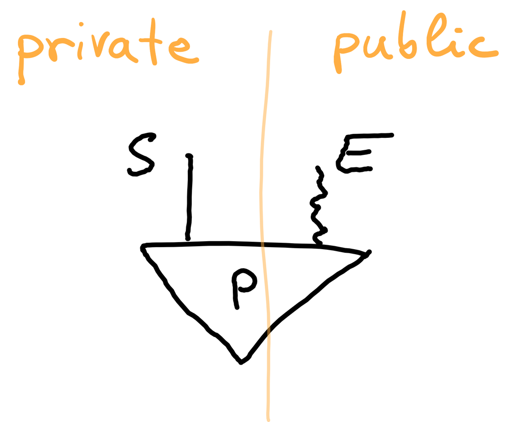
Resource Theory of Privacy and Private correlations

18/03/2024, Tallinn.

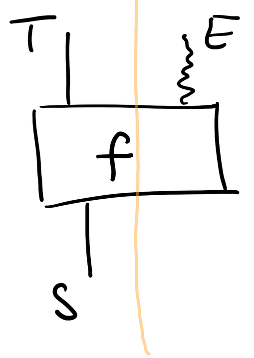
Talk by Tomáš Gonda (Uni of Innsbruck)
A collaboration with RW Spekkens & TC Fraser.

Introduction

- Resource objects: $[p, E] : I \to S$

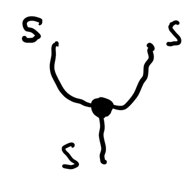


- Transformations: $[f, E] : S \to T$

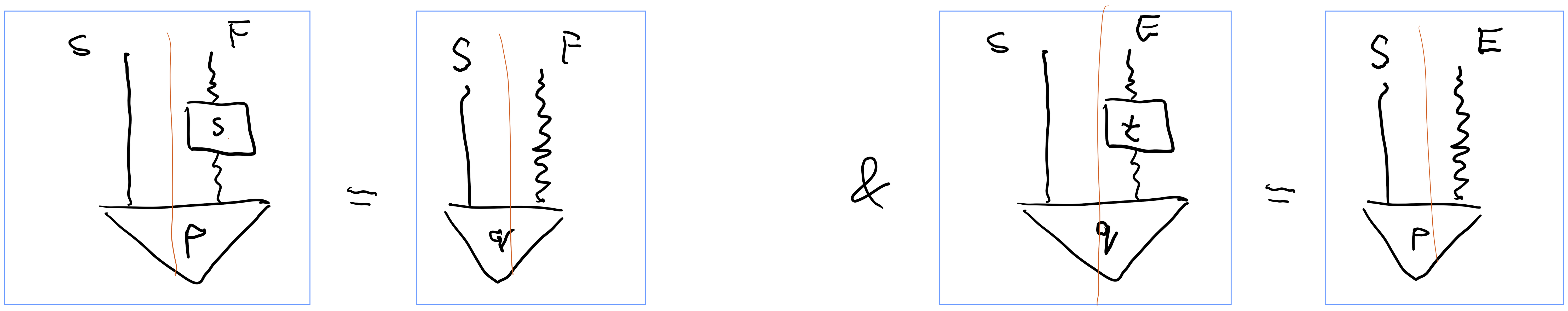


! no info. flow public → private

- Additional structure: gives a 'background' process theory C.

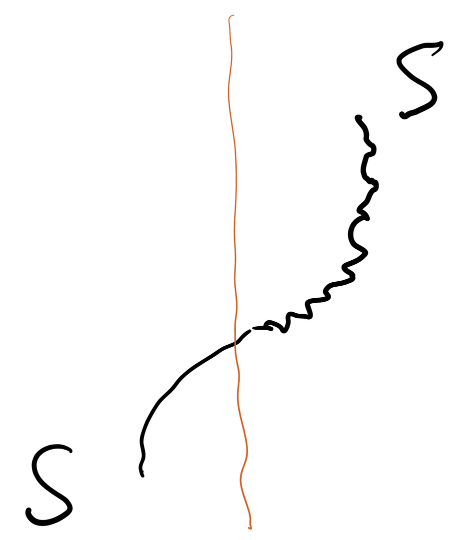
classical	quantum
joint prob. distribution	bipartite quantum state
stochastic map	quantum channel
copy  delete $\bar{1}_S$	delete $\bar{1}_S$

- Environment-processing (ep) equivalence $[p, E] \sim_{ep} [q, F]$ if

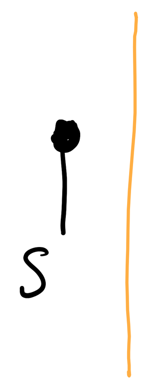


- Transparent operations

  - $[f, E] : S \to T$ is transparent if f is left-invertible.
  - $\mathrm{Trans}(C)$ is subcategory of $\mathrm{Leak}(C)$ containing transparent ones.
  - In FinStoch, e.g. $\begin{pmatrix} 1 & 0 \\ 0 & 1/2 \\ 0 & 1/2 \end{pmatrix}$ but not $\begin{pmatrix} 1/2 & 0 \\ 1/2 & 1/2 \\ 0 & 1/2 \end{pmatrix}$.

discarding: $[\mathrm{dump}_S, S] : S \to I$  is transparent.

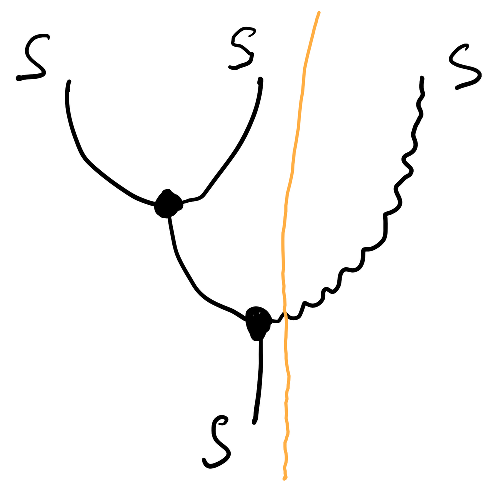
↳ the only transparent morphism up to $\sim_{ep}$.

