 Let **unital quantum maps** be the subtheory of **causal quantum maps** obtained by restricting to processes satisfying (13.3). Then:

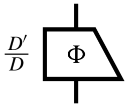
purity := **causal quantum states/unital quantum maps**

The following is an alternative characterisation of unital quantum maps.

Proposition 13.13 A quantum map Φ is unital if and only if:



and



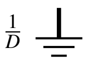
are both causal.

Proof Unital quantum maps are causal by definition, and if we take the adjoint of (13.3), the resulting equation is causality of $\frac{D'}{D}\,\Phi$. □

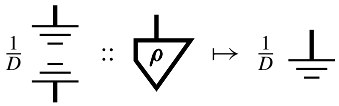
So in particular, if a quantum map Φ has input and output types with the same dimension, Φ is unital precisely when Φ and the adjoint of Φ are both causal. Hence, if a quantum map is pure and unital, the map and its adjoint must both be isometries, so the following characterisation is immediate.

Corollary 13.14 A pure quantum map is unital if and only if it is unitary.

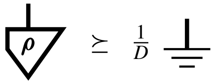
As a result, the only pure unital maps must go between systems of the same dimension, so in particular there are no pure unital states or effects. Going beyond pure maps, there is precisely one unital state:



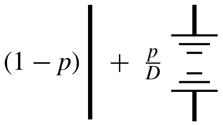
This follows from the fact that discarding is the unique causal effect. Consequently, the maximally mixed state is the unique free state in **purity**. One therefore expects that it can be obtained via conversion from any other state. This is indeed possible, since the process that discards a state and replaces it with the maximally mixed state:



is clearly unital, so it is a free process in **purity**. Hence:

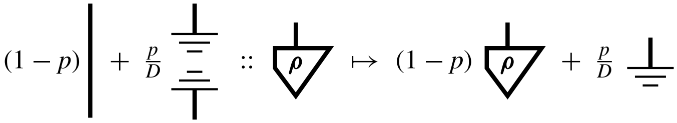


Less drastically, the process that adds some noise to a given state:

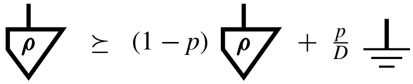


(13.4)

is also a free process for **purity**, which we'll call a *noise map*. Since:

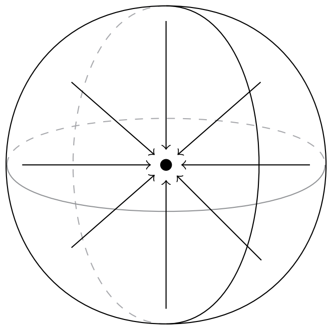


it follows that:

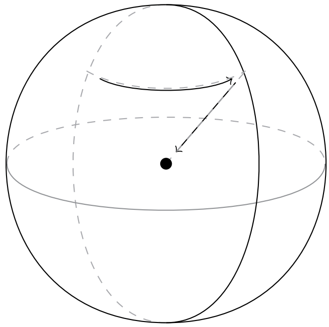


Remark 13.15 In quantum information literature, and especially in quantum optics, a noise map is often referred to as a *depolarizing channel*.

So, which states can be converted to others via unital quantum maps? If we initially restrict to qubits, we can start to get a picture of this by looking at the geometry of the Bloch ball. We already know that unitaries and noise maps are free processes, so we can see how these act on the Bloch ball. Since a noise map simply mixes its input state with the maximally mixed state, it shrinks any point in the Bloch ball towards the centre:

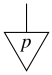


We already know that unitaries give rotations of the Bloch ball, so by composing a noise map with a unitary, any point on the Bloch ball can be taken to any other point closer (or equally close) to the centre of the Bloch ball:

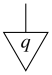


Hence, if $\boldsymbol{\rho}'$ is not further away from the centre of the Bloch sphere than $\boldsymbol{\rho}$, then $\boldsymbol{\rho} \succeq \boldsymbol{\rho}'$ in **purity**. In fact, the converse is also true. Rather than proving this directly, we can actually give a characterisation for this convertibility relation that works in all dimensions. We will make use of the following preorder.

Definition 13.16 For probability distributions:

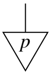


$$\leftrightarrow \begin{pmatrix} p^1 \\ \vdots \\ p^n \end{pmatrix}$$

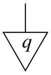


$$\leftrightarrow \begin{pmatrix} q^1 \\ \vdots \\ q^n \end{pmatrix}$$

we say that *p majorizes q*, written:



$$\succeq$$



if, after rearranging the numbers in each probability distribution in decreasing order:

$$p^1 \geq p^2 \geq \cdots \geq p^n \qquad\qquad q^1 \geq q^2 \geq \cdots \geq q^n$$

we have:

$$\begin{cases} p^1 & \geq & q^1 \\ p^1+p^2 & \geq & q^1+q^2 \\ & \vdots & \\ p^1+\cdots+p^n & \geq & q^1+\cdots+q^n \end{cases} \tag{13.5}$$

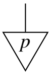
It is straightforward to check that this gives a preorder, which we call the *majorization order*. It is not a partial order since the same elements in different order, e.g. point distributions, are equivalent with respect to majorization:

$$\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix} \simeq \begin{pmatrix}0\\1\\\vdots\\0\end{pmatrix} \simeq \cdots \simeq \begin{pmatrix}0\\0\\\vdots\\1\end{pmatrix}$$

while obviously being non-equal. Furthermore, even if we consider probability distributions up to reordering of elements, this does not give a total order, since, e.g.:

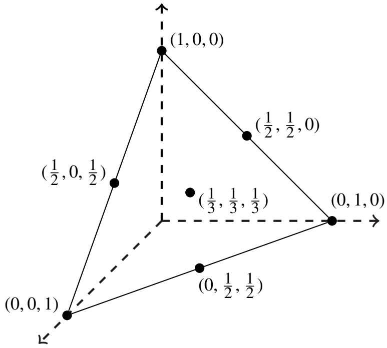
$$\begin{pmatrix}\frac{1}{2}\\\frac{1}{2}\\0\end{pmatrix} \not\succeq \begin{pmatrix}\frac{3}{4}\\\frac{1}{8}\\\frac{1}{8}\end{pmatrix} \qquad\qquad \begin{pmatrix}\frac{3}{4}\\\frac{1}{8}\\\frac{1}{8}\end{pmatrix} \not\succeq \begin{pmatrix}\frac{1}{2}\\\frac{1}{2}\\0\end{pmatrix}$$

Exercise 13.17 Probability distributions:

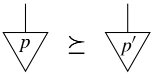


$$\leftrightarrow \quad \begin{pmatrix}p^1\\p^2\\p^3\end{pmatrix}$$

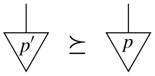
can be represented on a triangle by taking the p^is to be coordinates:


(1, 0, 0)
$(\frac{1}{2}, \frac{1}{2}, 0)$
$(\frac{1}{2}, 0, \frac{1}{2})$
$(\frac{1}{3}, \frac{1}{3}, \frac{1}{3})$
(0, 1, 0)
$(0, \frac{1}{2}, \frac{1}{2})$
(0, 0, 1)

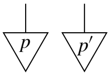
For an arbitrary probability distribution p', depict the region on the triangle of all probability distributions p for which we have:



and the region for which we have:

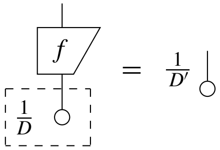


Majorization gives us a preorder, which we can turn into a preordered monoid by taking ⊗ to be the usual parallel composition of probability distributions:



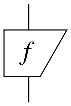
To show that this is compatible with the majorization ordering, it is helpful to give an alternative characterisation of majorization. This alternative characterisation is closer to the soul of resource theories in that it presents majorization as a conversion relation, namely, convertibility by means of doubly stochastic maps.

Definition 13.18 *Doubly stochastic maps* are classical processes f (cf. Definition 8.11) such that:

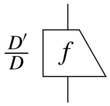


(13.6)

Or equivalently, they are classical maps f where:



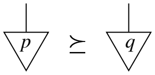
and



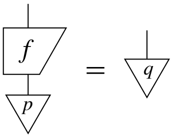
are both causal.

Proposition 13.19 The following are equivalent:

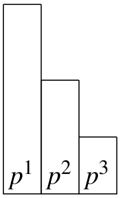
- p majorizes q:



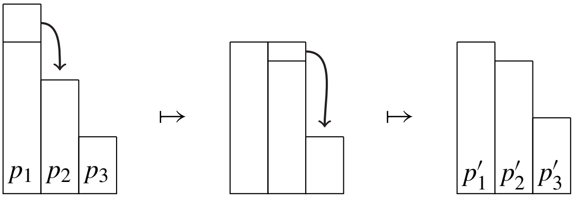
- There exists a doubly stochastic map such that:



Proof (sketch) The majorization preorder admits a ‘tower of Hanoi’ interpretation, where $p^1, \ldots, p^n$ represent different stacks:



To realise conversion, one first 'moves' $p^1 - q^1$ from p^1 to p^2, so that p^1 becomes q^1, then one moves $(p^1 + p^2 - q^1) - q^2$ from $p^1 + p^2 - q^1$ to p^3, so that p^2 has become q^2, and so on, e.g.:



The fact that one can do so requires:

$$p^1 - q^1 \geq 0 \qquad p^1 + p^2 - q^1 - q^2 \geq 0 \quad \ldots \quad p^1 + \cdots + p^{n-1} - q^1 - \cdots - q^{n-1} \geq 0$$

which, after moving all the numbers q^i to the RHS of the inequalities, exactly recovers the majorization condition. Since the composition of doubly stochastic maps is again doubly stochastic, it suffices to show the 'Hanoi moves' can be realised by doubly stochastic maps, and vice versa. We leave this as an exercise. □

Exercise 13.20 Show that whenever p majorizes q, there exists a doubly stochastic map sending p to q by giving the matrices that realise the 'Hanoi moves' in the above proof. Hint: use the fact that a matrix for a generic 2×2 doubly stochastic map is of the form:

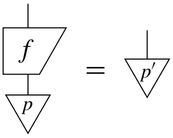
$$\begin{pmatrix} 1-x & x \\ x & 1-x \end{pmatrix}$$

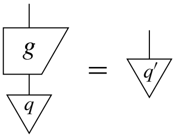
where $0 \leq x \leq 1$. Conversely, show that for f a doubly stochastic map and p a probability distribution, $p \succeq f \circ p$ in the majorization preordering as defined in (13.5).

Thus we have the following proposition.

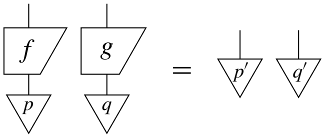
Proposition 13.21 Majorization, together with ⊗-composition, makes the set of probability distributions for a classical system into a preordered monoid.

Proof If for doubly stochastic maps f and g we have:





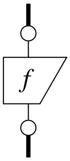
i.e. $p \succeq p'$ and $q \succeq q'$, then:



so since $f \otimes g$ is evidently also doubly stochastic, $p \otimes q \succeq p' \otimes q'$. □

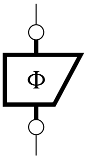
Unital quantum maps are characterised by the fact that they as well as their adjoints are causal, and doubly stochastic maps are characterised by the fact that they as well as their adjoints are causal. This looks like a theorem waiting to happen, and indeed these two concepts are mutually related by encoding/measurement.

Theorem 13.22 If a classical map f is doubly stochastic, then:



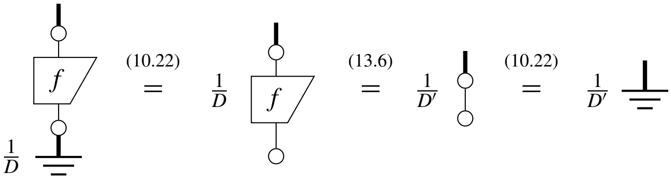
(13.7)

is a unital quantum map, and if a quantum map Φ is unital, then:



is a doubly stochastic (classical) map.

