An Operational Approach to Quantum Information Theory

Notes by Michele Dall'Arno (dallarno.michele@yukawa.kyoto-u.ac.jp)

Quantum Information Unit School

Kyoto University, 29 June – 3 July, 2020

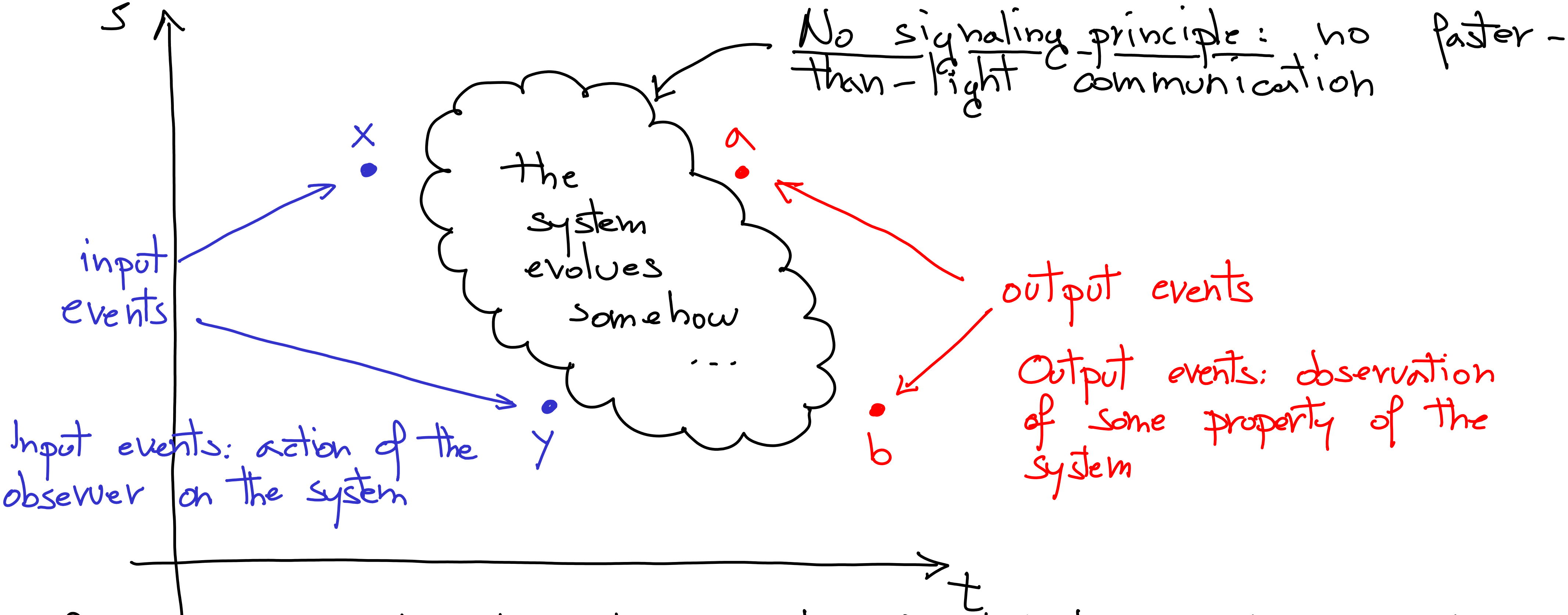
Introduction

- Quantum theory is usually introduced by means of the Hilbert space formalism, a set of abstract mathematical axioms.
- Here, we introduce quantum theory within the operational framework usually referred to as "general probabilistic theories".
- We certainly do not aim at completeness: our overview is a lightweight and simplified introduction to the topic.
- You probably won't recognize in here the traditional "textbook" quantum mechanics (where all states are pure, measurements are projective, trasformations are unitaries ...) at first.

Contents

- But we give a thorough presentation of all the building blocks: states, measurements, their transformations (channels), and transformations of their transformations (higher order maps).
- We will also present the simplest protocols:
  - steering
  - teleportation
  - dense coding
- And the main result about classical communication over quantum channels (Frenkel and Weiner's theorem).

We start from a Minkowski space-time*



* for an approach where the space-time is derived, see the works by Bisio, D'Ariano, Perinotti, Tosini.

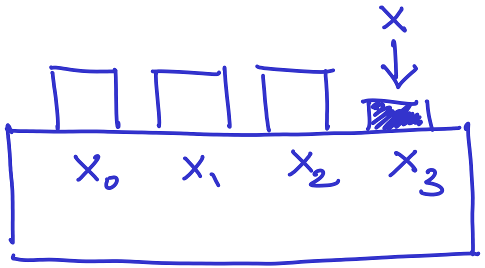
Input and Output events

Input events correspond to the selection of a specific value x for a random variable X with values in some alphabet $\mathcal{X}$.

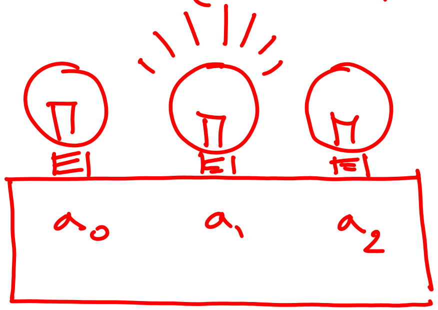
Output events correspond to the reading of a specific value a for a random variable A with values in some alphabet $\mathcal{A}$.