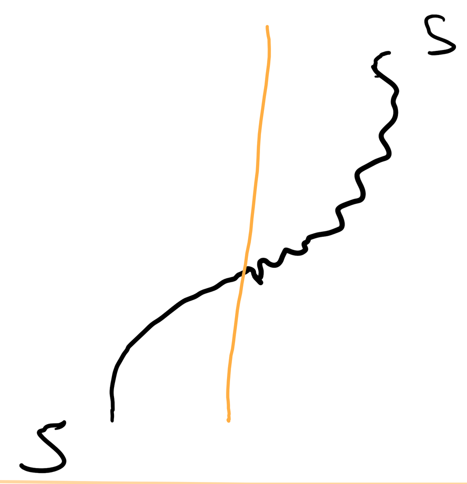
deleting 

is not transparent (we want E to be a universal environment)

Given a process theory $\mathcal{C}$, $\mathcal{L} := \mathrm{Trans}(\mathcal{C})/\sim_{ep}$ is a process theory.

Markov category structure: public copy & discarding





2 Resource theories of privacy, given by subcategories

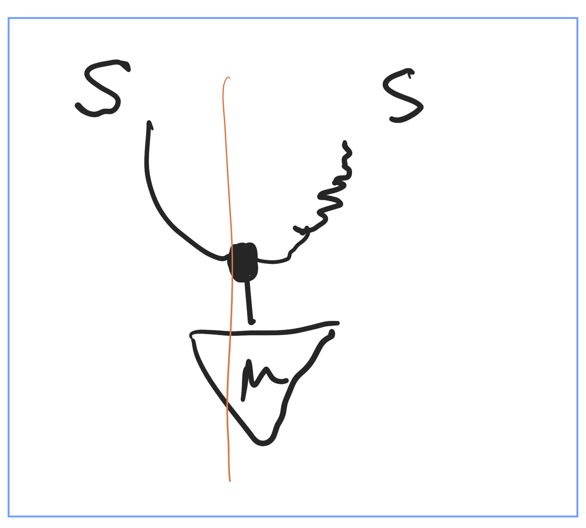
$\mathcal{L}_{pub} \subseteq \mathcal{L}$ of public operations (both classical and quantum)

$\mathcal{L}_{uip} \subseteq \mathcal{L}$ of universal-ignorance-preserving operations

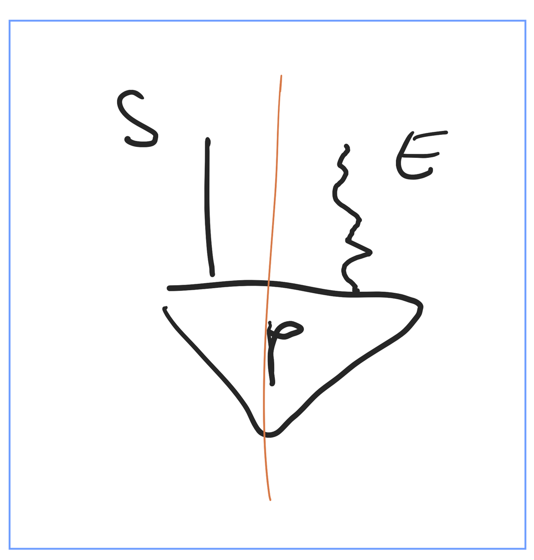
(quantum version unclear)