Proof The proof directly follows from the fact that measure and encode both are causal, and each other's adjoints. For example, unitality of (13.7) can be established as follows:

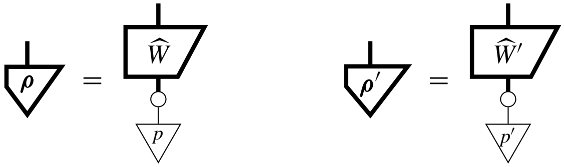


□

Remark 13.23 We have tried to conform with standard terminology, but it would of course have made perfect sense to call doubly stochastic maps, instead, ‘unital classical maps’ or to call unital quantum maps, instead, ‘doubly causal quantum maps’.

This correspondence between unital quantum maps and doubly stochastic maps translates into a correspondence between the convertibility of quantum states and the convertibility of probability distributions. The key bridge here is the spectral theorem, which, thanks to Proposition 8.56, lets us express a quantum state in terms of a probability distribution.

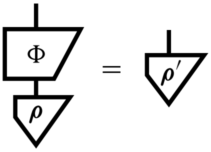
Lemma 13.24 For quantum states ρ and ρ', which decompose as:



(13.8)

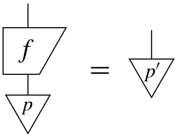
for unitaries $\widehat{W}$ and $\widehat{W}'$ and probability distributions p and p', the following are equivalent:

- there exists a unital quantum map Φ such that:



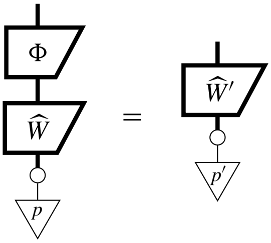
(13.9)

- there exists a doubly stochastic map f such that:

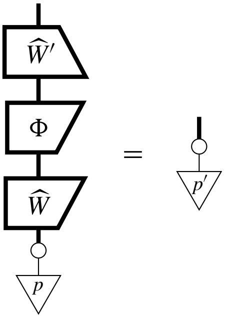


(13.10)

Proof Assume first that ρ and ρ' are related by a unital quantum map Φ as in (13.9). Then, by (13.8):

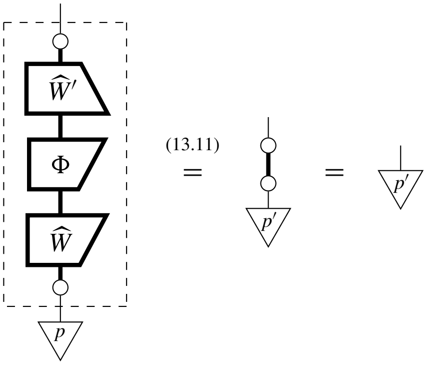


We can then use unitarity to move $\widehat{W}'$ to the LHS:

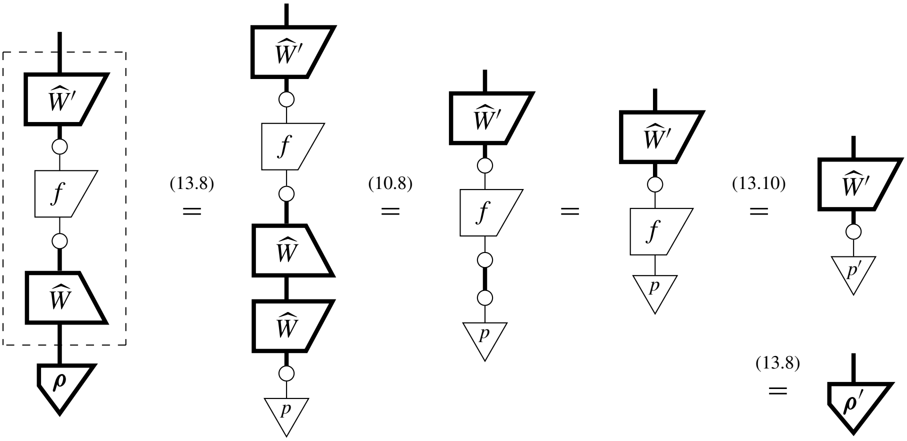


(13.11)

Then, measuring both sides yields:



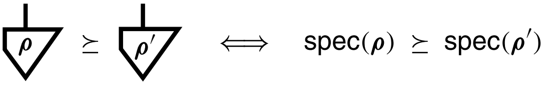
By Proposition 13.22, the map applied in the LHS to p is doubly stochastic, since all quantum maps involved are unital. Conversely, assuming p and p' are related by a doubly stochastic map as in (13.10), it follows that:



where, again by Proposition 13.22, the quantum map applied in the LHS to $\boldsymbol{\rho}$ is unital. □

Using more traditional notation, we refer to the probability distribution p related to the state $\boldsymbol{\rho}$ in equation (13.8) as the *spectrum* of $\boldsymbol{\rho}$, written $\mathsf{spec}(\boldsymbol{\rho})$ (cf. Definition 5.73). Together, Proposition 13.19 and Lemma 13.24 yield the following characterisation of convertibility in **purity** in terms of majorization.

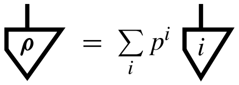
Theorem 13.25 The conversion relation of **purity** for the states of a fixed quantum system of arbitrary dimension is given by:


ρ
$\succeq$
ρ'
$\iff$
$\mathsf{spec}(\boldsymbol{\rho}) \succeq \mathsf{spec}(\boldsymbol{\rho}')$

where the second $\succeq$ is the majorization preordering.

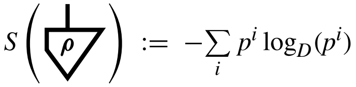
13.2.2 Measuring (Im)purity

A typical measure of purity is the *von Neumann entropy* of a quantum state. This is computed as follows. First, use Corollary 6.68 to decompose ρ over an ONB of pure states:



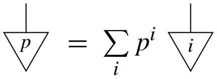
(13.12)

Then, the von Neumann entropy is computed as:

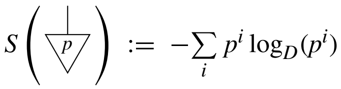


where $\log_D(p^i)$ is the logarithm of p^i for some fixed base D, which is typically taken to be the dimension of a single system, e.g. 2 for qubits. In that case, the entropy varies from 0 for pure states to 1 for the maximally mixed state.

Remark 13.26 For a classical probability distribution:

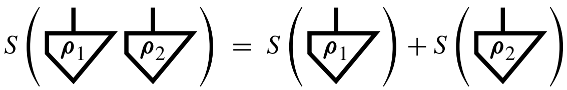


the quantity:



is the *Shannon entropy*. Since every quantum state diagonalises, it encodes a probability distribution with respect to some ONB. The von Neumann entry is then the Shannon entropy of that encoded probability distribution.

Now, this almost gives us an additive measure, in the sense of Definition 13.11. Indeed, it satisfies:

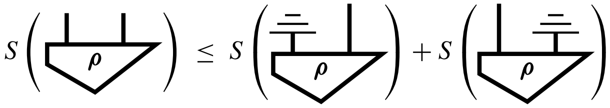


(13.13)

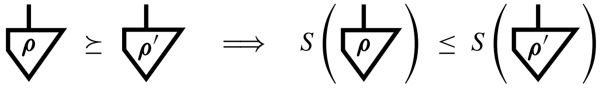
which follows straightforwardly from the fact that:

$$\log_D(p^i q^j) = \log_D(p^i) + \log_D(q^j)$$

Moreover, for general states of two systems, we have:



with equality if and only if $\boldsymbol{\rho}$ is separated. However, von Neumann entropy is not a measure of *purity*, but rather a measure of *impurity*. That is, for $\succeq$ the purity preorder, we have:



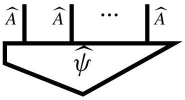
Remark 13.27 Given that mixing stands for introducing a lack of knowledge, this means that the maximally mixed state is the 'least informative' state, in contrast to pure quantum states, which are 'maximally informative'. Thus there is a close connection between mixedness/entropy of quantum state and its information content. Studying this and related issues is an important part of *quantum information theory*.

13.3 Entanglement Theory

While entanglement is a very different concept from purity, involving at least two systems, when characterising the conversion relation of the resource theory of entanglement, we'll encounter many of the same ingredients.

We'll actually study two distinct resource theories of entanglement, one that is roughly on par with **purity** in terms of how fine-grained the conversion relation becomes, and one that is much coarser. The latter is so coarse in fact, that for two- and three-qubit states, it yields only a finite number of equivalent resources. Along the way, we will see that, that while 'entanglement' is a single word, it can stand for very different things.

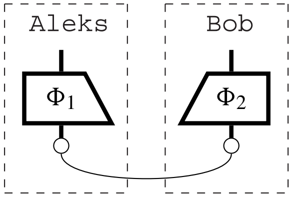
Throughout this section we consider pure states of the form:



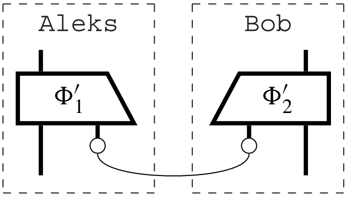
i.e. states whose type consists of two or more copies of the same system. This is not an essential assumption, but it simplifies things a bit.

13.3.1 LOCC Entanglement

If it is entanglement that we cherish, then the free processes should be the ones that create no new entanglement. We already saw that disentangled states are of the form:



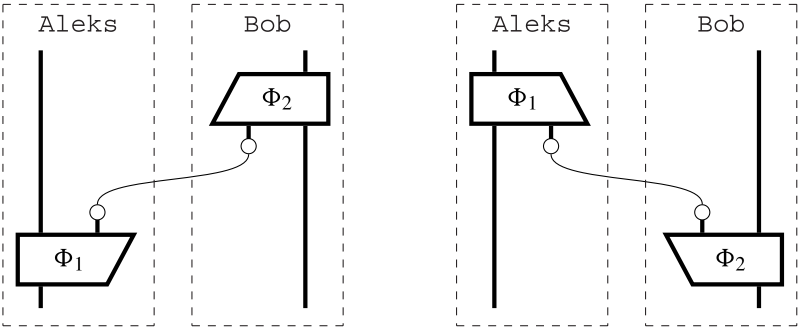
and given the discussion in Section 8.3.5 one may be tempted to think that the kind of processes that don't create any entanglement are those of the form:



(13.14)

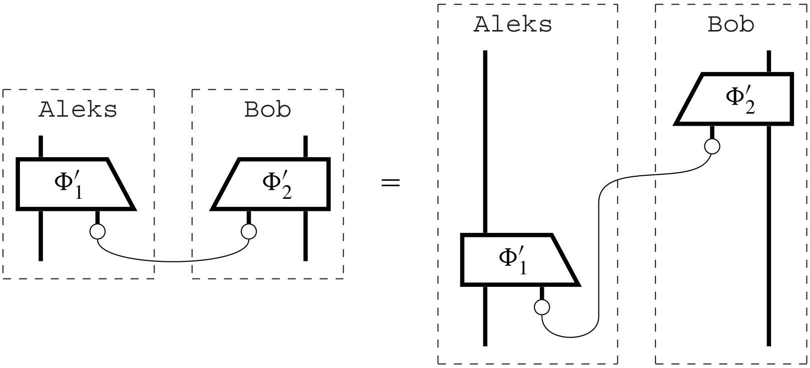
However, in that discussion we ignored causality, for the simple reason that states are always causal, up to a number. However, for processes, causality is a non-trivial requirement. Within the context of resource theories, it is important that one can actually realise 'free' processes, since otherwise there isn't much free about them! Non-causal quantum maps can only be realised non-deterministically, and if we're unlucky, rather than converting our resource we may as well have lost it all together. Hence, we'll restrict to only causal free processes for the time being.