$$\mathcal{X} = \{x_0, x_1, \ldots\}$$

$$\mathcal{A} = \{a_0, a_1, \ldots\}$$



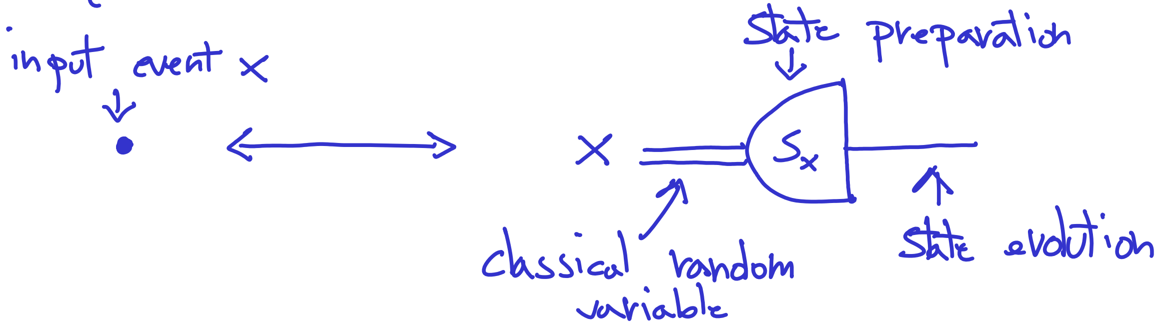
$\longrightarrow X = x_3$



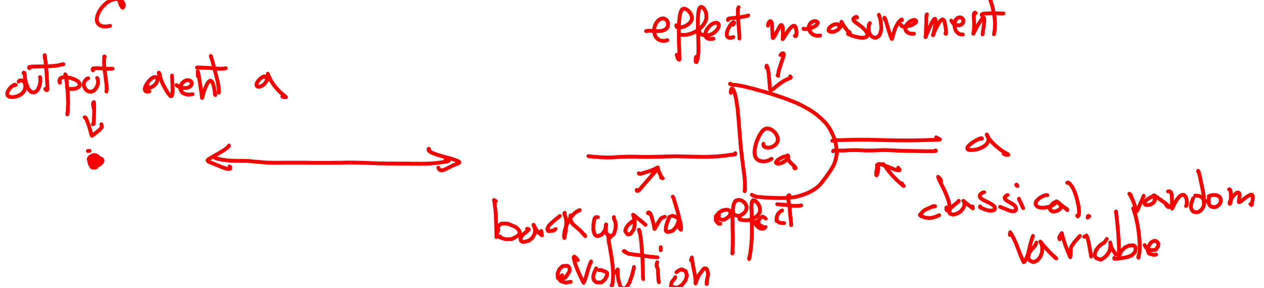
$\longrightarrow A = a_1$

How do we describe the evolution of the system?

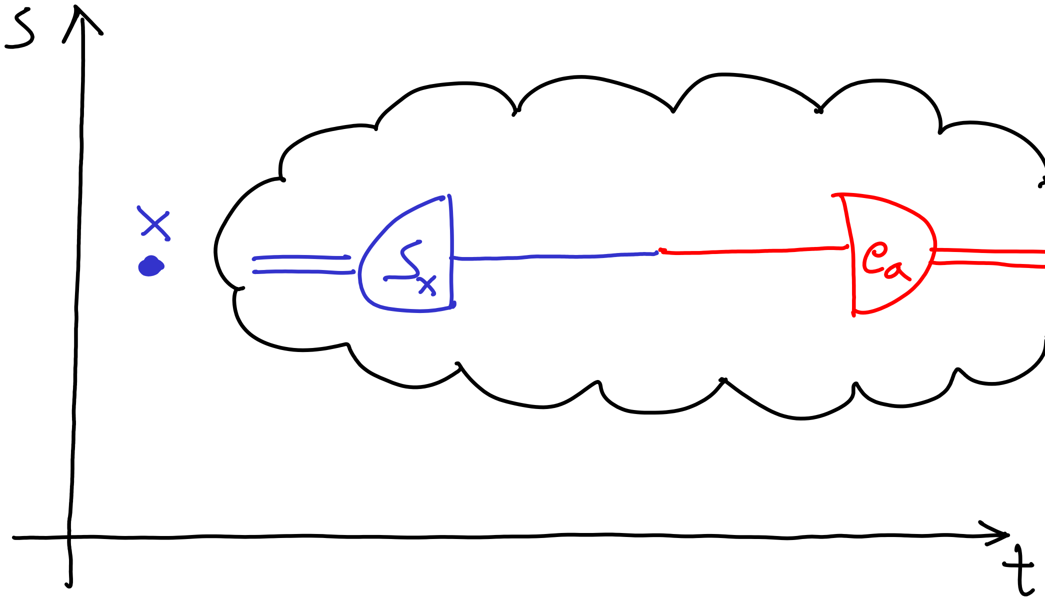
For example, we could say that an input event x prepares a "state" S_x.
Using the circuit notation:



For example, we could say that an output event a measures an "effect" e_a.
Using the circuit notation:



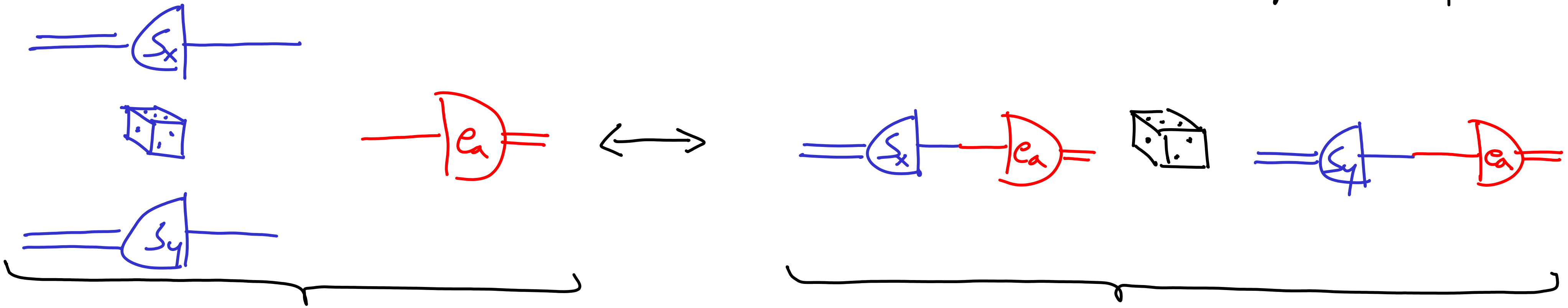
Simple example: an input event followed by an output event



From this description of the evolution of the system we must be able to compute the probability $p(A=a \mid X=x)$ of output a given input x.