① Universal ignorance in Probability Theory

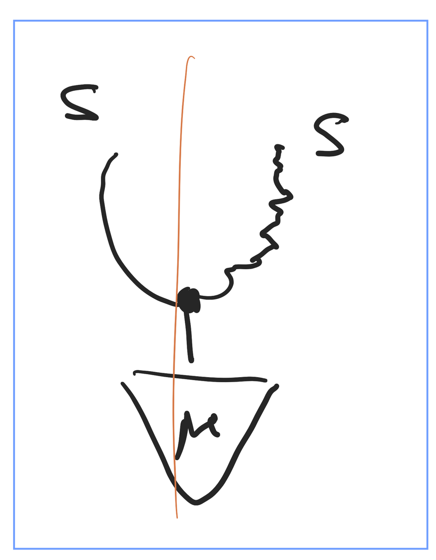
- **Public States**



or any

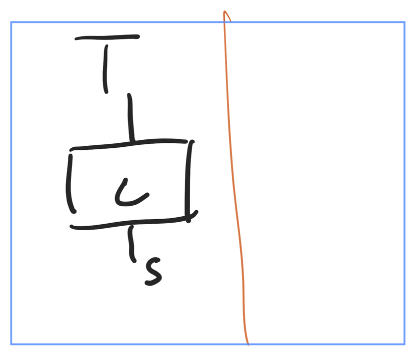


$\sim_{ep}$



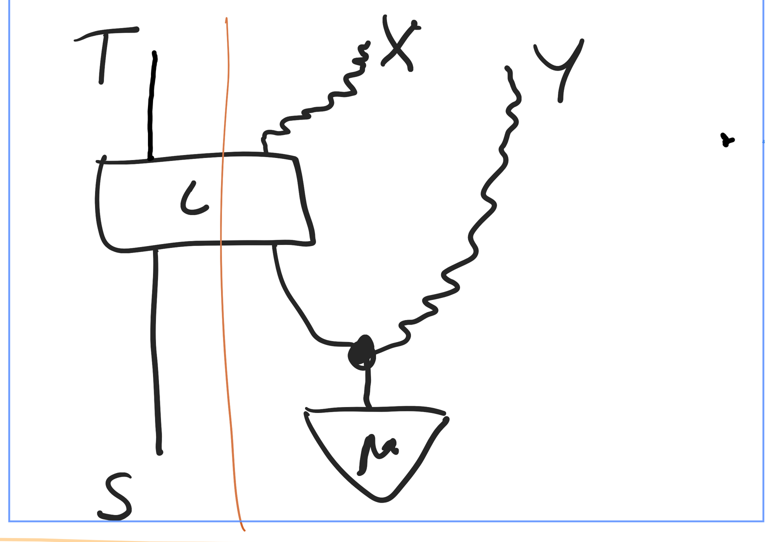
- **Public Operations**

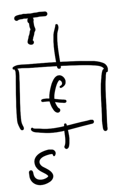
(i) discarding $[dump_S, S]$



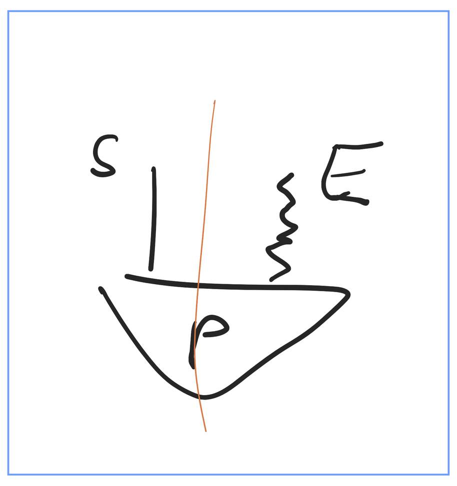
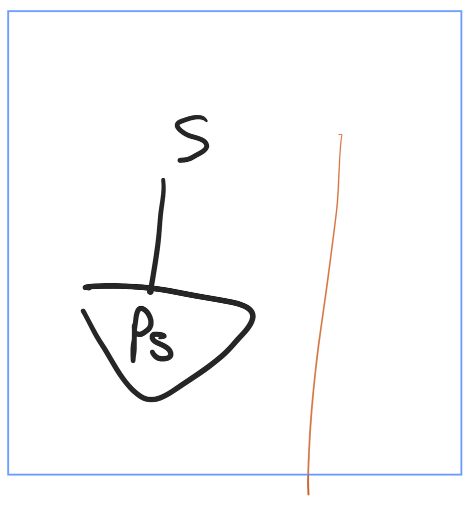
(ii) injective deterministic

(iii) public states

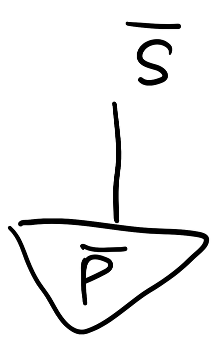
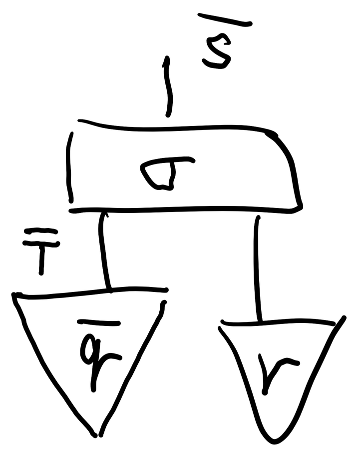
Proposition: Every public operation is ep-equivalent to  .

Proposition: Every  has a public dilation.

- **Resource Ordering**

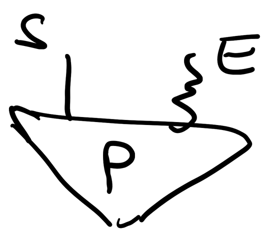
$[p, E]$ is *private* if  $\sim_{ep}$ 

Theorem: For private $[p, I]$, $[q, I]$ we have $[p, I] \succsim_{pub} [q, I]$ iff

 =  for a bijection σ.

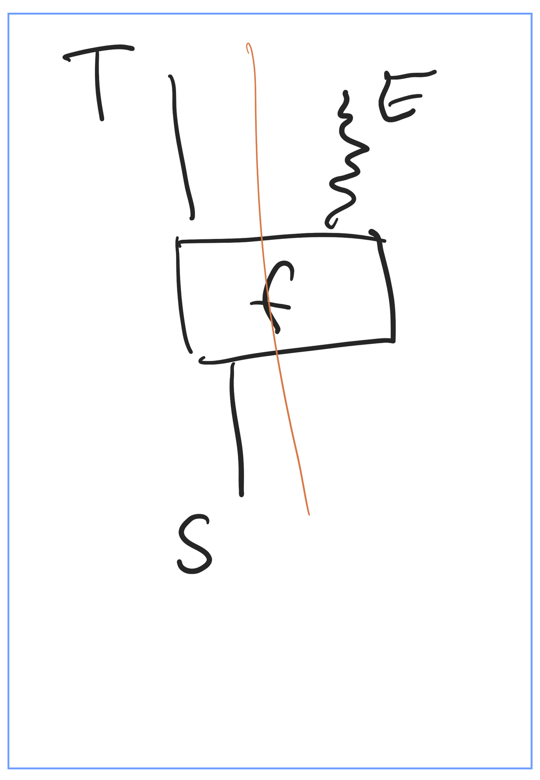
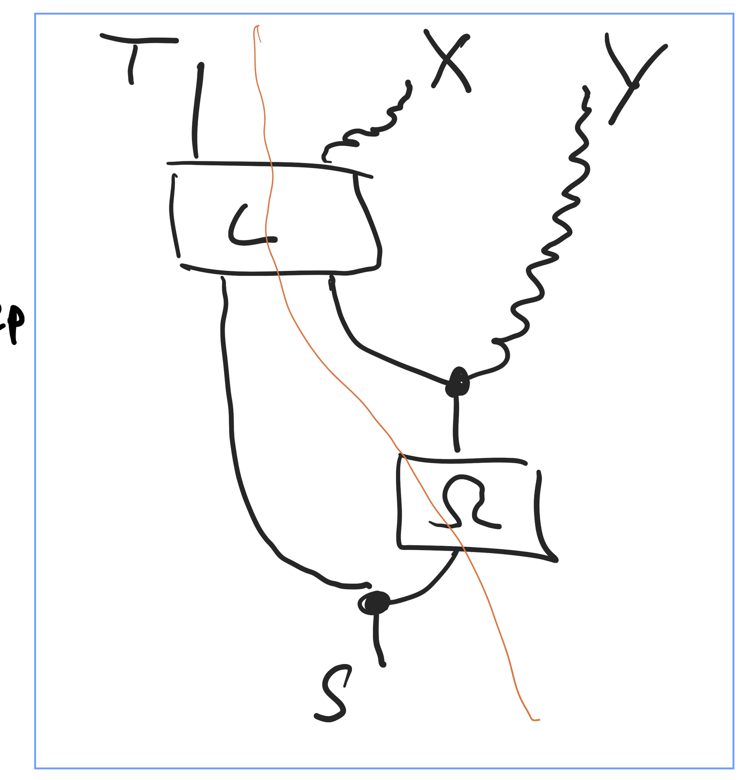
In particular $|\bar{S}|$ divides $|\bar{T}|$.