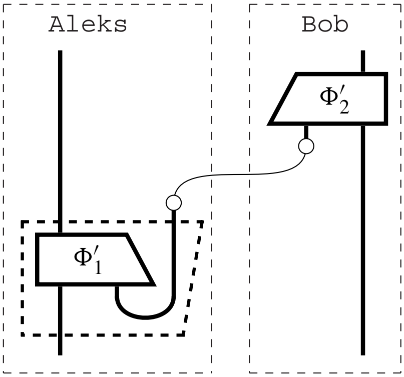
Once causality enters the picture, we should distinguish whether (i) Aleks and Bob share a classical cup; (ii) Aleks sends some classical data to Bob; or (iii) Bob sends some classical data to Aleks. So, in addition to (13.14), we should also consider processes of the form:



(13.15)

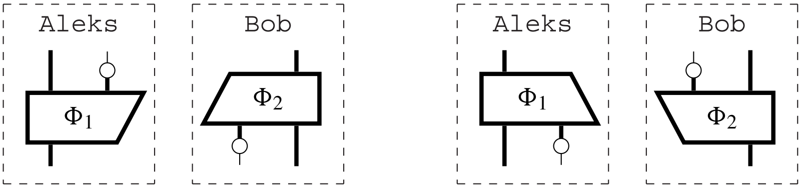
Luckily, once we consider these two forms, we no longer need to think about (13.14), because this arises as a special case of Aleks sending classical data to Bob (or vice versa):



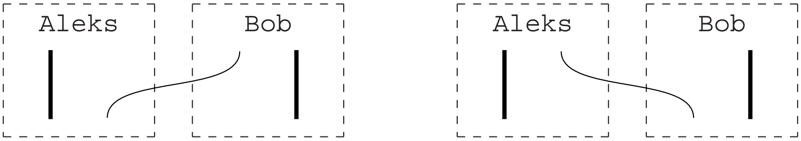
$=$ 

Quantum processes of the forms (13.15), and compositions thereof, are referred to as *LOCC-operations*, for the reason that they can be decomposed in two kinds of basic processes, namely:

- Local (causal) Operations :=



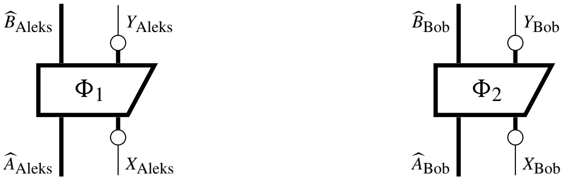
- Classical Communication :=



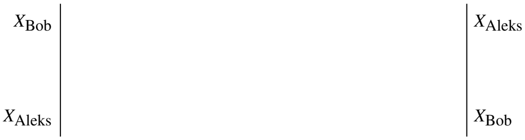
Now, throughout this book we have drawn dashed grey boxes with names of people (or extinct birds) attached to them. We never really said what this means formally. However, this is really simple. We can capture this by creating a new process theory, called **quantum processes²**, which has exactly the same processes, but two copies of each (classical and quantum) type, one for Aleks and one for Bob:

$$\widehat{A} \rightsquigarrow (\widehat{A}_{\text{Aleks}}\, , \widehat{A}_{\text{Bob}}) \qquad\qquad X \rightsquigarrow (X_{\text{Aleks}}\, , X_{\text{Bob}})$$

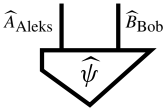
In this new process theory, local operations are then just the quantum processes that only connect Aleks' types to Aleks' types and Bob's to Bob's, e.g.:


$\widehat{B}_{\text{Aleks}}$
Y_{Aleks}
Φ_1
$\widehat{A}_{\text{Aleks}}$
X_{Aleks}
$\widehat{B}_{\text{Bob}}$
Y_{Bob}
Φ_2
$\widehat{A}_{\text{Bob}}$
X_{Bob}

Then, classical communication is just a classical wire, where we label one end by Aleks' type and the other by the corresponding type for Bob (or vice versa):



and **pure quantum states²** is the set of states of the form:

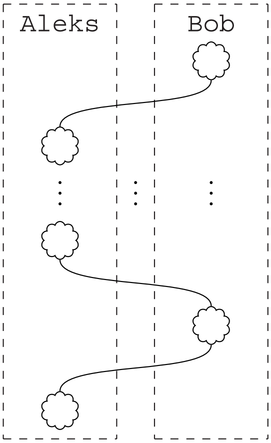


Of course, the same can be done for any number of agents.

Definition 13.28 Let **locc²** be the subtheory of **quantum processes²** obtained by restricting to processes corresponding to local operations, classical communication, and compositions thereof. Then:

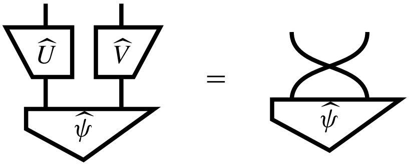
$$\textbf{LOCC entanglement}^{\mathbf{2}} \;:=\; \textbf{pure quantum states}^{\mathbf{2}}/\textbf{locc}^{\mathbf{2}}$$

So general quantum processes that don't create entanglement involve a game of ping-pong of classical communication between the two agents:



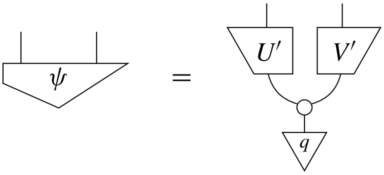
How long does this game have to go on in order to obtain the most general kind of conversions? Fortunately, one single use of classical communication already does the job, since the two forms (13.15) are in fact interchangeable. To show this, we first observe that we can interchange the roles of the two systems of a bipartite state via unitaries.

Lemma 13.29 For any pure bipartite state $\widehat{\psi}$ there exist unitaries $\widehat{U}$ and $\widehat{V}$ that swap the two systems:

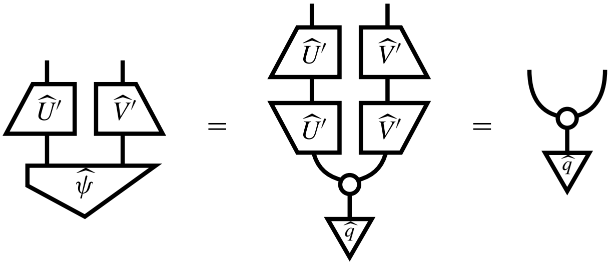


(13.16)

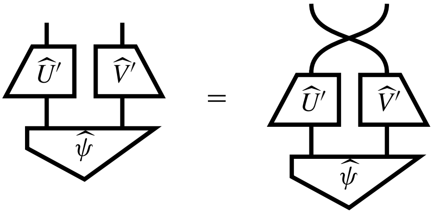
Proof Applying the singular value decomposition from Exercise 8.50 (which relies on the fact that the two systems are the same) to ψ gives:



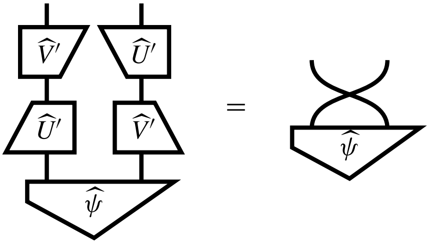
for unitaries U' and V'. Then:



Since the RHS is invariant under swapping, we have:



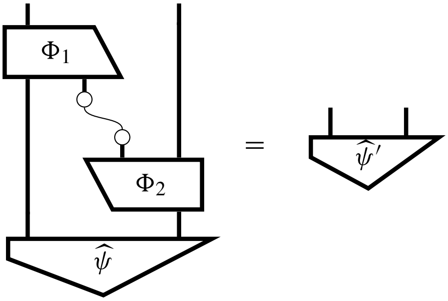
Moving all of the unitaries to the LHS then completes the proof:



□

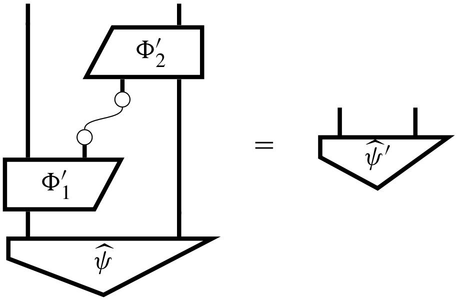
Importantly, to realise this swapping we need only local operations. As a consequence of this ‘local swapping’, we get the following.

Proposition 13.30 There exist Φ_1 and Φ_2 such that:



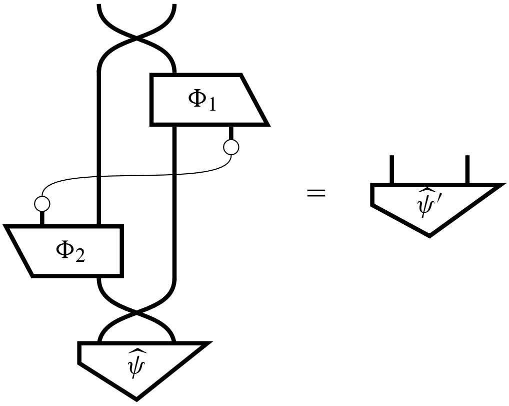
(13.17)

if and only if there exist Φ'_1 and Φ'_2 such that:

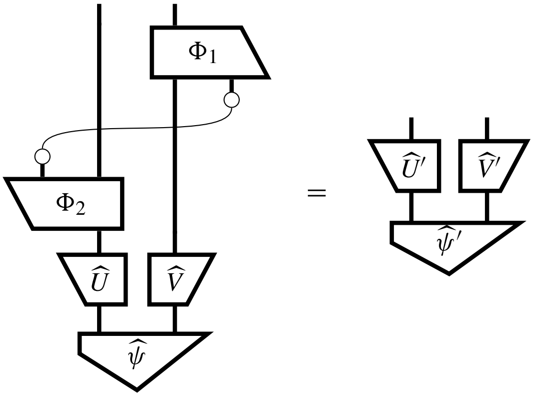


(13.18)

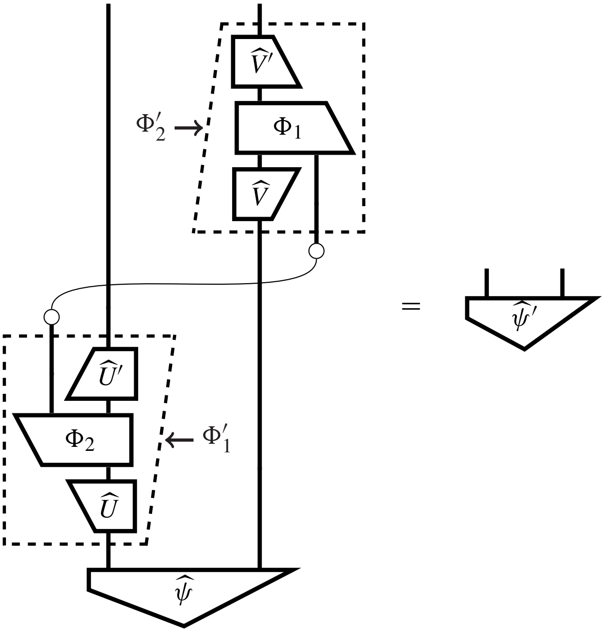
Proof Let Φ_1 and Φ_2 satisfy (13.17). Deforming the LHS gives:



Then, since $\widehat{\psi}$ and $\widehat{\psi}'$ are both pure bipartite states, we can apply Lemma 13.29 to remove the two swaps:

