Title: Purity and reversibility as a paradigm for Quantum Information Processing

Date: Feb 02, 2010 04:00 PM

URL: http://pirsa.org/10020070

Abstract: In this talk I will report on a recent work [arXiv:0908.1583], which investigates general probabilistic theories where every mixed state has a purification, unique up to reversible channels on the purifying system. The purification principle is equivalent to the existence of a reversible realization for every physical process, namely that to the fact that every physical process can be regarded as arising from the reversible interaction of the input system with an environment that is eventually discarded. From the purification principle one can also construct an isomorphism between transformations and bipartite states that possesses all structural properties of the Choi-Jamiolkowski isomorphism in Quantum Mechanics. Such an isomorphism allows one to prove most of the basic features of Quantum Information Processing, like e.g. no information without disturbance, no joint discrimination of all pure states, no cloning, teleportation, complementarity between correctable and deletion channels, no programming, and no bit commitment, without resorting to the mathematical framework of Hilbert spaces.

PURITY AND REVERSIBILITY AS A PARADIGM FOR QIP

Giulio Chiribella
Perimeter Institute for Theoretical Physics

Joint work with G M D'Ariano and P Perinotti
Quantum Information Theory Group
Pavia University

Quantum Foundations Seminar, Perimeter Institute,
February 2 2010

OUTLINE

- Background: operational-probabilistic theories
- Causal theories and theories with local discriminability
- The Purification Axiom and its consequences

OUTLINE

- Background: operational-probabilistic theories
- Causal theories and theories with local discriminability
- The Purification Axiom and its consequences

BACKGROUND: OPERATIONAL-PROBABILISTIC THEORIES

MOTIVATION OF THIS WORK

- Ultimate goal: deriving the mathematical framework of QM from few physical principles

- Intermediate goals: understanding structural aspects of QM on the basis of elementary concepts

  → simpler proofs of quantum results

  → less hypotheses needed for proving theorems

BACKGROUND: OPERATIONAL-PROBABILISTIC THEORIES

SYSTEMS AND TESTS

-Systems: A, B, C, ..., I = trivial system (nothing)

-Tests: $\{\mathcal{C}_i\}_{i \in X}$

A : input system

B : output system

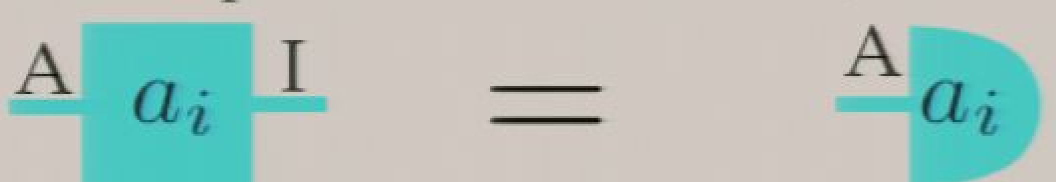
i: outcome

$\mathcal{C}_i$: event of the test

Special cases of tests:

- trivial input: preparation-test, ρ_i : preparation-event

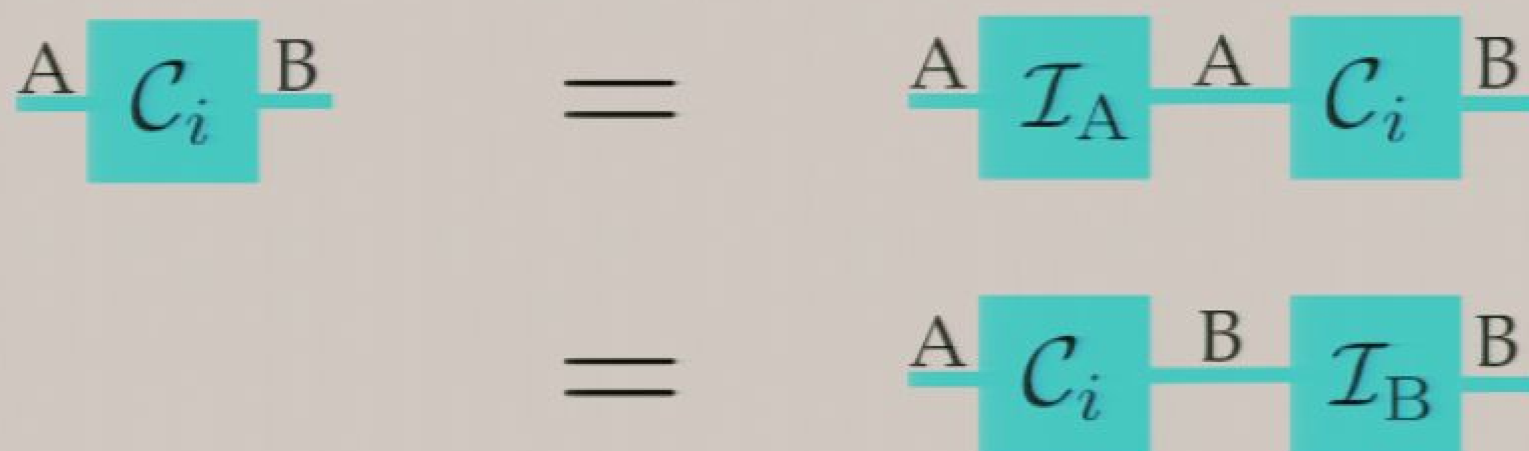
- trivial output: observation-test, a_i : observation-event



SEQUENTIAL COMPOSITION

-Cascades of tests:

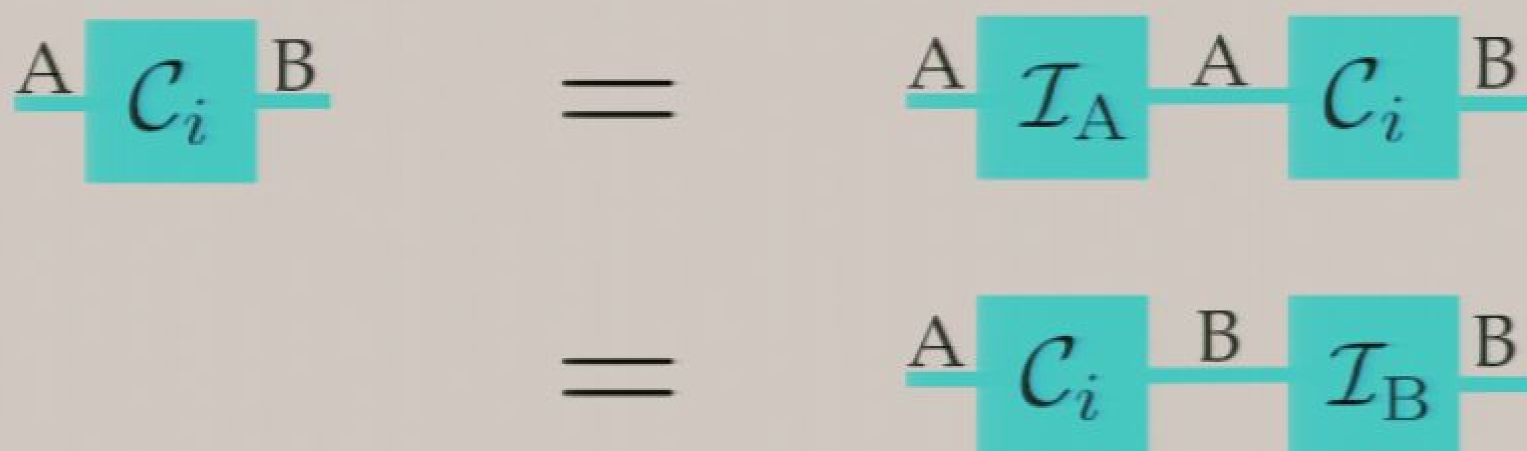
-Identity tests:



SEQUENTIAL COMPOSITION

-Cascades of tests:

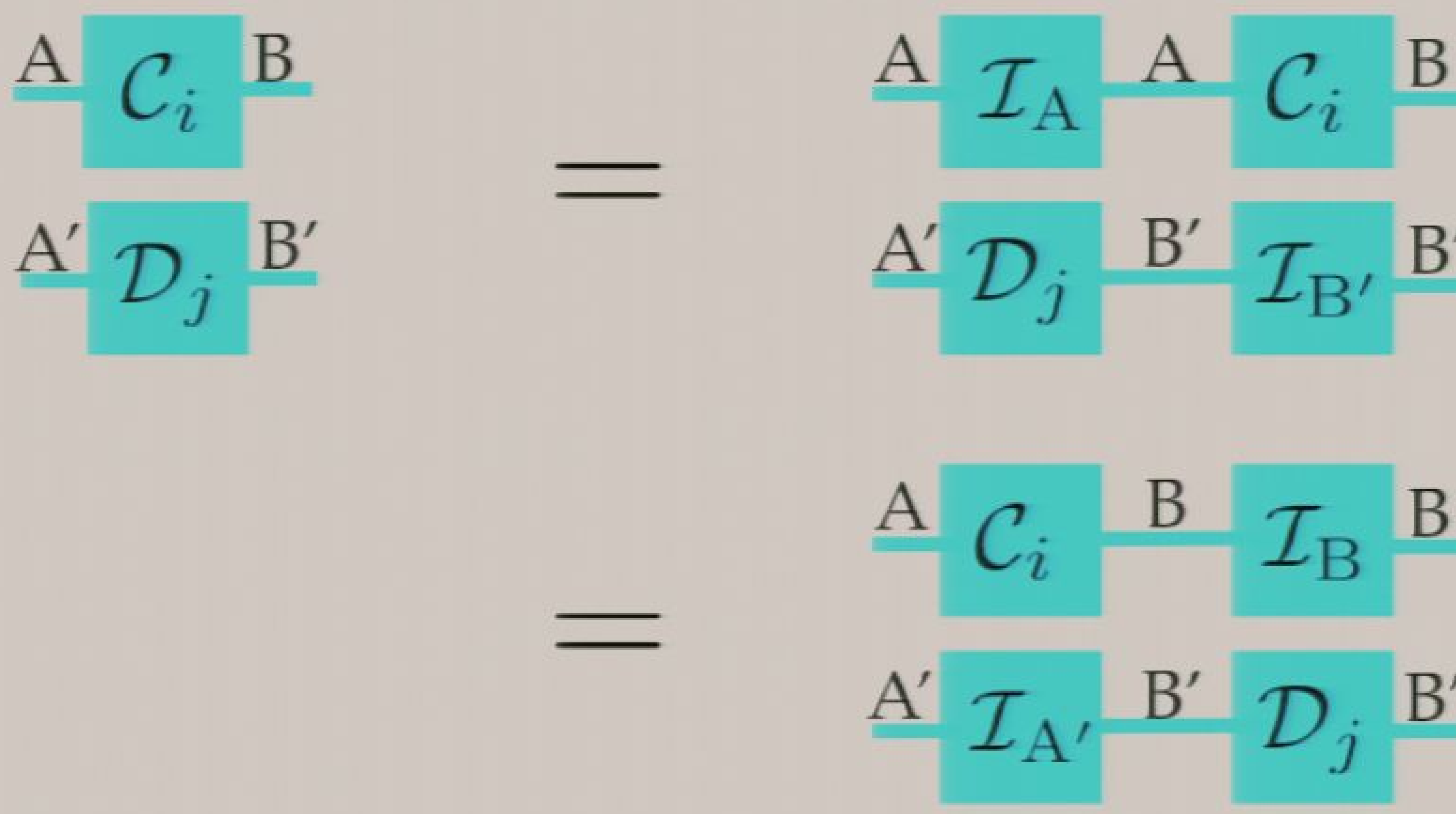
-Identity tests:



PARALLEL COMPOSITION

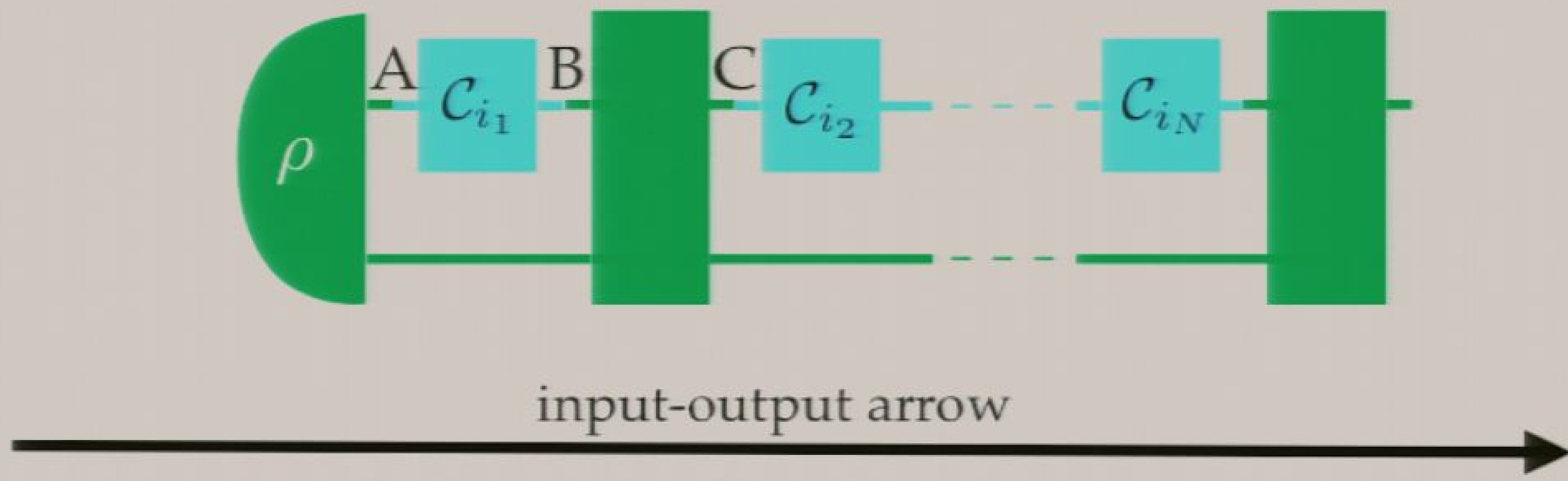
-Composite systems: AB, ABC   (trivial composition: A=AI=IA)

-Composite tests:



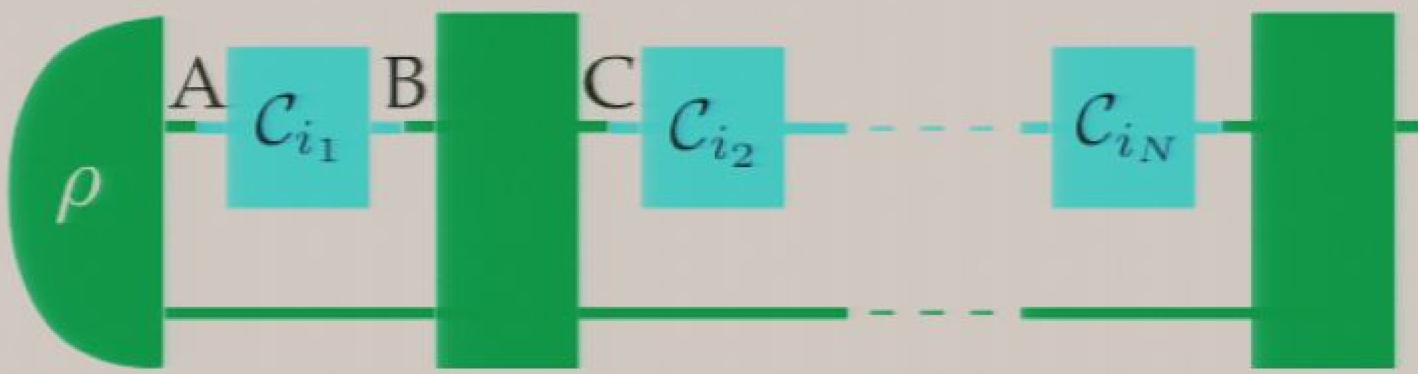
CIRCUITS

OPERATIONAL THEORY: a theory of devices that can be mounted to form circuits.