e.g. for $p = \begin{pmatrix} 1/2 \\ 1/2 \\ 0 \end{pmatrix}$, $\bar{p}$ is $\begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix}$. In general, see "Absolute continuity, supports and idempotent splitting in categorical probability".

Conjecture: For , $e \in E$, and $t \in \mathbb{N}$, the probability that t divides $|\mathrm{Supp}(p_{|E}(-\,|\,e))|$ is a resource monotone.

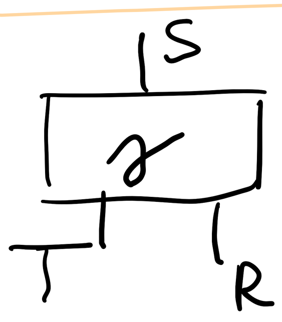
Question: How to characterize the full ordering?

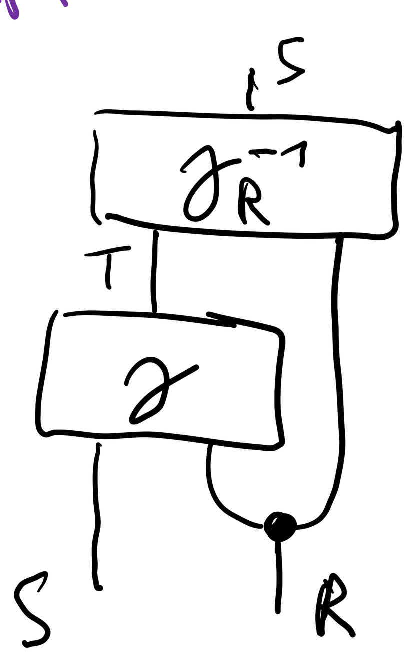
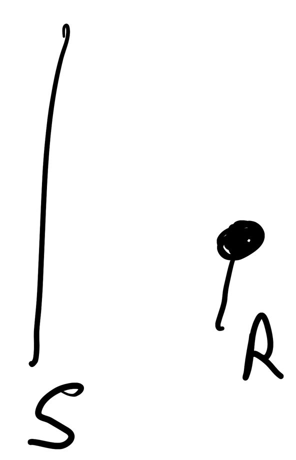
- **Universal Ignorance Preserving (UIP) Operations**

A trasparent $[f, E]$ is *UIP* if  $\sim_{ep}$ 

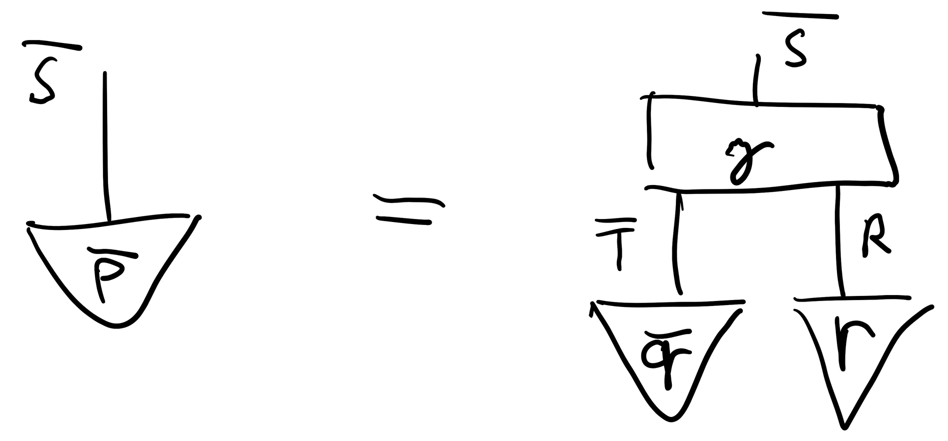
for ι injective deterministic.

Lemma: For public states, $\succsim_{pub}$ coincides with $\succsim_{UIP}$. They differ in general.

Def:  is *R-parametrized left invertible* if

$\exists\, \gamma_R^{-1} : S \otimes R \to T$ such that  = 

Theorem: For private states, $[p, I] \gtrsim_{UIP} [q, I]$ iff $\exists\, r: I \to R$ and a deterministic, R-parametrized left-invertible $g: T \otimes R \to \bar{S}$ such that