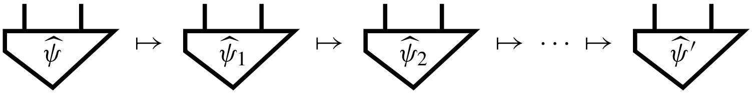


Then, moving the unitaries to the LHS:

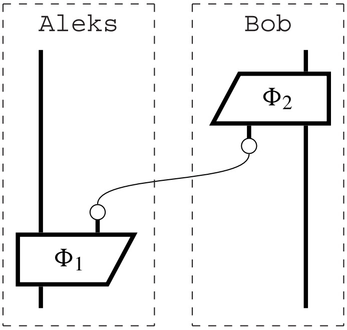


we obtain processes Φ'_1 and Φ'_2 satisfying (13.18). The converse follows symmetrically. □

For the sake of simplicity, assume that we have a LOCC protocol where each step deterministically yields a pure state:

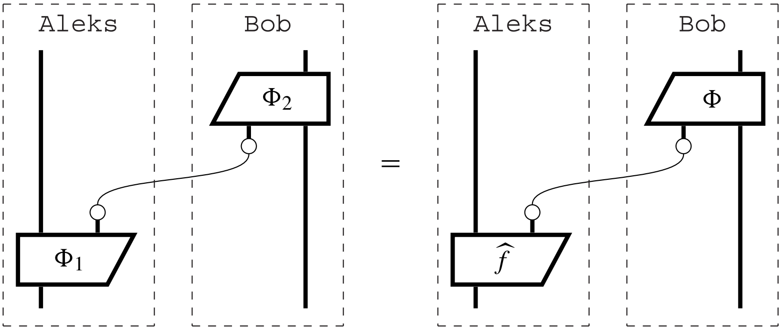


Then, this consists of a $\circ$-composition of processes satisfying (13.17) or (13.18). So, by applying Proposition (13.30), we can make all of the classical wires go from Aleks to Bob and bundle them together into a single classical wire. Hence we obtain a process of the form:

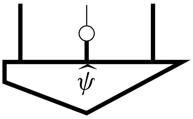


(13.19)

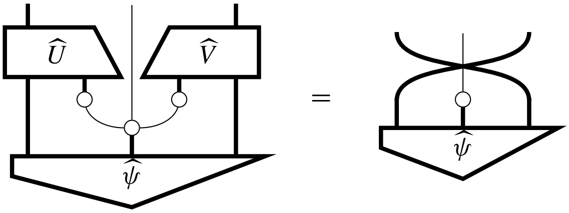
Exercise 13.31 Show that (by possibly increasing the size of the classical system) we can furthermore assume that Φ_1 in (13.19) is pure. That is, for all (causal) Φ_1 and Φ_2 there exist (causal) $\widehat{f}$ and Φ such that:



Exercise* 13.32 Show that any LOCC protocol can be rewritten in the form (13.19) without assuming each step determinstically yields a pure state. Hint: first purify Aleks' and Bob's processes such that each step yields a 'non-deterministic' pure state:



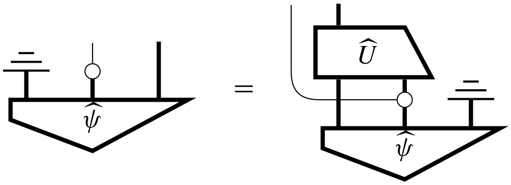
and use the following generalisation of Lemma 13.29: For any non-deterministic state $\widehat{\psi}$, there exist controlled unitaries $\widehat{U}$, $\widehat{V}$ such that:



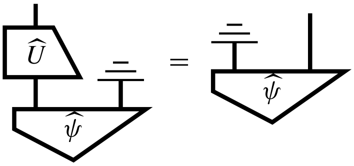
(13.20)

In the proof of the characterisation of the conversion relation for this resource theory we will make use of the following fact that tells us how the reduced states when discarding a different system are related.

Lemma 13.33 For every non-deterministic bipartite state $\widehat{\psi}$ (i.e. a pure bipartite state with a classical output) there exists a controlled unitary $\widehat{U}$ such that its two reduced states are related as follows:

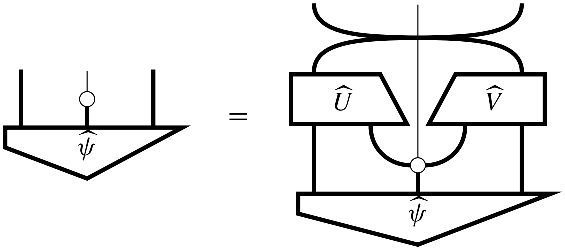


In the special case where the classical system is trivial, this becomes:



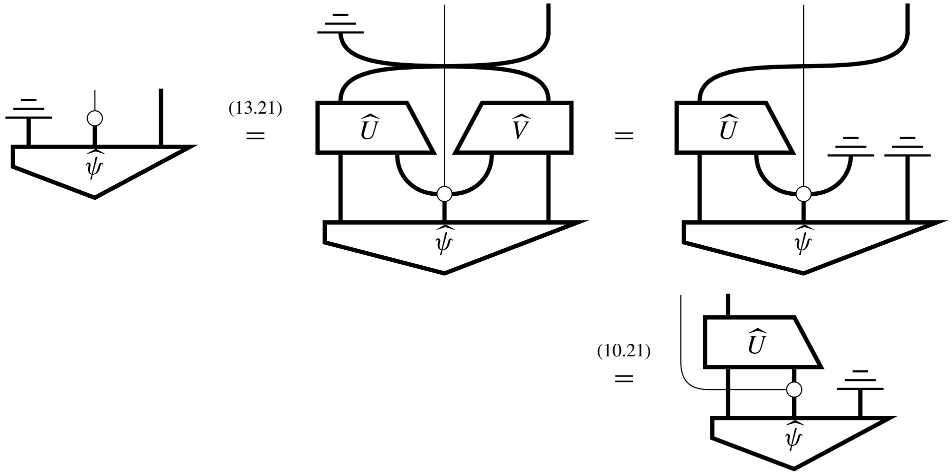
for some unitary $\widehat{U}$.

Proof We can rewrite equation (13.20) of Exercise* 13.32 as follows:



(13.21)

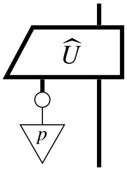
Then, using causality of the controlled unitary $\widehat{V}$ (in the second step):



□

We also will rely on the following fact.

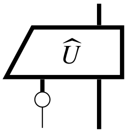
Lemma 13.34 Any mixture of unitaries:



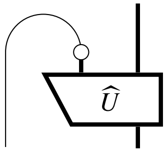
(13.22)

is a unital quantum map.

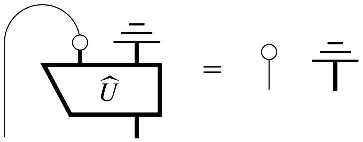
Proof From equations (10.45) it follows that for any controlled unitary:



its ‘controlled inverse’:

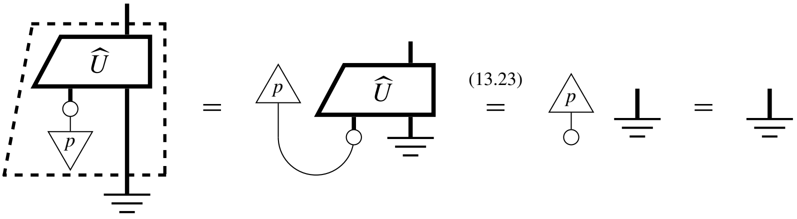


is also a controlled unitary, and in particular, it is causal:



(13.23)

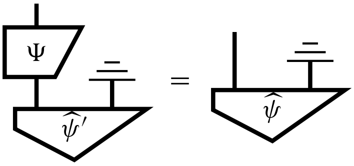
The adjoint of this equation then yields unitality of (13.22):



□

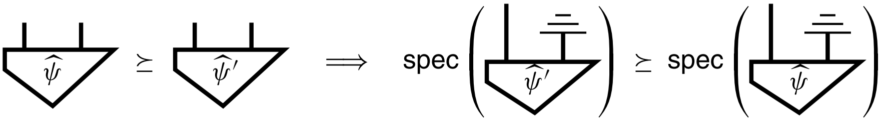
We now have enough ingredients to characterise the conversion relation for **LOCC entanglement²**, which looks a lot like the one for **purity**.

Theorem 13.35 If a bipartite state $\widehat{\psi}$ can be converted into a bipartite state $\widehat{\psi}'$ in **LOCC entanglement²**, then there exists a unital quantum map Ψ that converts the reduced state of $\widehat{\psi}'$ into the reduced state of $\widehat{\psi}$:



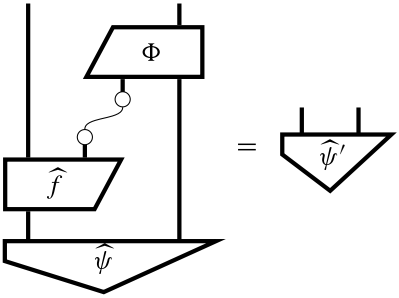
(13.24)

Hence, the conversion relation of **LOCC entanglement²** for bipartite states of a pair of the same fixed quantum system is given by:



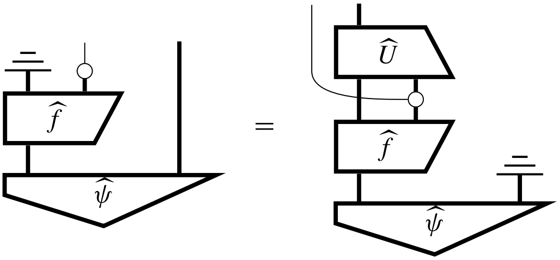
where the second $\succeq$ is the majorization preordering.

Proof Assume $\widehat{\psi} \succeq \widehat{\psi}'$. That is, thanks to Proposition 13.30 and Exercise 13.31, there exist quantum processes $\widehat{f}$ and Φ such that:

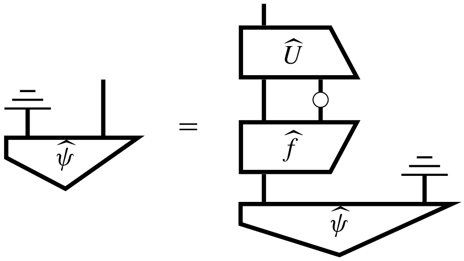


(13.25)

We will start with the RHS of (13.24), and work our way to the LHS. For this purpose, let us first focus just on local operation $\widehat{f}$ on the LHS of (13.25). Applying $\widehat{f}$ to $\widehat{\psi}$ yields a non-deterministic pure state; hence, by Lemma 13.33, there exists a controlled unitary such that:

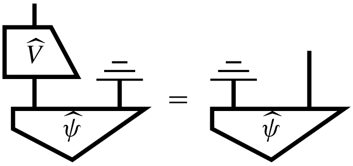


Then, deleting the classical output on both sides yields this equation:



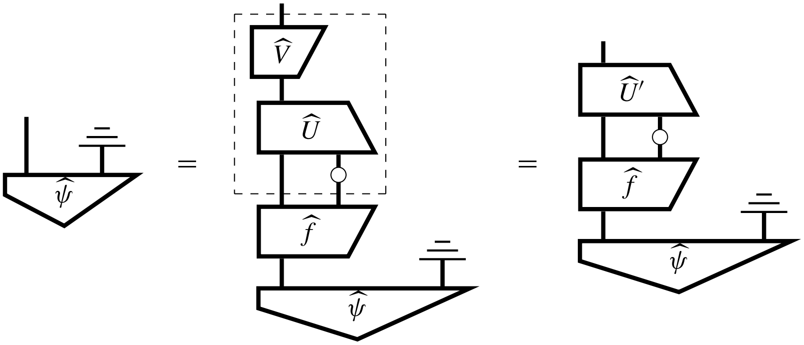
(13.26)

where we used causality to eliminate $\widehat{f}$ on the LHS. Next, by the second part of Lemma 13.33 there exists a unitary $\widehat{V}$ such that:



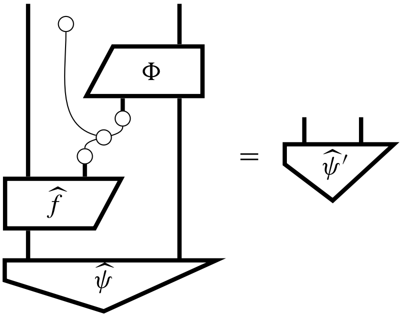
(13.27)

Combining equations (13.26) and (13.27), then moving $\widehat{V}$ to the RHS we obtain:

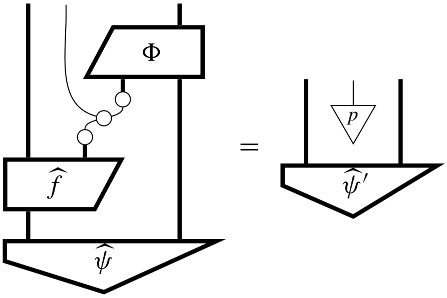


(13.28)

Now, we will modify equation (13.25) a bit so that we can plug it into the RHS of (13.28). By Proposition 8.59 we know that if deleting a classical system yields a pure state, then the classical system separates. Applying this to (13.25), which we can rewrite as:

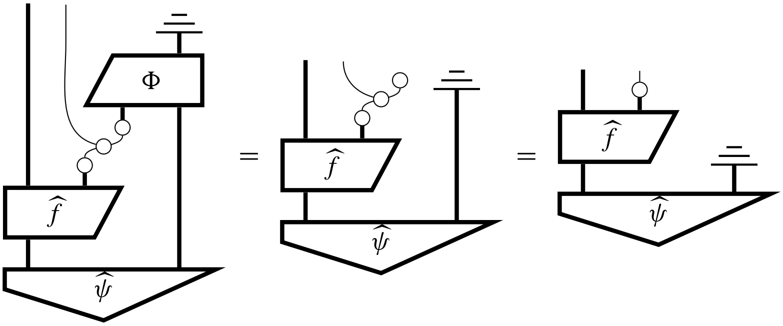


yields the following separation:



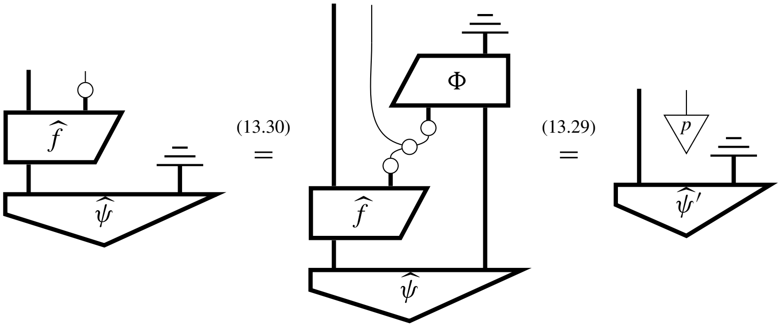
(13.29)

for some probability distribution p. By causality of Φ we also have:



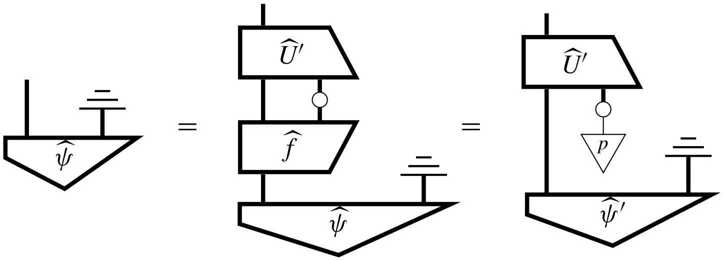
(13.30)

Hence:

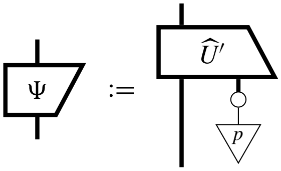


(13.31)

This equation can now be plugged into (13.28), which yields:

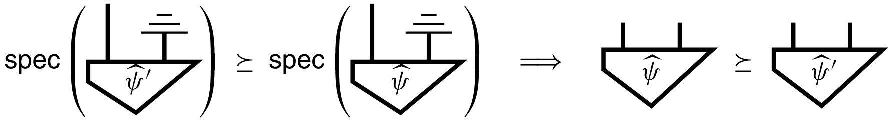


By Lemma 13.34 the quantum map:



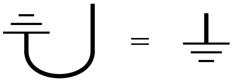
is unital, so we indeed obtain equation (13.24). □

Exercise* 13.36 Prove the converse to Theorem 13.35. Namely, show:



Comparing Theorem 13.25 and Theorem 13.35 we see that less purity of the reduced state means more entanglement.

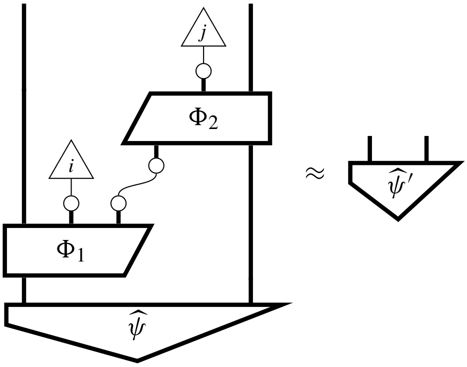
Example 13.37 Since the reduced state of the Bell state is the maximally mixed state:



it can be converted into any other bipartite pure state via LOCC. In other words, it is *LOCC-maximal*.

13.3.2 SLOCC Entanglement

We started the previous section with an argument that the very nature of 'freeness' requires causality of all processes involved in conversion of resources. However, the situation changes if instead of one pair of systems in state $\widehat{\psi}$, one has an unlimited supply of systems in that state. Then, if we try to convert to a state $\widehat{\psi}'$ by some non-deterministic LOCC process, we only need at least one branch to succeed:



Using terminology of Definition 13.7, this amounts to having a non-zero conversion rate from $\widehat{\psi}$ to $\widehat{\psi}'$:

$$r(\widehat{\psi} \succeq \widehat{\psi}') > 0$$

Since by Theorem 6.94) any quantum map can be realised as a branch of a (causal) quantum process, passing to this more liberal kind of local operation is equivalent to allowing local operations to be any cq-map, not just the causal ones. These new 'free' processes are called *SLOCC-operations*, as they can be decomposed in two kinds of basic processes:

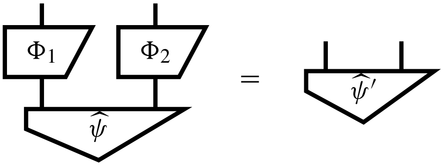
- <u>S</u>tochastic <u>L</u>ocal <u>O</u>perations (a.k.a. possibly non-causal cq-maps) and
- <u>C</u>lassical <u>C</u>ommunication

Definition 13.38 Let **sloccᒾ** be the subtheory of **quantum maps²** obtained by restricting to processes realising stochastic local operations, classical communication, and compositions thereof. Then:

$$\textbf{SLOCC entanglement}^{\mathbf{2}} \;:=\; \textbf{pure quantum states}^{\mathbf{2}}\textbf{/slocc}^{\mathbf{2}}$$

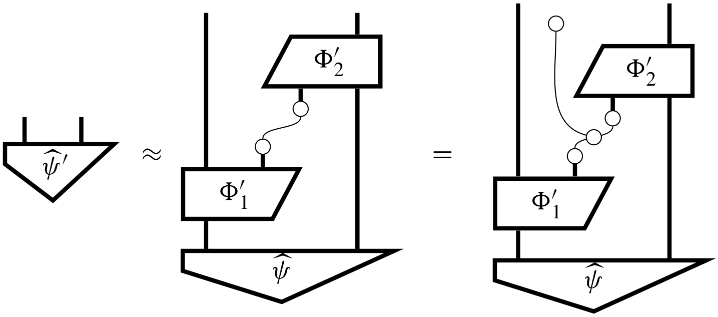
Though it looks pretty similar to **LOCC entanglement²**, this resource theory is actually a lot easier to work with. For one thing, classical communication now becomes irrelevant.

Theorem 13.39 A bipartite state $\widehat{\psi}$ can be converted into a bipartite state $\widehat{\psi}'$ in **SLOCC entanglement²** if and only if there exist quantum maps Φ_1 and Φ_2 such that:

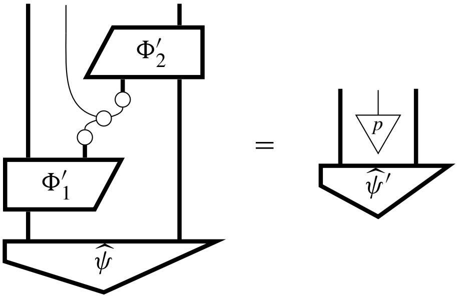


(13.32)

Proof Assume $\widehat{\psi} \succeq \widehat{\psi}'$; then there exist cq-maps Φ'_1 and Φ'_2 such that:

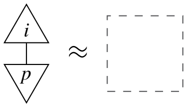


so by Proposition 8.59 we have:



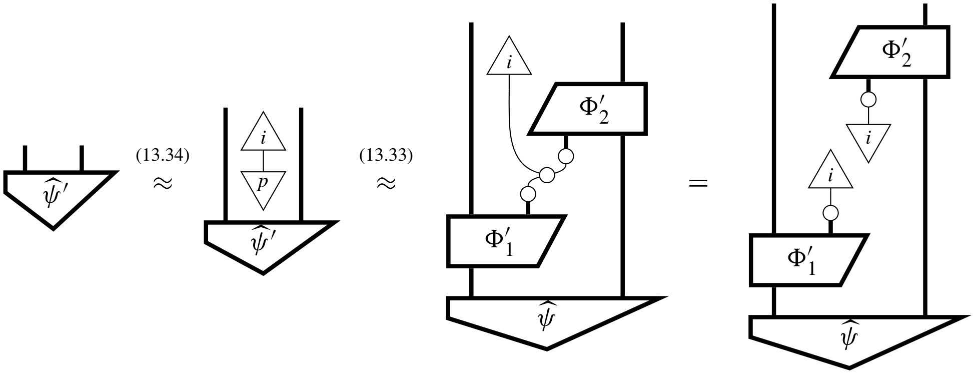
(13.33)

for some p. Since p is a (causal) probability distribution, there must be some ONB effect i such that:

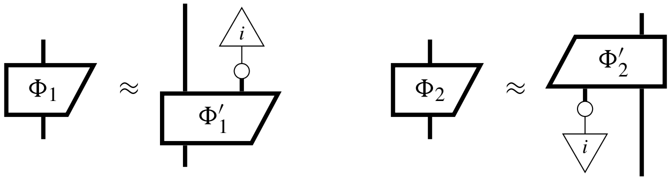


(13.34)

Hence:

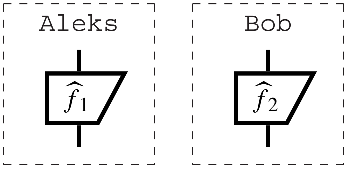


Letting:



(up to an appropriately chosen number) yields equation (13.32). □

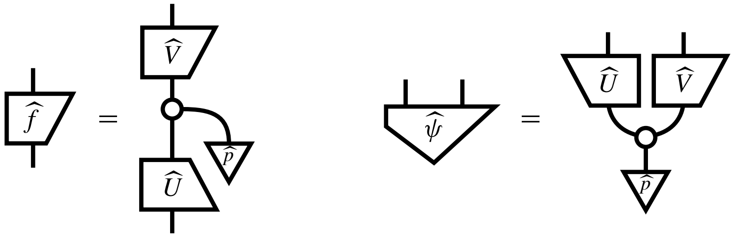
Exercise 13.40 Show, using a similar technique to the proof above, that it suffices to consider only pure quantum maps as local operations:



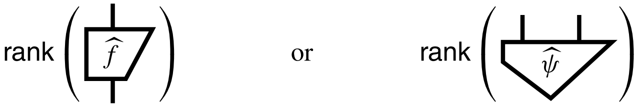
(13.35)

In order to characterise convertibility in **SLOCC entanglement**[2] we make use of the following standard notion from linear algebra, adopted to pure quantum maps.