CIRCUITS

OPERATIONAL THEORY: a theory of devices that can be mounted to form circuits.



input-output arrow

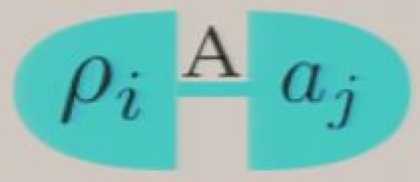
An operational theory is a language,
and its words are well-formed circuits.

PROBABILISTIC STRUCTURE

PROBABILISTIC STRUCTURE

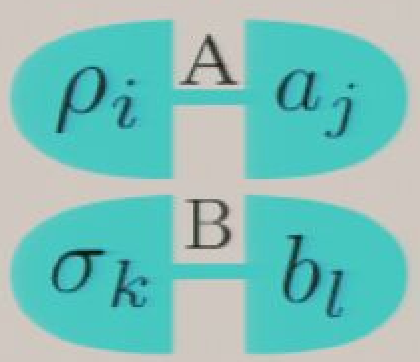
On top of the language of circuits we add a probabilistic structure:

- Events from the trivial system to itself are probabilities

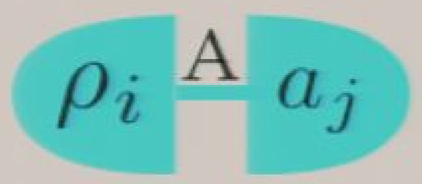


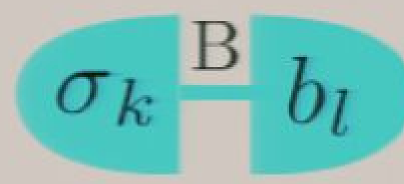
$$= \; p(a_j, \rho_i)$$

- Their composition is the product of probabilities:



$$=$$

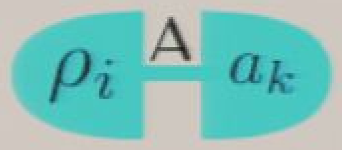


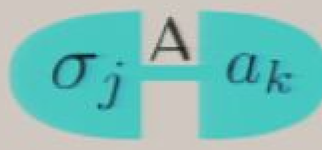


$$= \; p(a_j, \rho_i)p(b_l, \sigma_k)$$

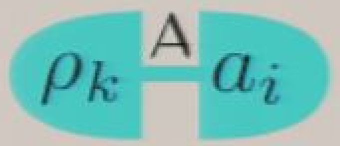
STATES, EFFECTS, AND TRANSFORMATIONS

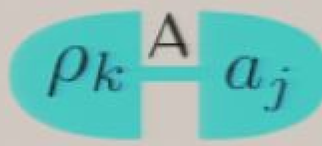
Equivalence classes of events (cf. Holevo's book):

$\rho_i \simeq \sigma_j$ if 

$=$ 

$\forall a_k \longrightarrow$ "states"

$a_i \simeq a_j$ if 

$=$ 

$\forall \rho_k \longrightarrow$ "effects"

States and effects span (finite dimensional) vector spaces

In general, events $\longrightarrow$ linear transformations

COARSE-GRAINING

Coarse-graining of a test: a new test obtained by joining outcomes

$$\mathcal{C}'_j = \sum_{i \in \mathrm{X}_j} \mathcal{C}_i$$

Single-outcome tests $\longrightarrow$

- deterministic states
- deterministic effects
- deterministic transformations ("channels")

For deterministic $\rho, \mathcal{C}, e$:

$= 1$

CAUSAL THEORIES

DEFINITION

A theory is causal if the probability of an outcome is independent of the choice of subsequent tests:

$$\sum_j \rho_i \stackrel{\mathrm{A}}{\text{—}} a_j = \sum_k \rho_i \stackrel{\mathrm{A}}{\text{—}} b_k$$

In other words, the choice of a test can only affect the outcome probabilities of tests that happen "later".