What are states and effects, and how to combine them?

Operationally, the probability of the convex combination of experiments must equal the convex combination of the probabilities of each experiment.

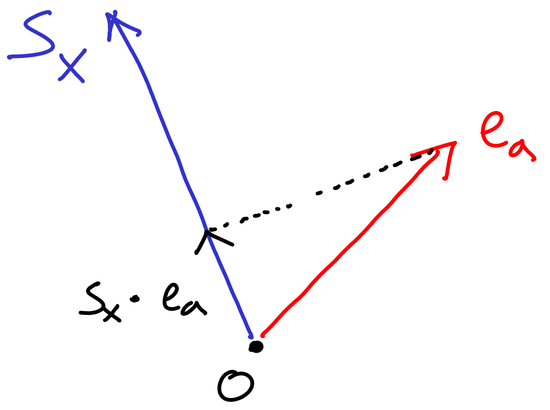


$$p(a|\lambda x + (1-\lambda)y) = \lambda\, p(a|x) + (1-\lambda)\, p(a|y)$$

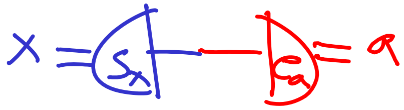
and the same for the convex combination of effects.

Hence, states and effects belong to linear spaces and their combination is a bilinear function (w.l.o.g., the inner product).

Simple example continued ...



$$\longleftrightarrow \quad s_x \cdot e_a = p(a|x) \quad \longleftrightarrow$$

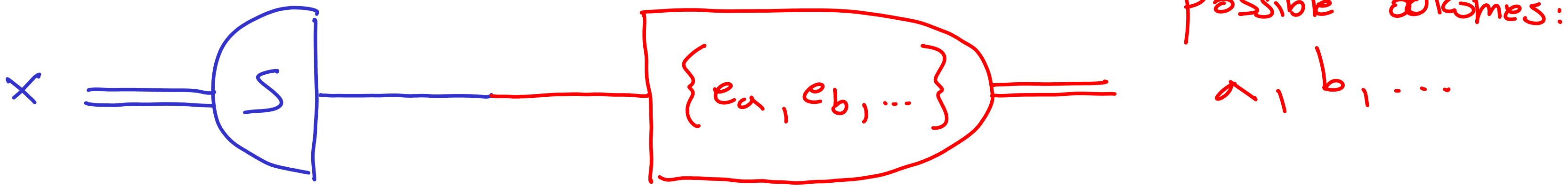


The existence of a unit effect

While we can choose to prepare a state s_x by selecting random variable x, we cannot a priori choose the measured effect e_a.

$$\Downarrow$$

Measurements are collection of effects, one of which is measured any time the measurement is performed.



$\sum_a p(a|x) = 1 \iff$ any measurement always produces exactly one outcome

$\iff$ there exists a unit effect u such that $s \cdot u = 1$ for any state s.

Destructive measurements

A destructive measurement is hence a collection of effects $\{e_a\}$ such that:

$$\sum_a e_a = u.$$

$$\left(\sum_a p(a|x) = \sum_a (e_a \cdot s) = \left(\sum_a e_a\right) \cdot s = u \cdot s = 1 \right)$$

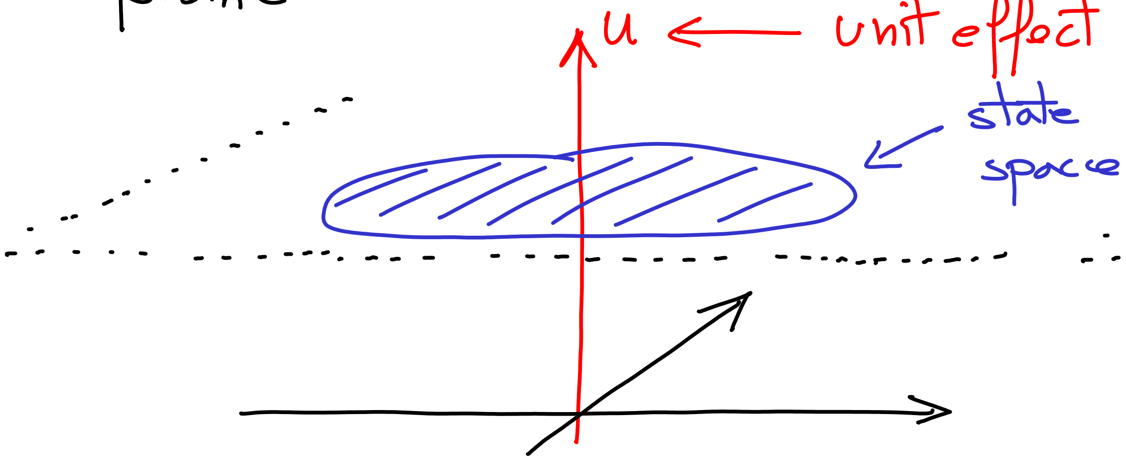
Of course, $\{u\}$ itself is a (trivial) measurement.