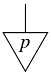
Definition 13.41 For a pure quantum map or bipartite state, represented in terms of its singular value decomposition:



its *rank*, respectively:



is the number of non-zero entries in the matrix of p:

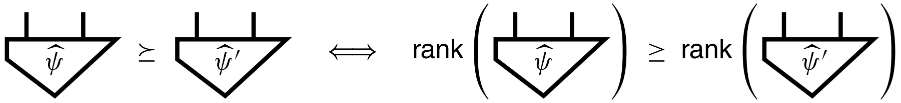


$$\leftrightarrow \begin{pmatrix} p^1 \\ \vdots \\ p^n \end{pmatrix}$$

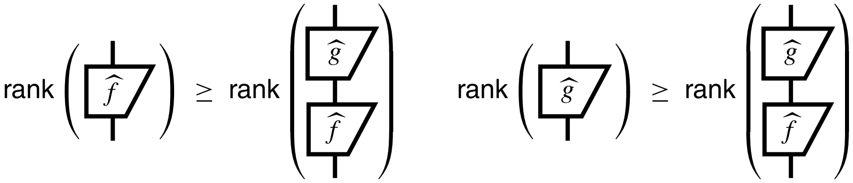
Remark 13.42 Just as the ‘sideways’ singular value decomposition of a bipartite state is often called the Schmidt decomposition, the ‘sideways’ rank of a bipartite state is often called the *Schmidt rank* in the literature.

We have already encountered the extreme cases of rank.

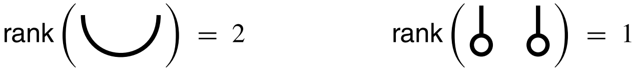
Exercise 13.43 First, show that 'maximum rank' is the same as 'non-degenerate' as in Definition 4.75, that the cup has maximum rank, and that 'rank 1' is the same as separable. Next, show that the conversion relation $\succeq$ for **SLOCC entanglement**[2] is given by:



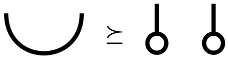
where you can make use of the fact that for pure quantum maps $\widehat{f}$ and $\widehat{g}$:



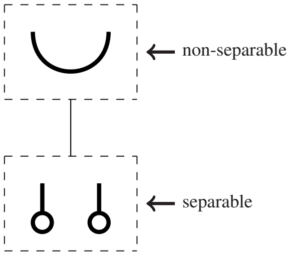
Thus, two bipartite states are equivalent (cf. Definition 13.4) if and only if they have the same rank. Since every bipartite qubit state must have either rank 1 or rank 2, for example:



there are only two *equivalence classes*: the class of states equivalent to the Bell state and the class of those equivalent to a separable state. Furthermore, any separable state can be obtained from a non-separable one via SLOCC-operations, hence:

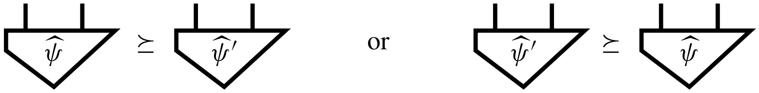


Since there are finitely many equivalence classes, we can depict this conversion relation as a *convertibility diagram*:



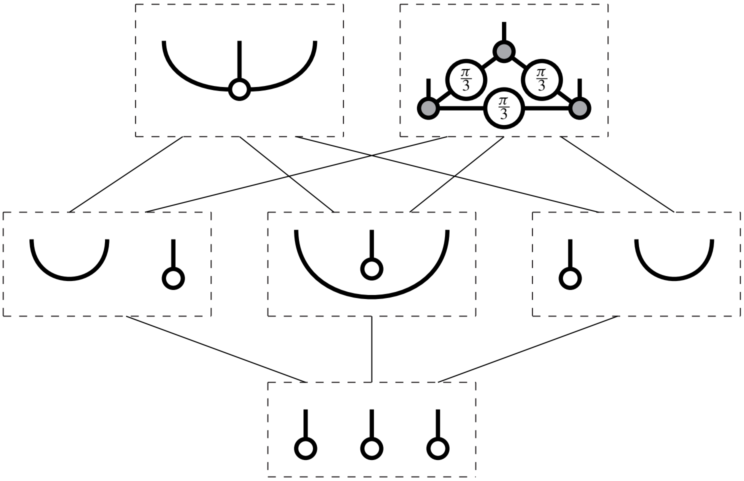
where the boxes represent equivalence classes, and the downward edge(s) represent(s) when one class is convertible to other.

Whereas LOCC-convertibility captures quantitative differences in entanglement, SLOCC-convertibility is much better at capturing purely 'qualitative' differences, e.g. 'separable' versus 'non-separable'. In the bipartite case, as we just saw, this creates a very simple total ordering on SLOCC-equivalence classes, dictated by the rank. So for all bipartite states $\widehat{\psi}$ and $\widehat{\psi}'$, either:

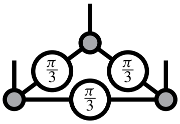


However, once we go beyond two systems, the situation changes. We start to get states that are SLOCC-maximal, but in inequivalent ways.

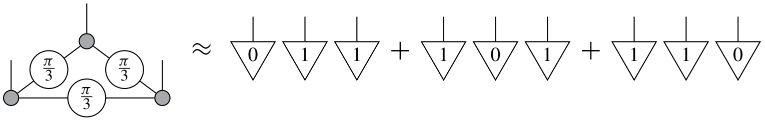
Theorem 13.44 The conversion relation for **SLOCC entanglement**[3], when restricting to qubits, is given by:



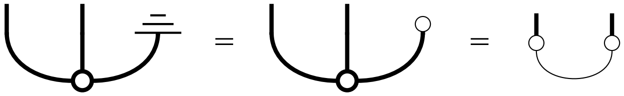
The key feature of this convertibility diagram is that at the top level we have two incomparable classes, respectively, witnessed by the GHZ state that we have encountered before, and something new, called the *W state*:



Exercise 13.45 Show that:



The qualitatively different entanglement properties between the GHZ state and the W state are a bit more subtle than, say, separable versus non-separable. For instance, if for a GHZ state we discard a system, the remaining two systems disentangle:

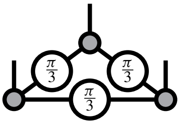


whereas for a W state they do not. In the next section, we see an even more striking difference between ‘GHZ-spiders’ and this new kind of ‘arachnid’.

Remark 13.46 Once one goes beyond three qubits, it is no longer the case that we get finitely many SLOCC-equivalence classes. There are simply too many free parameters for a state for four or more systems to cancel out via SLOCC-operations. One can still study parametrized SLOCC-equivalence classes (a.k.a. ‘SLOCC super-classes’) for four or more systems, but these are not nearly as well understood.

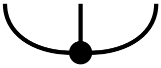
13.3.3 Exploding Spiders

Rather than looking like a spider, W states look more like a spider orgy:



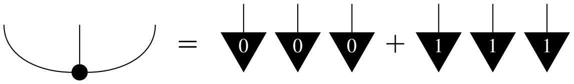
So what comes out? It cannot be just an ordinary spider, because of the following.

Proposition 13.47 For any spiders ● on a two-dimensional system, the state:

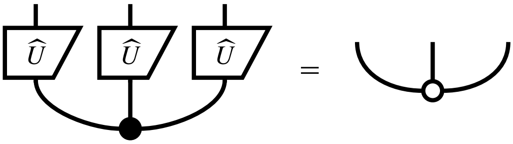


is SLOCC-equivalent to a GHZ state.

Proof From Theorem 8.41, any spider corresponds to an ONB. In particular:

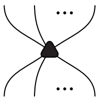


Then, for U the unitary that sends the ●-ONB to the ○-ONB, we have:

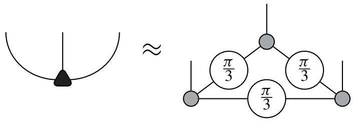


□

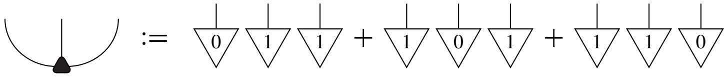
Since we can’t obtain the W state using normal spiders, we will obtain it using a different kind of spider-like arachnid. That is, we will define a family:



such that:



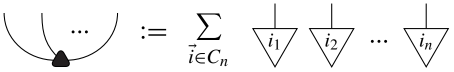
Following Exercise 13.45 we let:



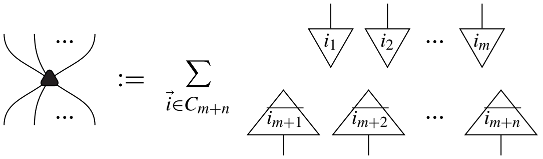
We can generalise this straightforwardly to produce n-partite states. First, consider all bit strings of length n containing a single 0:

$$C_n := \{011...1\ ,\ 101...1\ , ...\ ,\ 11...10\}$$

Then, to form the n-partite state, we sum over all bit strings $\vec{i} \in C_n$:

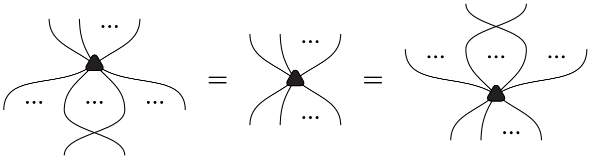


Similarly, we can obtain input legs, with a little modification: the input-ONB states should be negated. That is, for $\bar{i} := 1 - i$, we set:



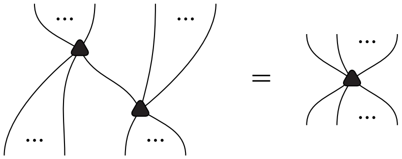
(13.36)

These new arachnids behave much like spiders, except they like each other a bit too much. For instance, standard spider behaviour includes obeying the leg-swapping equations:



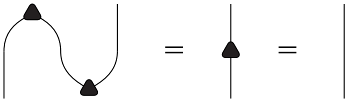
(13.37)

Also, if they are connected by a single leg, they fuse as expected:



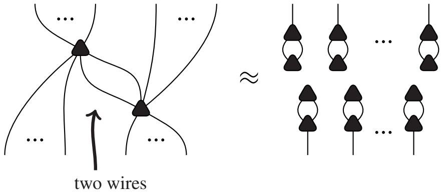
(13.38)

from whence we can derive most of usual stuff that holds for spiders. For instance, like spiders, these new things give us cups and caps:



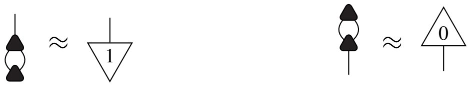
(13.39)

However, if these arachnids shake two (or more) legs, they become over-excited and explode:



(13.40)

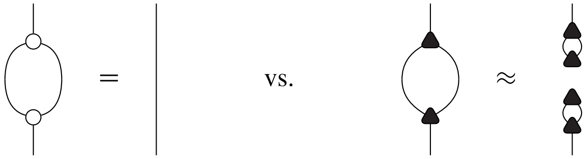
leaving a bunch of smoking stubs of legs behind:



Definition 13.48 A family ▲ of linear maps is called a family of *antispiders* if it satisfies equations (13.37), (13.38), and (13.40).