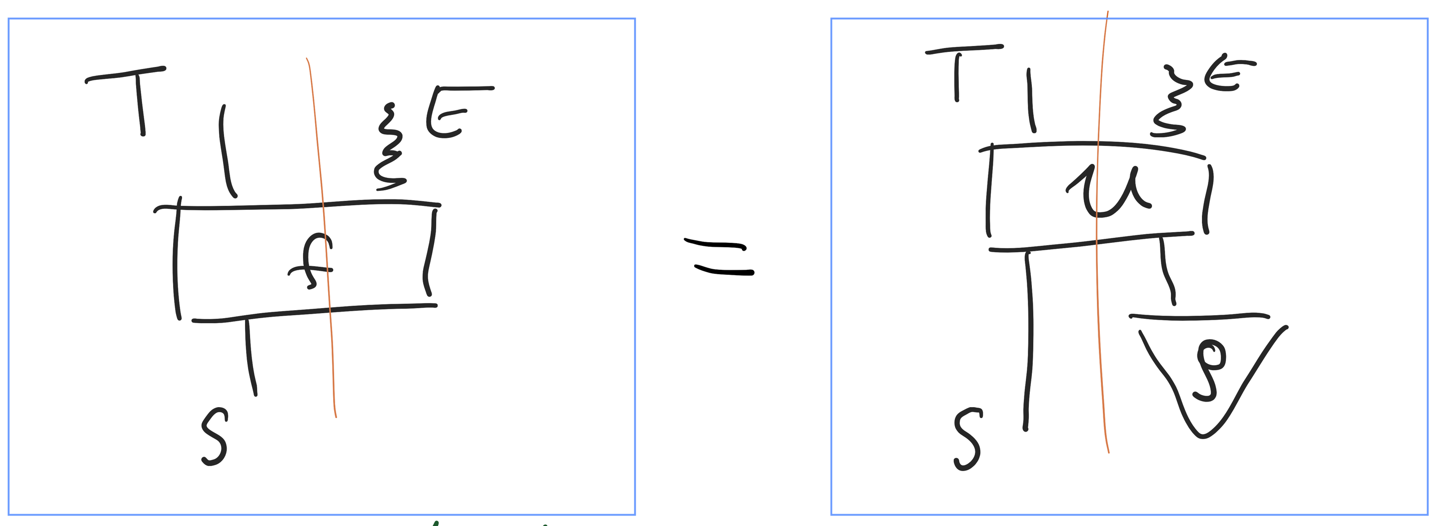
$(\star)$

For $|\bar{S}| = |\bar{T}|$ this says $\bar{q}$ majorizes $\bar{p}$.

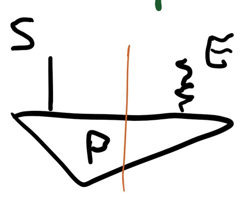
2 Universal Ignorance in Quantum Theory

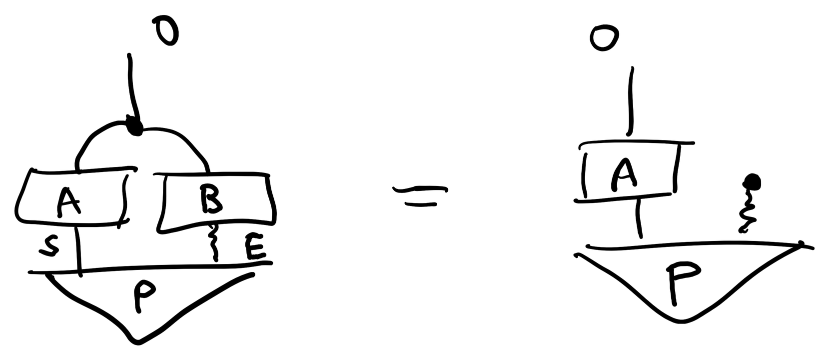
ep-equivalence, transparent operations, private states – as before

Theorem 2.1 [Nayak, Sen (2006)]: $[f, E]: S \to T$ is transparent iff $\exists$ a state $\rho: I \to R$ and a unitary $U: S \otimes R \to T \otimes E$ such that



- **Public quantum states**

Idea:  is public if $\forall$ measurements $A: S \to O$, $\exists$ a measurement $B: E \to O$ such that



Remark: A has to be a PVM else it could introduce private randomness.

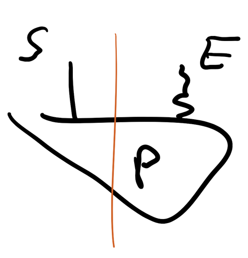
→ maximally entangled – public

→ diagonal state copied in eigen basis – not public

→ $|\psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$ for $S \cong \mathbb{C}^3$ – not public

→ product state $|\psi\rangle_S \otimes |\phi\rangle_E$ – not public

Thus isometries on S do NOT preserve public states.

Conjecture:  is public iff p is pure and has Schmidt rank $\dim(S)$.

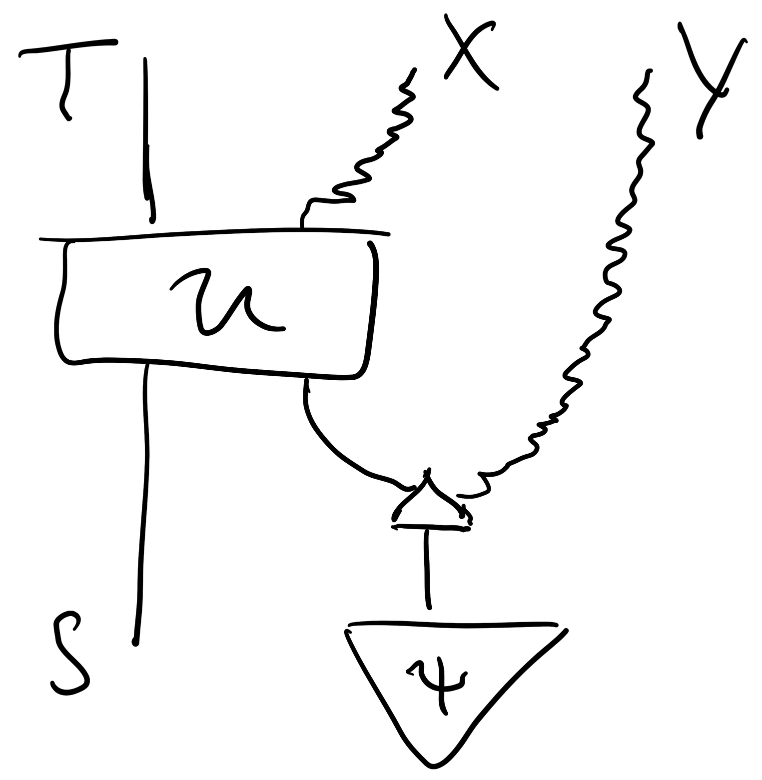
Question: What are public states for arbitrary C^*-algebras?

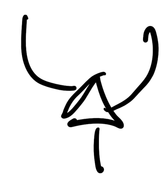
• Public Quantum Operations

(i) discarding a subsystem of S.