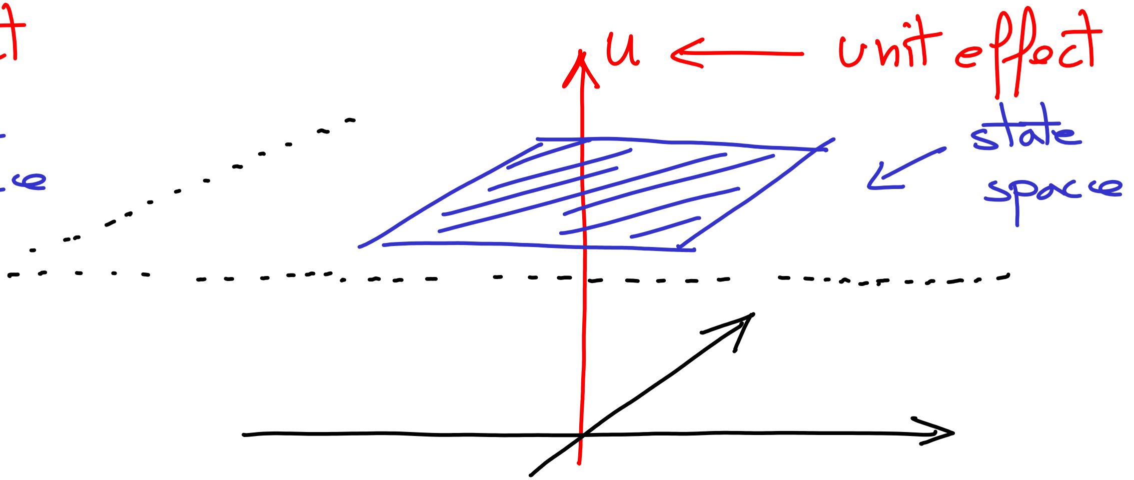
The state space and the effect space

What states and effects are legitimate?

- Non negativity of probabilities requires that for any state s and any effect e the inner product $s \cdot e \geq 0$.

- The existence of a unit effect requires that states lie on a hyperplane and the unit effect is orthogonal to such a hyperplane

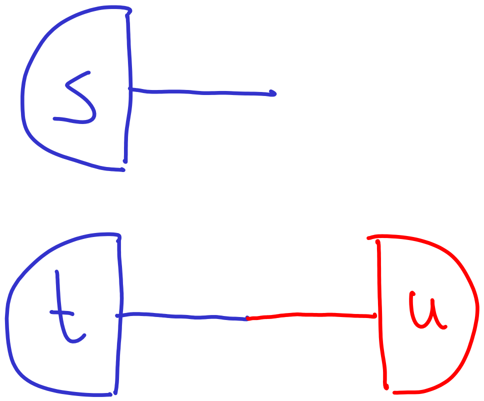




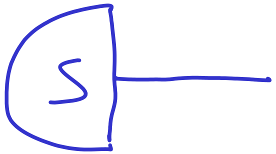
Composition of states and effects

How do two small systems compose to create a larger system?

Let's consider the following operational requirement:



$=$

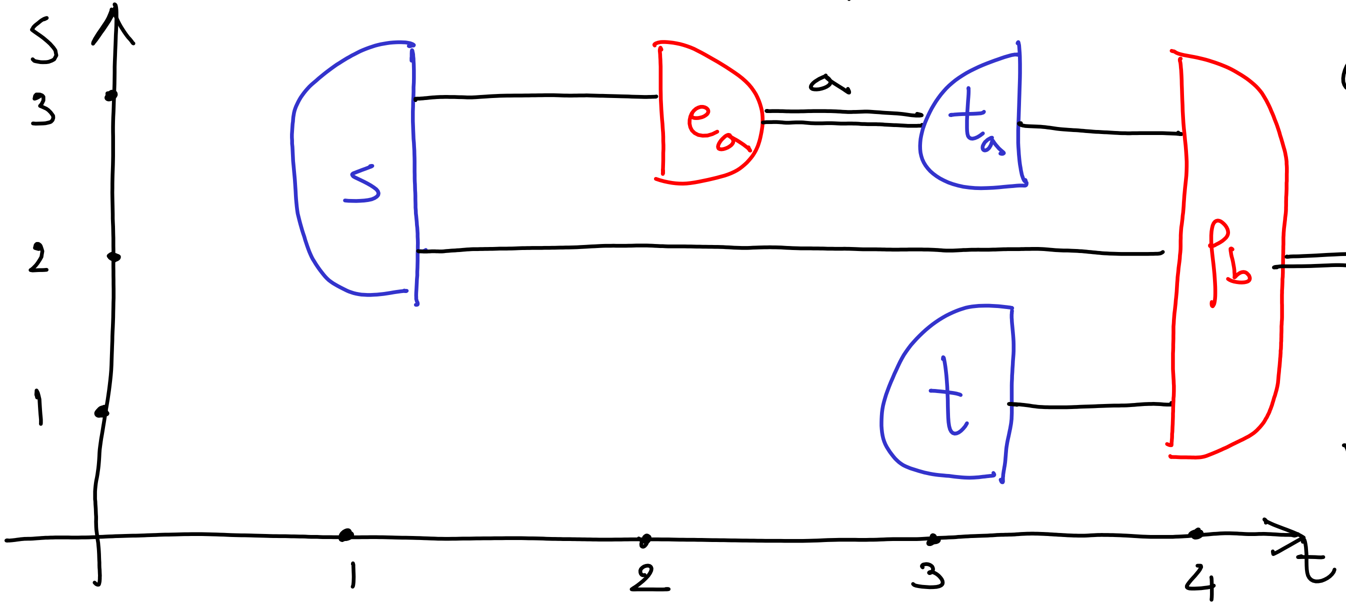


Discarding one system (measuring it with the unit effect) must return the other system.

The tensor product $s \otimes t$ satisfies this operational requirement.

Composition of states and effects is given by their tensor product.

More complex example



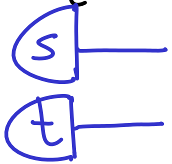
Composition allows us to build multipartite circuits.

Legitimate states and effects must give non-negative probabilities for any circuit.