Exercise 13.49 Show (13.36) indeed defines a family of antispiders.

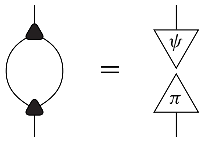
We can isolate the key difference between spiders and antispiders by looking at a simpler version of spider fusion, as compared with the 'antifusion' equation (13.40); namely, what happens to a single 'loop':



(13.41)

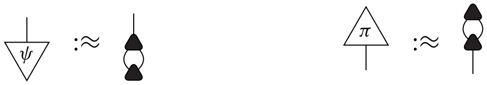
While in the case of spiders we get a plain wire, antispiders do the exact opposite: they separate. Although it looks like they separate in a very specific way, in fact it is already enough to say just that they separate:

Proposition 13.50 A family of linear maps satisfying (13.37) and (13.38) are antispiders if and only if:

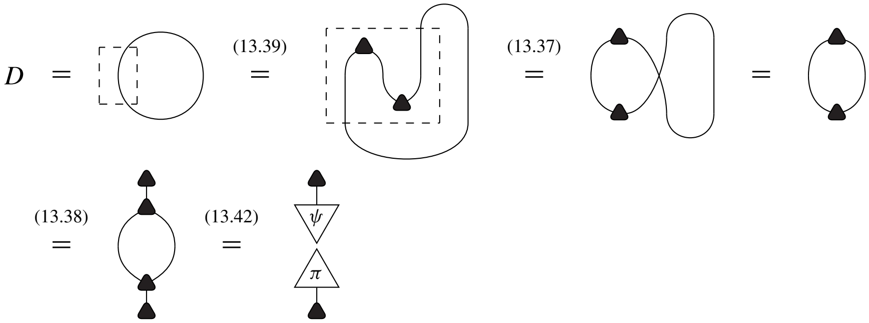


(13.42)

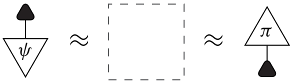
Proof Clearly antispiders satisfy (13.42), setting:



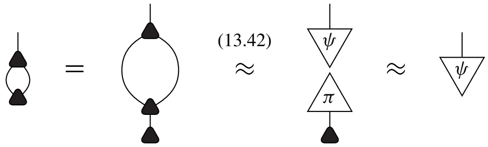
Conversely, assume (13.42). First, we have:

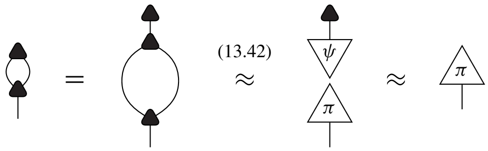


Since the LHS is non-zero, the two numbers on the RHS must also be non-zero, that is:

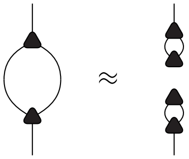


Now we can learn what ψ and π are, up to a number:





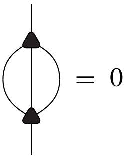
Substituting into (13.42), we obtain:



(13.43)

From this, it is straightforward to show that (13.40) follows. We leave this as an exercise for the reader. □

Exercise* 13.51 Show that for any antispider on a non-trivial ($D > 1$) system there cannot be ‘double loops’:

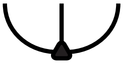


(13.44)

(Hint: first compute the number involved in equation (13.43).)

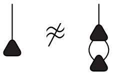
Just as with normal spiders and the GHZ state, the antispider equations totally characterise the SLOCC-equivalence class of W.

Theorem 13.52 Let ▲ be a family of antispiders for a two-dimensional system. Then:



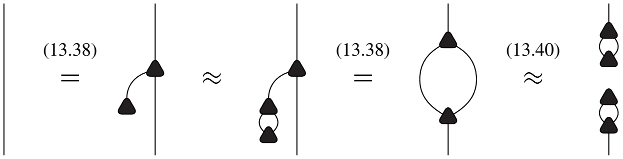
is SLOCC-equivalent to the W state.

Proof First, note that:

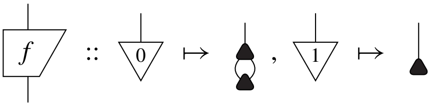


(13.45)

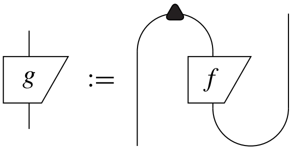
since otherwise the plain wire separates:



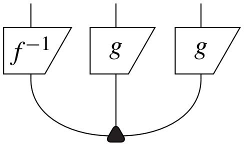
Hence the two states (13.45) form a basis for the two-dimensional system, so it is possible to define an invertible linear map f such that:



If we additionally let:



then by plugging in ○-ONB effects, it is straightforward to check that:

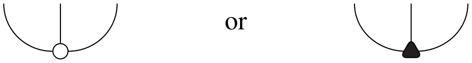


indeed gives a W state. □

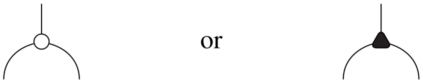
The bottom line is: once again we find the distinction between 'separable' and 'non-separable' playing a crucial role, this time in highlighting the qualitative difference between the two SLOCC-maximal states on three qubits.

13.3.4 Back to Basics: Arithmetic

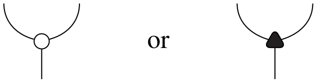
Theorem 13.44 tells us that there really are only two kinds of non-separable qubit states on three systems; that is, up to local operations, each such state is equivalent to either:



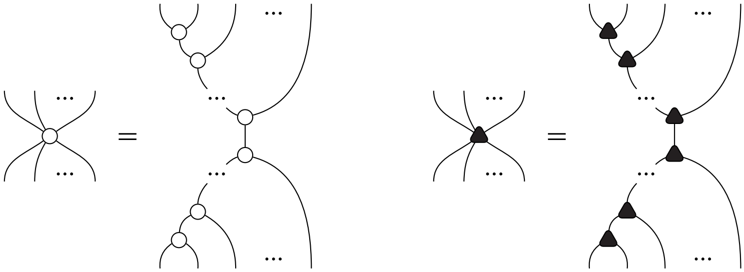
By bending some wires, we could just as easily say that any non-separable, linear map from two qubits to a qubit, up to local operations, must be equivalent to either:



or any one-to-two map must be locally equivalent to either:

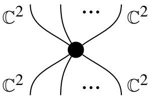


Because of (anti)spider fusion, an entire family of (anti)spiders is determined by these three-legged spiders:

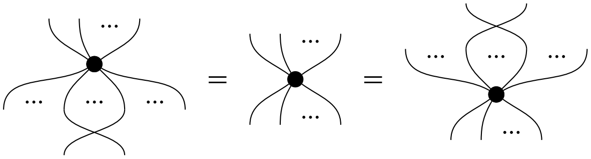


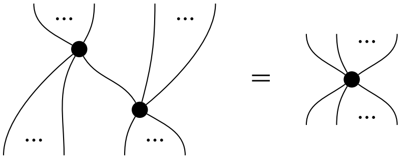
so one would expect spiders to reduce to just two cases as well, up to some local linear maps. This is indeed the case.

Theorem 13.53 Let:

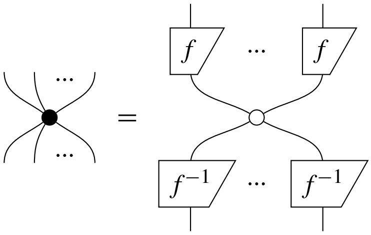


be a family of linear maps satisfying:

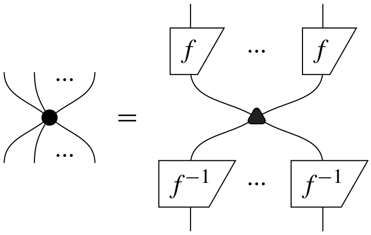




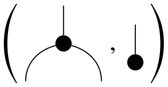
Then it must be the case that ● is *isomorphic* to either ○ or ▲. That is, there exists some isomorphism (i.e. invertible linear map) f such that either:



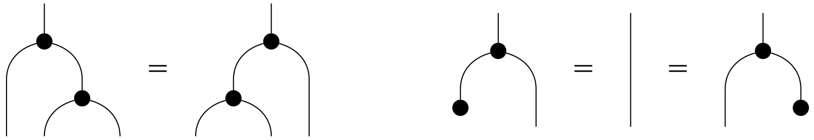
or



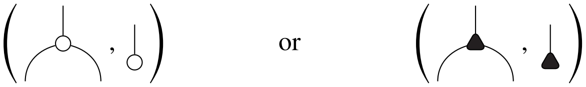
So spiders and antispiders are, in a strong sense, the only choice we have for a 'fusing' family of qubit operations. In fact, even without assuming we have a whole family of spiders, any pair of maps:



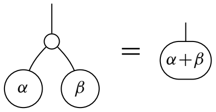
satisfying:



must be isomorphic to either:



But what are these two operations ○ and ▲? What do they do? Let's start with something we know about ○-spiders: how they interact with phase states:



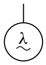
A phase state 'encodes' a complex number $e^{i\alpha}$, and when a pair of phase states meets a ○-spider, these numbers are multiplied:

$$\begin{pmatrix}1\\e^{i\alpha}\end{pmatrix}\star\begin{pmatrix}1\\e^{i\beta}\end{pmatrix}=\begin{pmatrix}1\\e^{i(\alpha+\beta)}\end{pmatrix}=\begin{pmatrix}1\\e^{i\alpha}\cdot e^{i\beta}\end{pmatrix}$$

In fact, as we saw back in Section 8.2.2.4 this will still be true if we replace complex numbers of the form $e^{i\alpha}$ with arbitrary complex numbers:

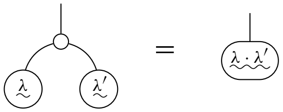
$$\begin{pmatrix}1\\\lambda\end{pmatrix}\star\begin{pmatrix}1\\\lambda'\end{pmatrix}=\begin{pmatrix}1\\\lambda\cdot\lambda'\end{pmatrix}$$

That is, by letting:



$$\leftrightarrow\begin{pmatrix}1\\\lambda\end{pmatrix}$$

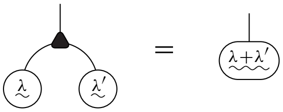
We have:



Since these 'generalised phases' form a basis, this totally characterises ○-matching for qubits. Hence:

Qubit spiders correspond to multiplication.

If we plug those same generalised phase states into the ▲-matching, something surprising happens:

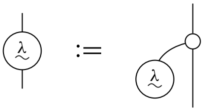


Hence:

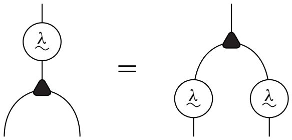
Qubit antispiders correspond to addition.

Now, if you have two numbers and you want to make one number, the first two things you would try are addition and multiplication. Surprisingly, when it comes to qubits, these are our only choices!

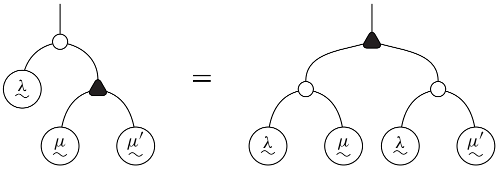
From here, we can start to play a similar game to that of the ZX-calculus and start to find a series of graphical rules governing the interaction of the ○-spider with the ▲-antispider. For instance, by letting:



we obtain generalised phase gates. Then, we can use a copy law:



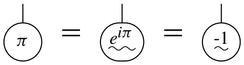
to capture the fact that ‘times’ distributes over ‘plus’:



which symbolically we know as:

$$\lambda \cdot (\mu + \mu') \;=\; \lambda \cdot \mu + \lambda \cdot \mu'$$

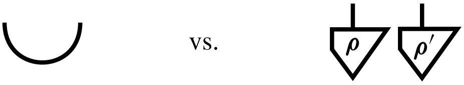
Just taking ○/▲, along with the usual π phase:



we obtain a language that is universal for linear maps whose matrices are restricted to integers, i.e. the process theory **matrices**($\mathbb{Z}$) $\subseteq$ **linear maps**. There even exists a graphical calculus that is complete for this theory. What is it? Well, we need to leave something for *Picturing Even More Quantum Processes*, don’t we?!