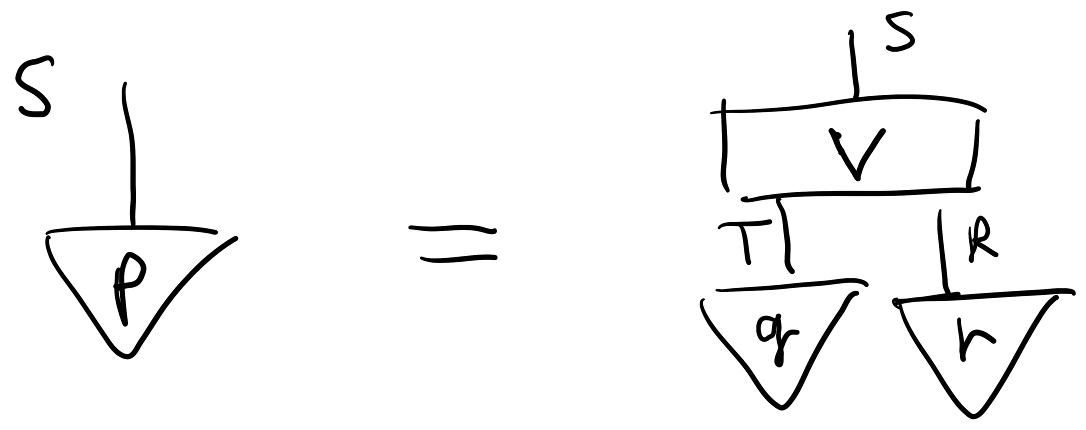
(ii) unitary maps on S.

(iii) public quantum states

Proposition: Every transparent public quantum operation has an rep-representative  for unitary $\mathcal{U}$,

pure ψ (with $\langle\psi|i\rangle \neq 0 \;\forall i$) and  being $|i\rangle \mapsto |i\rangle\otimes|i\rangle$.

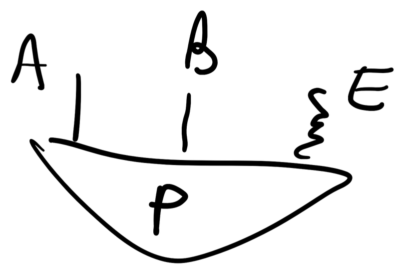
Lemma: For private $[p, I]$, $[q, I]$ we have $[p, I] \gtrsim_{pub} [q, I]$ iff $\exists$ an $r : I \to R$ and a unitary $V : T\otimes R \to S$ such that

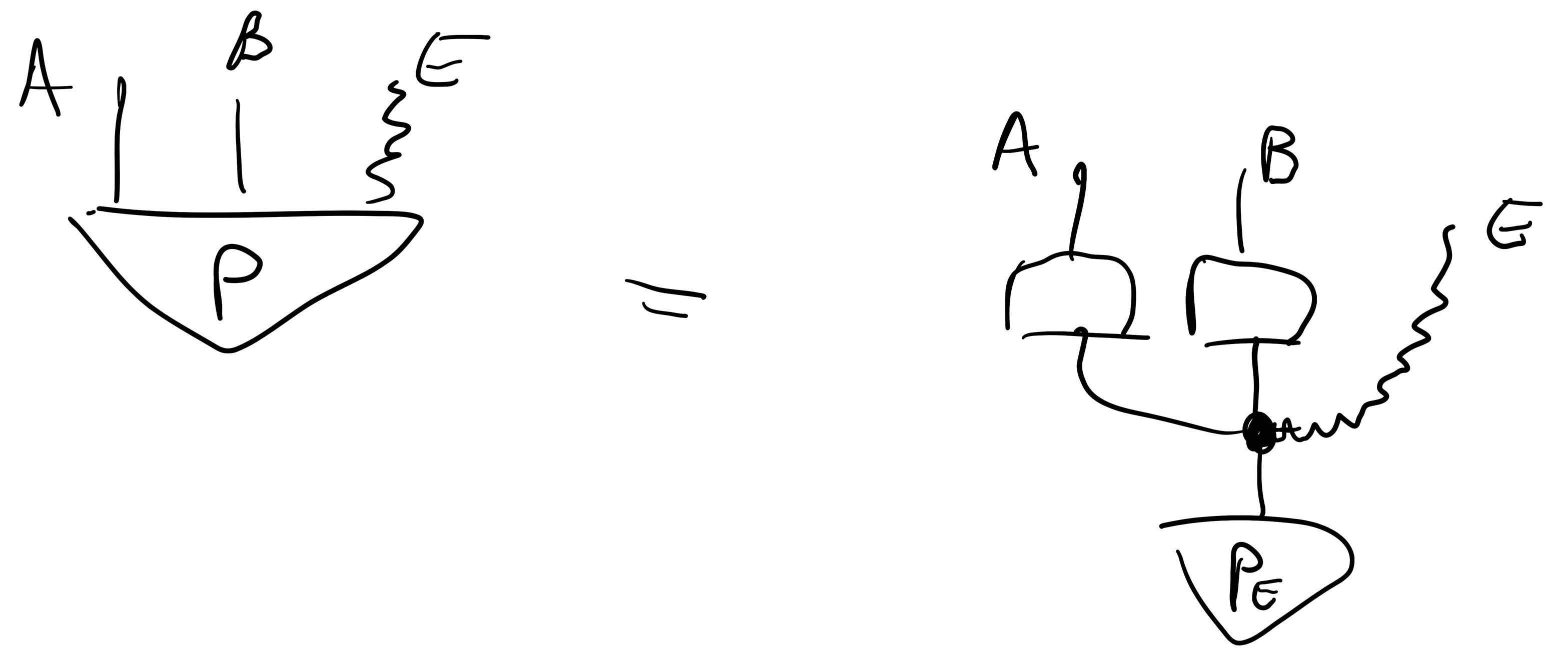


For pure states, this means $\dim S \geq \dim T$.