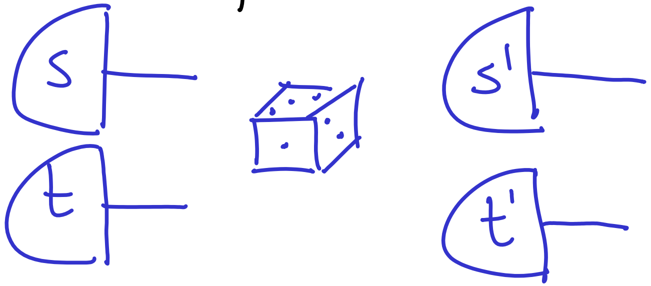
- State s is prepared at time 1 in locations 2 and 3.
- Part at location 3 is measured by measurement $\{e_a\}$ at time 2.
- At time 3, state t_a is prepared in location 3 based on outcome a. Simultaneously, state t is prepared in location 1.
- Finally, at time 4, measurement $\{f_b\}$ is performed at locations 1, 2, and 3.

Towards entanglement

The composition of states s and t is given by the tensor product

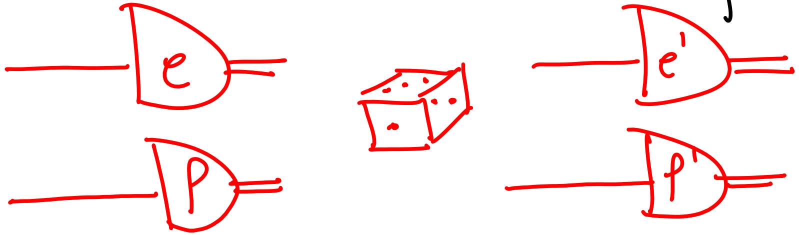
$s \otimes t =$ 

Operationally, convex combinations are also allowed, for example:



$= \lambda (s \otimes t) + (1-\lambda)(s' \otimes t')$

The same holds true for effects:

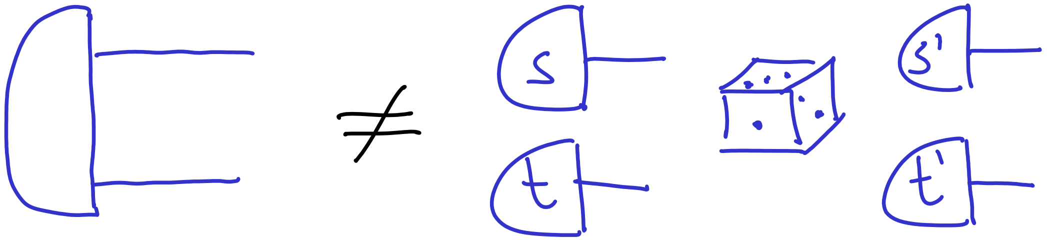


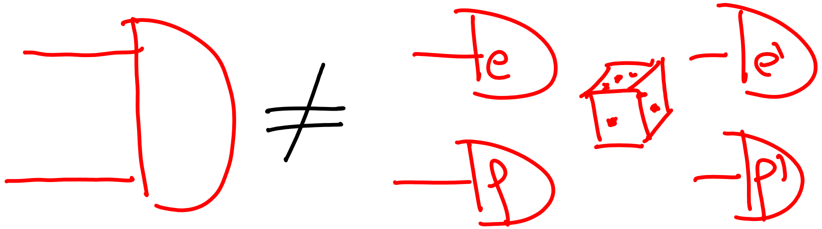
$= \lambda (e \otimes p) + (1-\lambda)(e' \otimes p')$

Entanglement

Are there multipartite states (resp. effects) that cannot be written as (a convex combination of) tensor products?

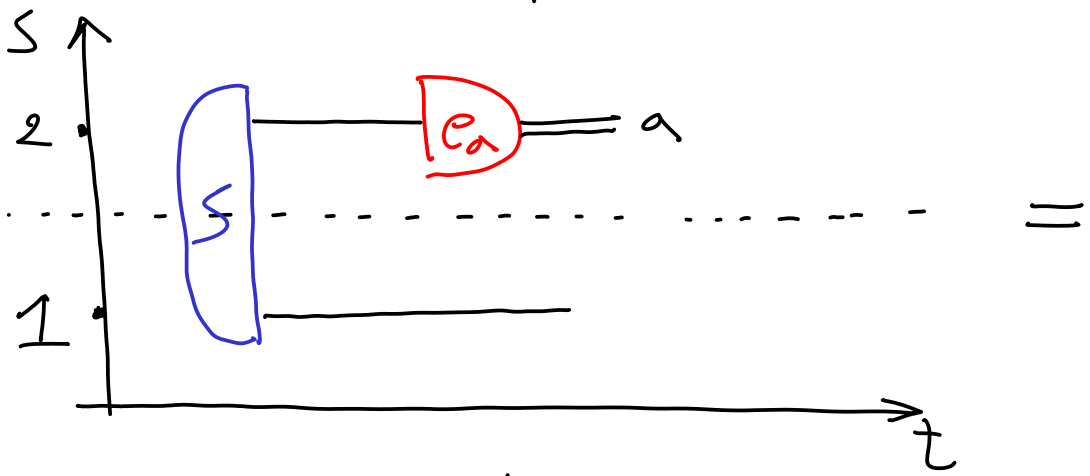
Operationally, states (resp. effects) are required to give non-negative probabilities. When they are not (a convex combination of) tensor products, we call them entangled.