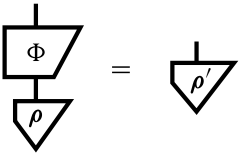
13.4 Summary: What to Remember

1. A *resource theory* is a kind of process theory where the types are called *resources* and the processes are called *resource conversions*. It captures the idea that resources (e.g. states) of some types are more valuable than others; e.g. entangled states are more desirable than separable states:



Given any process theory **P** (e.g. **quantum processes**) and a sub-theory of *free processes* **F**, a resource theory **P**/**F** arises whose:

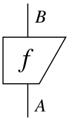
- types are the states of **P** and
- processes from a type ρ to ρ' are those Φ in **F** that convert ρ into ρ':



2. For a resource theory **R**, resource A can be *converted* into resource B:

$$A \succeq B$$

if and only if there exists a process in **R** that realises this conversion:



Denoting the resources by R, for any resource theory:

$$(R, \succeq, \otimes)$$

forms a *preordered monoid*, i.e. a preorder $(R, \succeq)$ for which we have:

$$A_1 \succeq B_1 \quad \text{and} \quad A_2 \succeq B_2 \qquad \Longrightarrow \qquad A_1 \otimes A_2 \succeq B_1 \otimes B_2$$

3. An *additive measure* for a resource theory is a function:

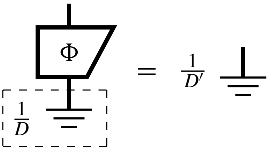
$$M : (R, \succeq, \otimes) \to \big(\mathbb{R}_{\geq 0}, \leq, +\big)$$

that preserves the preordered monoid structure; and a *supremal measure* is a function:

$$M : (R, \succeq, \otimes) \to \big(\mathbb{R}_{\geq 0}, \leq, \mathsf{max}\big)$$

that again preserves the preordered monoid structure.

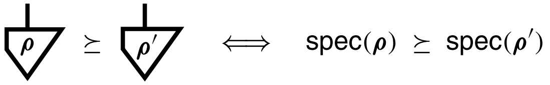
4. Unital quantum map are causal quantum maps Φ that also satisfy:



The resource theory **purity** arises from **quantum maps** by taking unital quantum maps as the free processes:

purity := **causal quantum states/unital quantum maps**

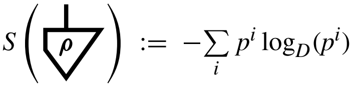
The conversion relation for **purity** is characterised by:



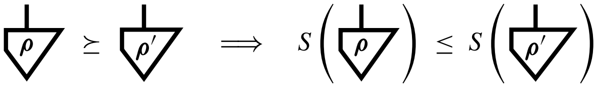
where the second ⪰ is the *majorization preordering*:

$$\left\{\begin{array}{rcl} p^1 & \geq & q^1 \\ p^1+p^2 & \geq & q^1+q^2 \\ & \vdots & \\ p^1+\cdots+p^n & \geq & q^1+\cdots+q^n \end{array}\right.$$

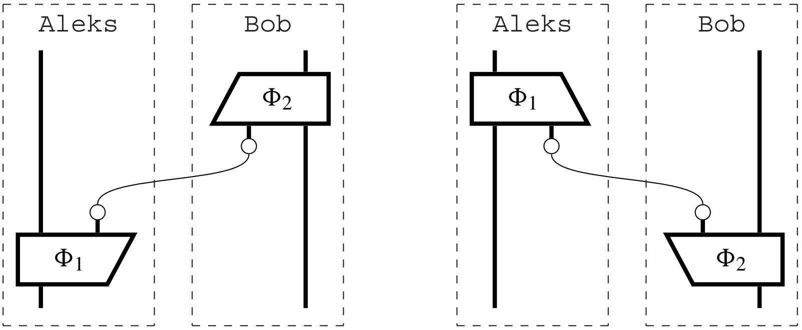
and the p^i are assumed to be in decreasing order. The *von Neumann entropy*:



gives an additive measure for (im)purity, namely:



5. The subtheory **locc²** of *LOCC-operations* (local operations and classical communication) consists of quantum processes of the form:

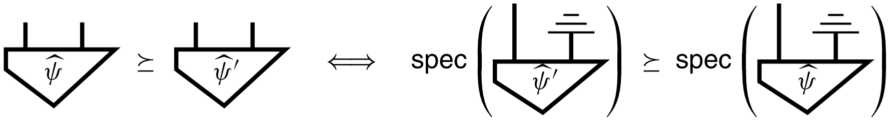


(13.46)

Then:

LOCC entanglement² := **pure quantum states²/locc²**

The conversion relation of **LOCC entanglement^2** is characterised by:

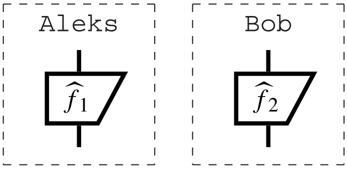

$\widehat{\psi}$ $\succeq$ $\widehat{\psi}'$ $\iff$ spec $\widehat{\psi}'$ $\succeq$ spec $\widehat{\psi}$

where the second $\succeq$ is again the majorization preordering.

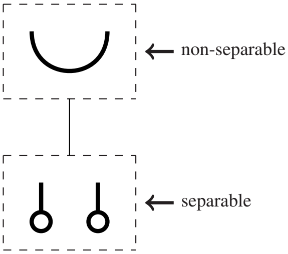
6. The subtheory **slocc**^{2} of *SLOCC-operations* (stochastic local operations and classical communication) consists of (possibly non-causal) cq-maps of the form of (13.46). Then:

$$\textbf{SLOCC entanglement}^2 \ := \ \textbf{pure quantum states}^2/\textbf{slocc}^2$$

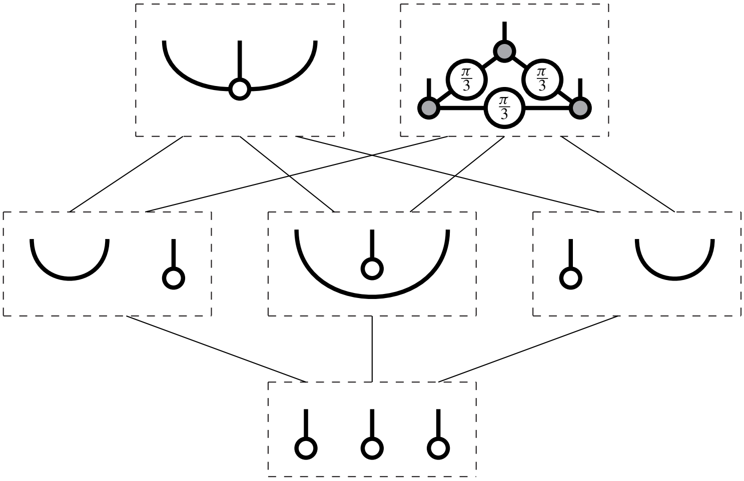
SLOCC-convertibility can furthermore always be realised by separable pure quantum maps:



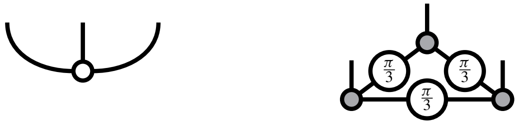
that is, classical communication is not necessary. For two qubits, there are only two *SLOCC-equivalence classes*:



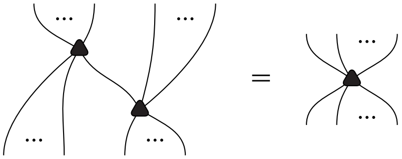
but for three qubits the story gets more interesting:



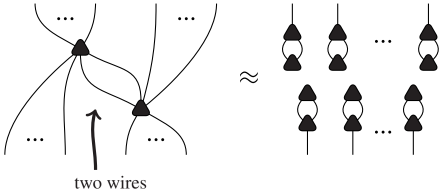
7. The states:



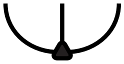
are the GHZ state and the *W state*. For any family of spiders over $\mathbb{C}^2$, the associated tripartite state is always SLOCC-equivalent to the GHZ state. On the other hand, for any family of *antispiders*, which still fuse when there is one wire:



but explode when there are two:

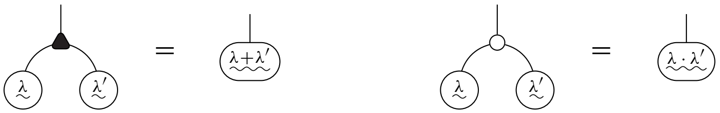


the associated tripartite state:



is SLOCC-equivalent to the W state.

8. Spiders and antispiders are the only two possibilities for spider-like families of linear maps on $\mathbb{C}^2$, and they correspond to 'plus' and 'times':



13.5 Historical Notes and References

The concept of a resource theory that we have adopted mainly emerged within the quantum information community. The process-theoretic formulation was put forward by Coecke et al. (2014). The notion of free processes first appeared in Horodecki et al. (2002). Many resource theories had already been proposed, e.g. entanglement (Horodecki et al., 2009), symmetry (Gour and Spekkens, 2008; Marvian and Spekkens, 2013), purity (Horodecki et al., 2003), non-equilibrium (Gour et al., 2013), and athermality (Brandão et al., 2013). Elaborations on the framework presented here include Fong and Nava-Kopp (2015) and

Fritz (2015). As resource theory is currently taking off as a subject, many more papers will have seen daylight by the time you read this.

A similar analysis to the one performed here, but within the framework of operational probabilistic theories (a hybrid of generalised probabilistic theories and process theories), can be found in Chiribella and Scandolo (2015). In that paper, the results presented here are referred to as an axiomatisation of thermodynamics. Also, our Lemma 13.29 is taken to be an axiom and is referred to as the *local exchangeability axiom*.

A discussion of the entropy associated to mixed quantum states was already in von Neumann (1927), which was in fact a long time before Shannon's seminal paper on entropy (Shannon, 1948), which started the field of information theory.

The majorization preordering dates back to Robert Franklin Muirhead (1903), who made several important contributions to mathematics but never held a faculty position. Theorem 13.25 is taken from Alberti and Uhlmann (1982). The fact that a mixture of unitaries yields a unital quantum map is a generalisation of one direction of Birkhoff's theorem, which states that mixtures of permutations and doubly stochastic maps are one and the same thing. Proposition 13.30 is taken from Lo and Popescu (2001) and Theorem 13.35 is taken from Nielsen (1999).

The SLOCC-classification of three qubits is taken from Dür et al. (2000). From four qubits onward there is an uncountably infinite set of SLOCC classes. One can nevertheless still identify finitely many parametrised 'super-classes' (see e.g. Verstraete et al., 2002; Lamata et al., 2007). The form of the W state in ZX-calculus is taken from Coecke and Edwards (2010).

The treatment of the W state as antispiders was introduced in Coecke and Kissinger (2010), and so was the interaction of spiders and antispiders. Further elaborations are in Herrmann (2010) and Kissinger (2012a). An extension of these ideas to qutrits can be found in Honda (2012). The encoding of spiders (a.k.a. the GHZ state) and antispiders (a.k.a. the W state) as 'times' and 'plus' first appeared in Coecke et al. (2010b). The completeness for the corresponding calculus is due to Hadzihasanovic (2015).