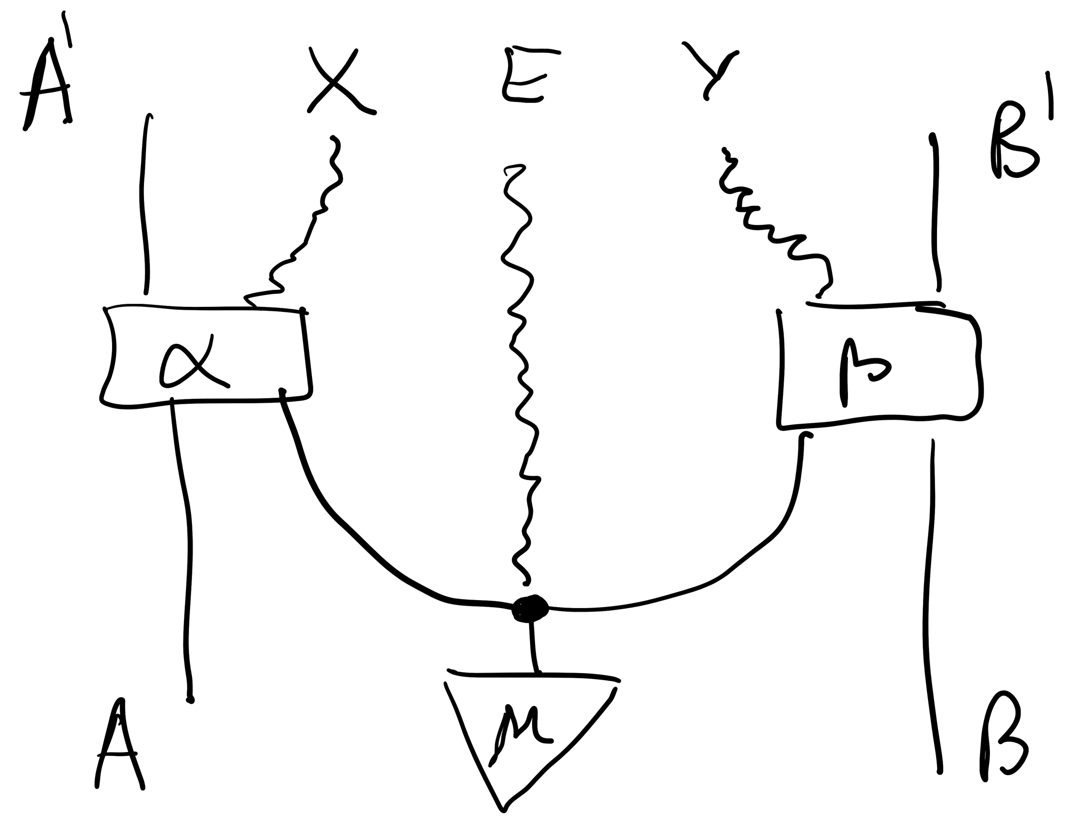
③ Shared Private Information

Two local parties, A, B.

- LOPSR, classical
  - (i) discard a subsystem of A or B
  - (ii) arbitrary local left-invertible operations
  - (iii) public correlations  s.t. $(A \perp B \mid E)_P$.

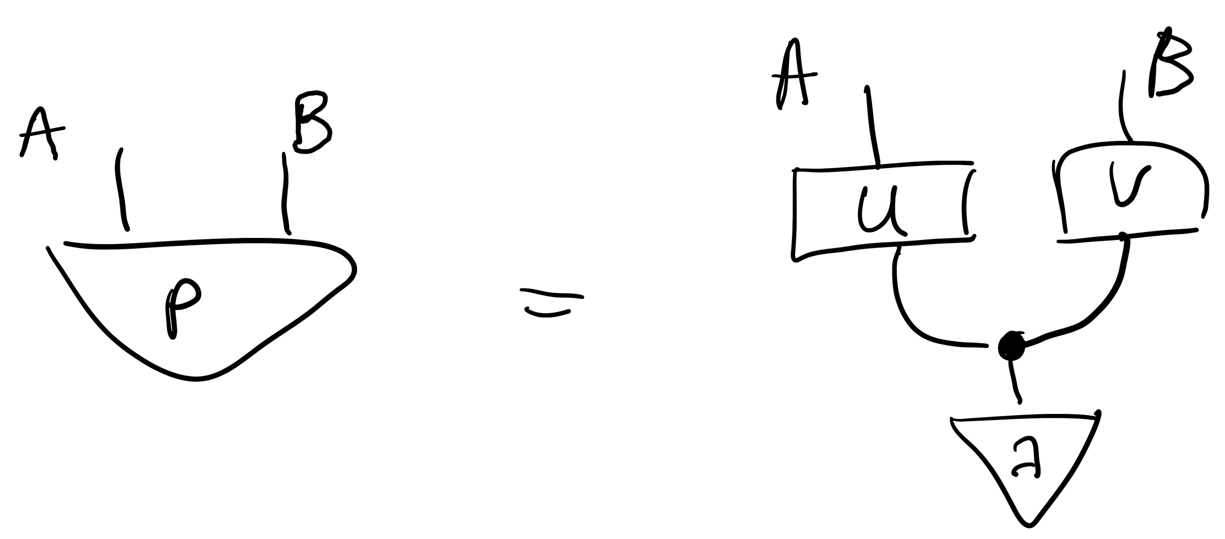
so 

Conjecture: A LOPSR operation has an $\sim_{ep}$-representative



for left-invertible α, β.

Among private states (fixed A, B), maximal elements are quasi-symmetric



for injective deterministic U, V.

Conjecture: For quasi-symmetric private states, $\succeq_{LOPSR}$ is like before for $\succeq_{pub}$.

Conjecture: p is quasi-symmetric iff it is nonsupplementation extremal, i.e.
↳ like pure in QT

$$q \succeq p \implies \exists r : q \sim p \otimes r$$

↳ resource order ↳ resource equivalence.

• QLOPSR, quantum

(i) discard a subsystem of A or B.

(ii) arbitrary local transparent operations.

(iii) public shared quantum state $I(A;B|E)_\rho = 0$

Conjecture: For pure private states, $\rho \succeq_{QLOPSR} \sigma \iff \rho \sim_{QLOPSR} \sigma \otimes r$ for some state $r_{R_A R_B}$.