Steering

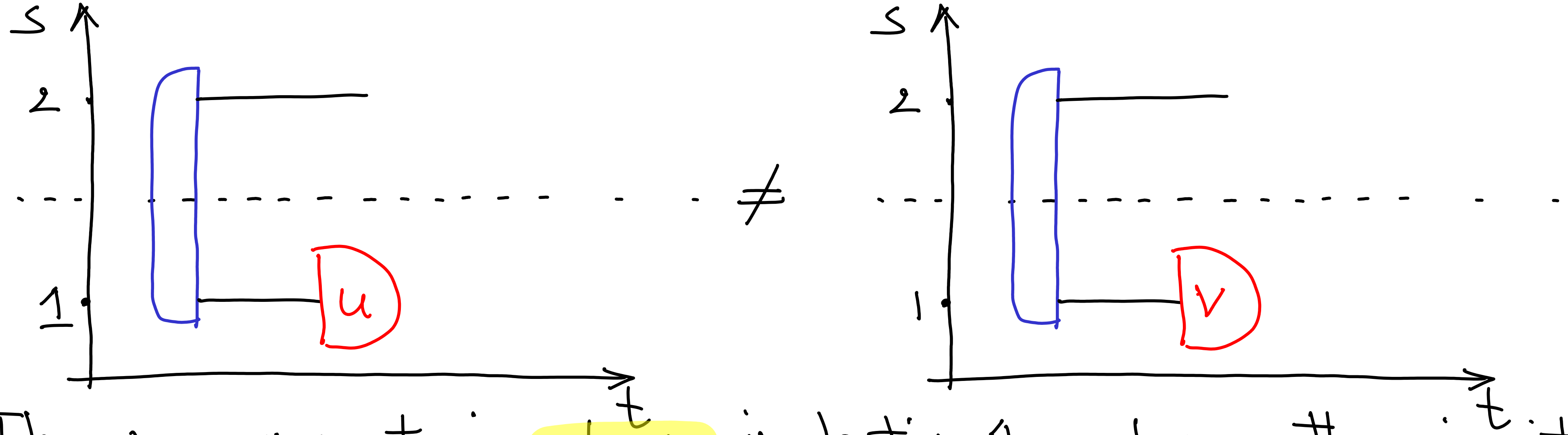
Shared entanglement can be used to istantaneously "steer" a state in a different location.



Observing outcome a of measurement $\{e_a\}$ istantaneously steered a state S_a (that depends on a) in location 1.
Outcome a was not choosen in location 2, hence ==no violation of the no signaling principle.==

The uniqueness of the unit effect (back to measurements)

Suppose there exists two inequivalent unit effects u and v. Then $u \cdot s = v \cdot s = 1$ for any state s. There exists an entangled state s such that measuring u or v in one location, steers different states in the other location.

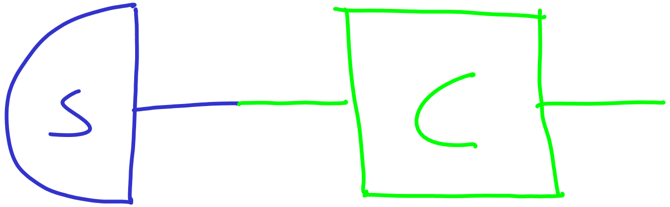


The measurement is chosen in location 1, hence there is istantaneous communication: no signaling principle is violated!

Transformations

So far we have trivial evolutions only: a state does not change until it is measured.

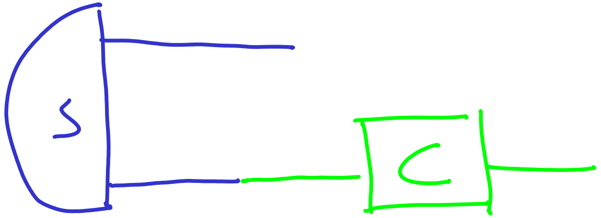
How to describe transformations of states?



$= C(s)$

for any state s and any transformation C, $C(s)$ must be a state, too. (positivity of C)

Operationally, state transformations (channels) must map states into states. Is this the only requirement?

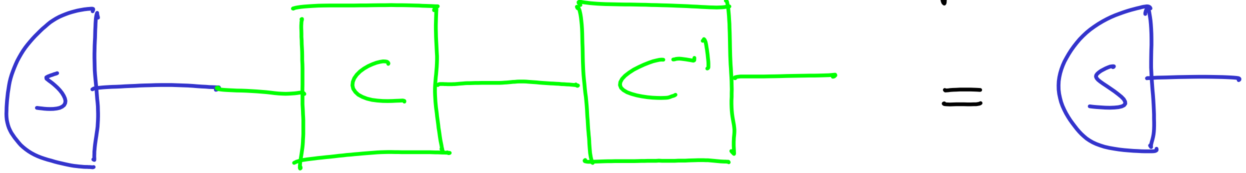


$= (id \otimes C)(s)$

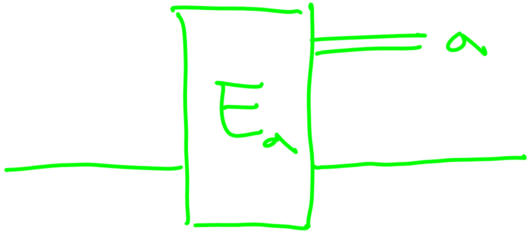
for any bipartite state s, $(id \otimes C)(s)$ must be a state (complete positivity of C)

Important instances of channels

- **Reversible channel** C: there exists a channel C^{-1} such that $C^{-1}(C(s)) = s$ for any state s.



- **Instrument** (non-destructive measurement) $\{E_a\}$: collection of completely positive maps such that $\sum_a E_a$ is a channel.