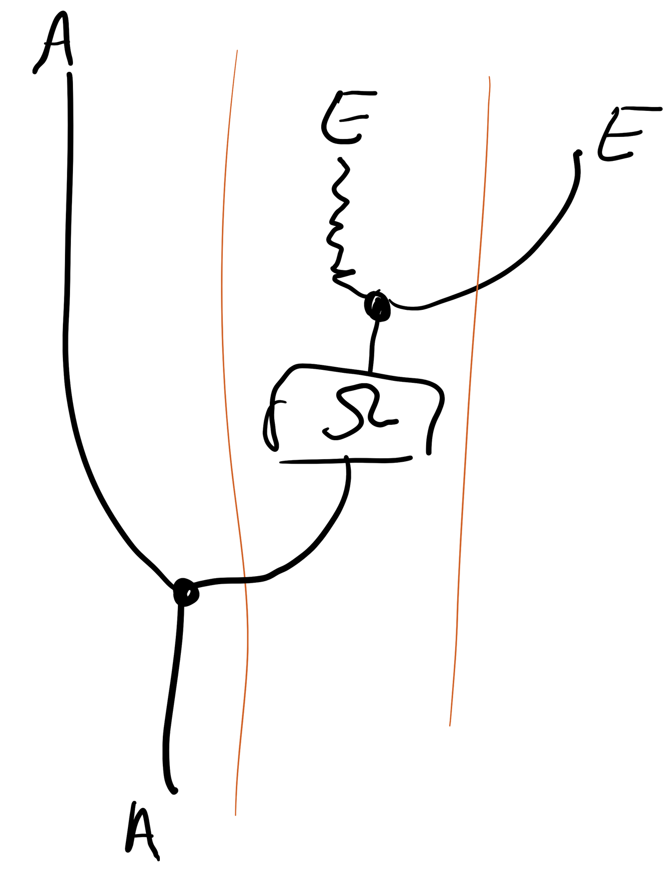
Conjecture: $\rho \sim_{QLOPSR} \sigma \iff$ they are interconvertible by local isometries (here ρ, σ are private, not necessarily pure)

Conjecture: Pure private states are the nonsupplementation extremal ones.

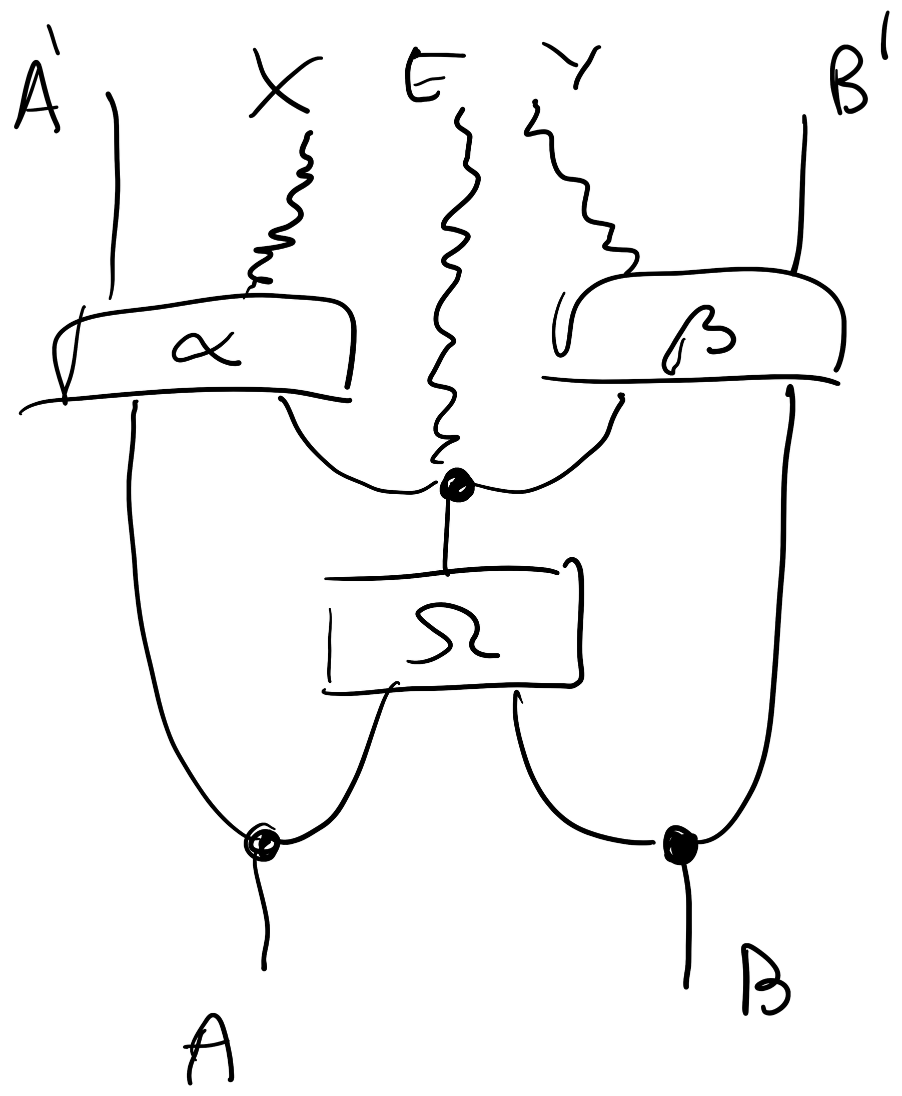
Conjecture: QLOPSR $\approx$ QLOSR (as resource orderings among private states)

- LOPC

LOPSR + public communication



Proposition: Every LOPC operation has an ~ep-representative



Theorem: For quasi-symmetric private states, $\succsim_{LOPC}$ is like (✪).

- QLOPC

QLOPSR + public (i.e. classical) communication

Conjecture: QLOPC ≈ LOCC (as preorders among public states)

Theorem [Nielsen (1999)]: For pure (private) quantum states,

$\succsim_{LOCC}$ is like (✪) for their Schmidt vectors.