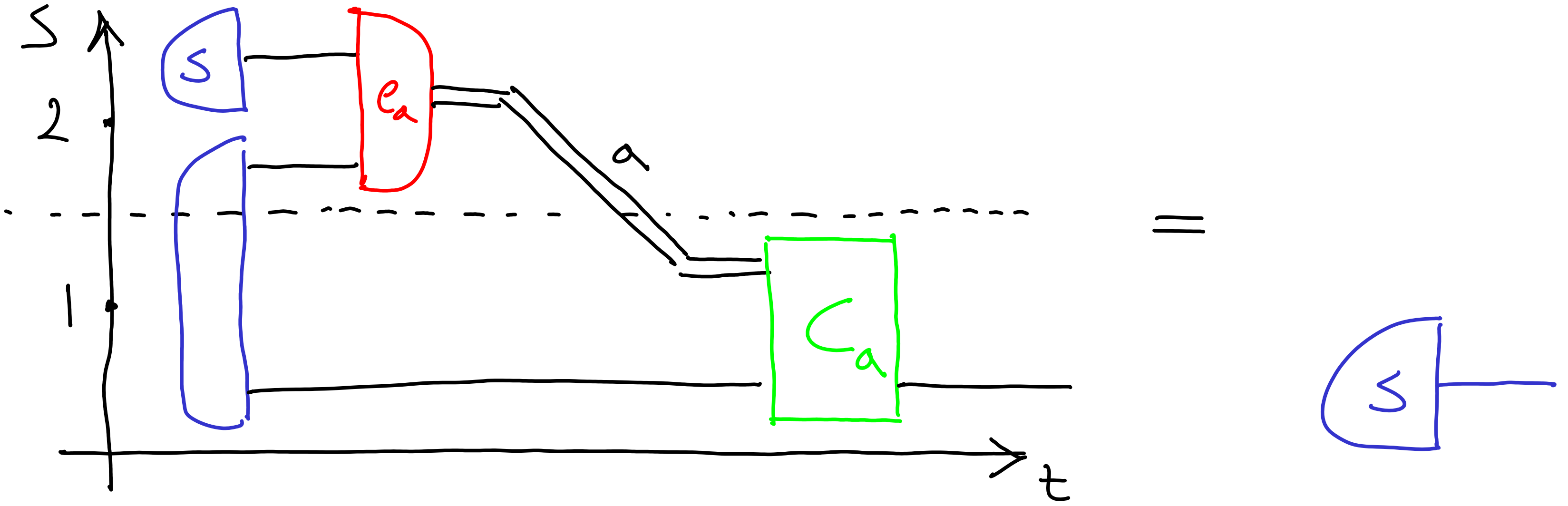


- States and effects are channels with trivial input and output, respectively.

Entanglement allows for teleportation

Teleportation: send a state from one location to another by means of classical communication and shared entanglement.

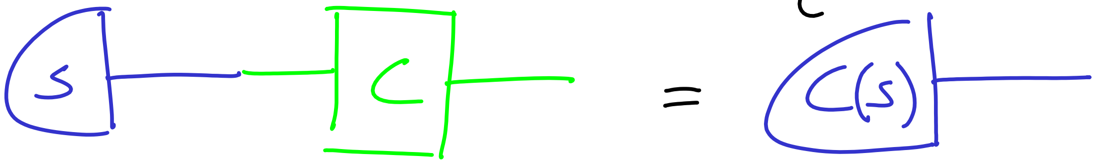
Suppose there exists a bipartite state t and a bipartite measurement $\{e_a\}$ such that



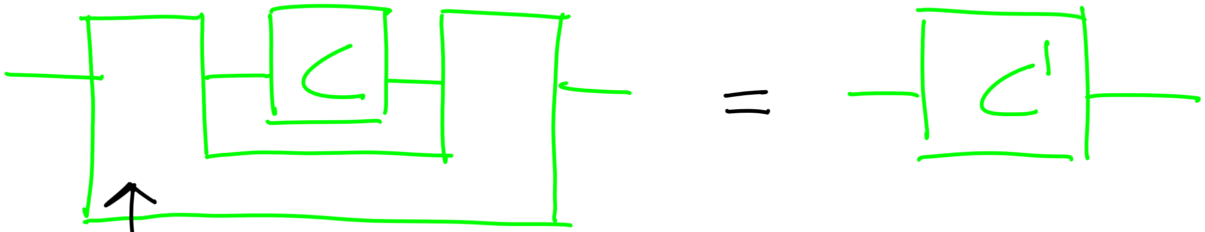
← teleportation!

Transformations of Transformations

Channels are the most general Transformations from states to states.



What are the most general transformations of channels?



this is called a higher order map.

For the theory of higher order maps, see PRSA 475 20180706 and references therein.

What makes Quantum Theory special?

Its state space! To introduce it we need to represent states in a different way.

First, the dimension of the vectorial space needs to be a square, say d^2. Then, rearrange entries as follows:

$$s = \begin{pmatrix} s_1 \\ s_2 \\ \vdots \\ s_{d^2} \end{pmatrix} \longrightarrow \begin{pmatrix} s_1 & s_{d+1} + i s_{d+2} & \cdots \\ s_{d+1} - i s_{d+2} & s_2 & \\ \vdots & & \ddots \\ & & & s_d \end{pmatrix}$$

$d^2 \times 1$ real vector $\qquad\qquad$ $d \times d$ Hermitian matrix

A little bit of linear algebra

- We denote with H^+ the adjoint of H, that is $H^+ = (H^T)^*$.
- A square matrix H is Hermitian iff $H^+ = H$.
- Any Hermitian matrix can be diagonalized by a unitary matrix:

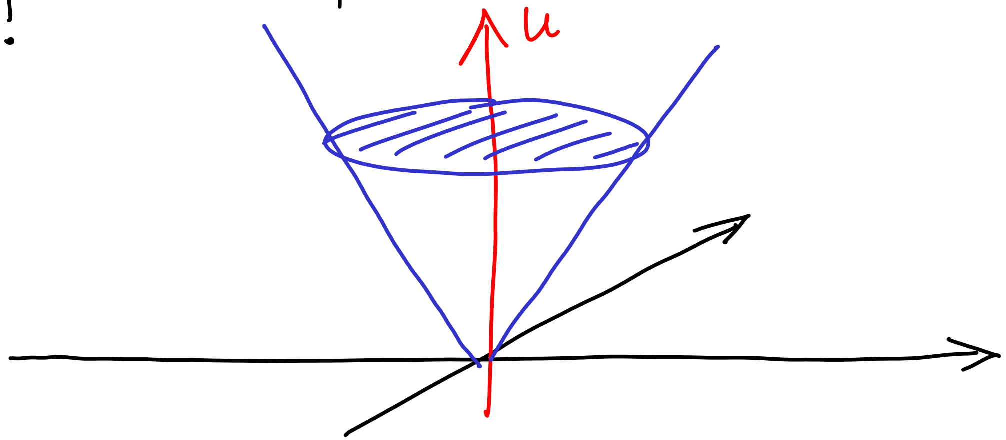
$$U H U^+ = \begin{pmatrix} h_1 & & 0 \\ & h_2 & \\ 0 & & \ddots \\ & & & h_d \end{pmatrix}, \quad \{h_k\} \text{ are the eigenvalues of } H.$$

- A Hermitian matrix H is positive semi-definite iff $h_k \geq 0 \ \forall k$, and we write $H \succcurlyeq 0$.

- Positive semidefinite matrices form a cone centered in 0, that is for any $H \succcurlyeq 0$ and any $\alpha \geq 0$, $\alpha H \succcurlyeq 0$.

Quantum Theory at last!

The quantum state space is the cone of positive semi-definite operators!



If this result looks unexplicable to you, congratulations:

- this is the only characteristics of quantum theory we introduce axiomatically rather than operationally.
- despite many efforts, no one really has an operational explanation for this.

(see e.g. M. Wilde, "Quantum Information Theory")

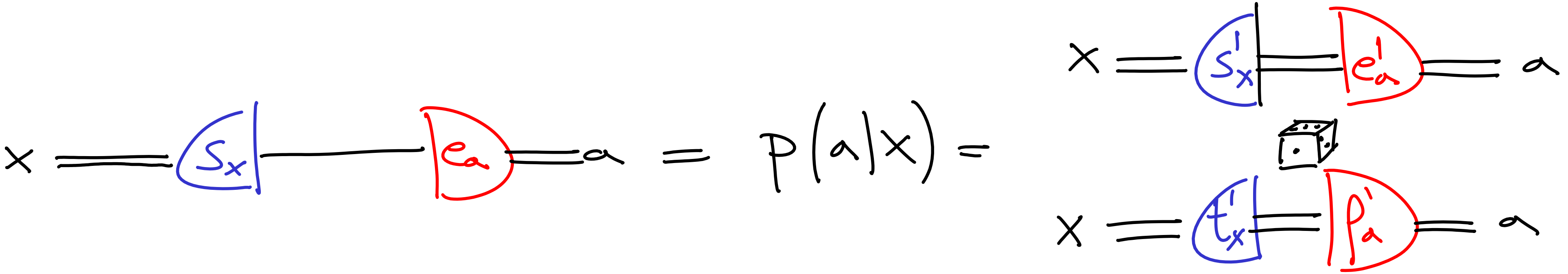
Summary of the building blocks of Quantum Theory

- Quantum states: positive semi-definite unit trace operators
- Quantum effects: positive semidefinite operators $\le \mathbb{1}$.
- Quantum unit effect: identity matrix $\mathbb{1}$.
- Quantum (destructive) measurement: collection $\{E_a\}$ of effects such that $\sum_a E_a = \mathbb{1}$.
- Quantum channel: completely positive trace preserving map.
- Reversible quantum channel: unitary
- Quantum instrument (non destructive measurement): collection $\{\mathcal{E}_a\}$ of completely positive maps such that $\sum_a \mathcal{E}_a$ is trace preserving.

Frenkel and Weiner's Theorem (Comm. Math. Phys. 340, 563)

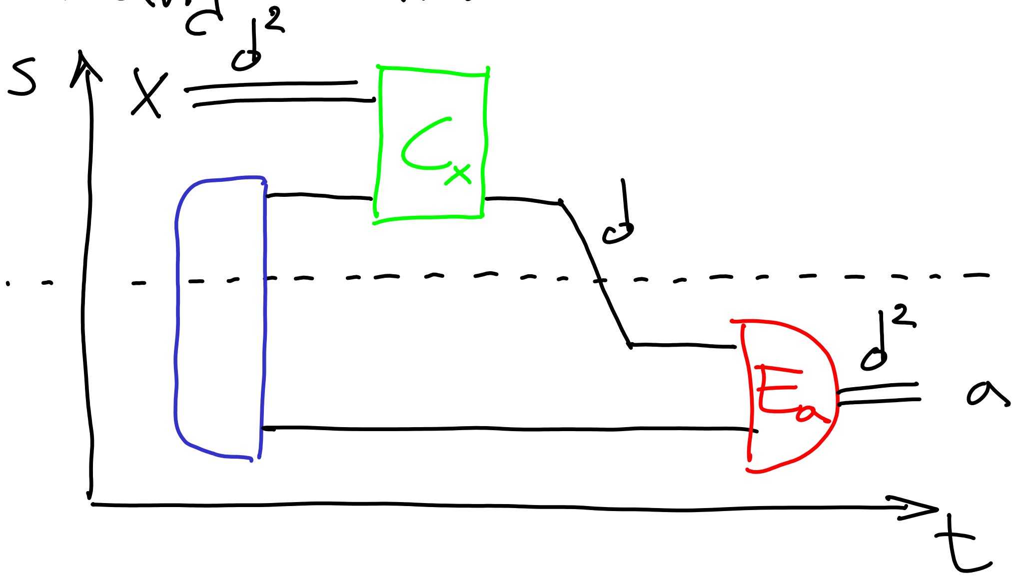
It is not possible to encode more than a d-dimensional classical system into a d-dimensional quantum system.

For any collection $\{s_x\}$ of quantum states and any measurement $\{e_a\}$ the probability $p(a|x)$ can be reproduced with classical states, measurements, and shared randomness.



Dense coding

It is possible to violate FW theorem by using shared entanglement!



$a = x$