DEFINITION

A theory is causal if the probability of an outcome is independent of the choice of subsequent tests:

$$\sum_j \rho_i \stackrel{A}{\text{—}} a_j = \sum_k \rho_i \stackrel{A}{\text{—}} b_k$$

In other words, the choice of a test can only affect the outcome probabilities of tests that happen "later".

The input-output arrow becomes the arrow of the information flow

EQUIVALENT CONDITIONS

Equivalent condition #1: there is a unique normalized effect e

Marginal states are uniquely defined (no-signaling)

Equivalent condition #2: the choice of a test can be conditioned by the outcomes of previous tests

EQUIVALENT CONDITIONS

Equivalent condition #1: there is a unique normalized effect e

Marginal states are uniquely defined (no-signaling)

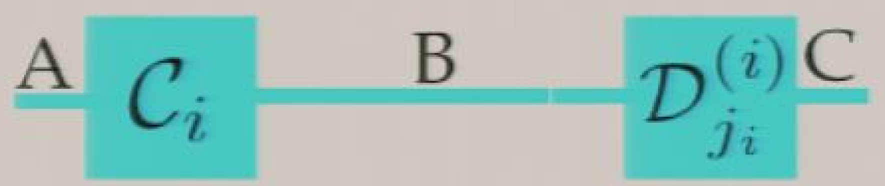
Equivalent condition #2: the choice of a test can be conditioned by the outcomes of previous tests

EQUIVALENT CONDITIONS

Equivalent condition #1: there is a unique normalized effect e

Marginal states are uniquely defined (no-signaling)

Equivalent condition #2: the choice of a test can be conditioned by the outcomes of previous tests



DEFINITION

A theory is causal if the probability of an outcome is independent of the choice of subsequent tests:

$$\sum_j \rho_i \overset{\mathrm{A}}{\text{—}} a_j = \sum_k \rho_i \overset{\mathrm{A}}{\text{—}} b_k$$

In other words, the choice of a test can only affect the outcome probabilities of tests that happen "later".

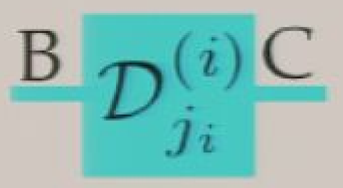
The input-output arrow becomes the arrow of the information flow

EQUIVALENT CONDITIONS

Equivalent condition #1: there is a unique normalized effect e

Marginal states are uniquely defined (no-signaling)

Equivalent condition #2: the choice of a test can be conditioned by the outcomes of previous tests



EQUIVALENT CONDITIONS

Equivalent condition #1: there is a unique normalized effect e

Marginal states are uniquely defined (no-signaling)

Equivalent condition #2: the choice of a test can be conditioned by the outcomes of previous tests

CONVEXITY

CONVEXITY

Theorem: If a theory is causal and non-deterministic, then the sets of states, effects, and transformations of every system are convex.

Mixed state:

$$\rho^{\mathrm{A}} = (1-p)\, \sigma^{\mathrm{A}} + p\, \tau^{\mathrm{A}}$$

with $\sigma \neq \tau, \qquad p \in (0,1)$

Mixed state: coarse-graining of a more refined preparation-test

Pure state: no possibility of refinement

EQUIVALENT CONDITIONS

Equivalent condition #1: there is a unique normalized effect e

Marginal states are uniquely defined (no-signaling)

Equivalent condition #2: the choice of a test can be conditioned by the outcomes of previous tests

CONVEXITY

INTERNAL STATES

Refinement set D_ρ := { states in the convex decomposition of ρ }

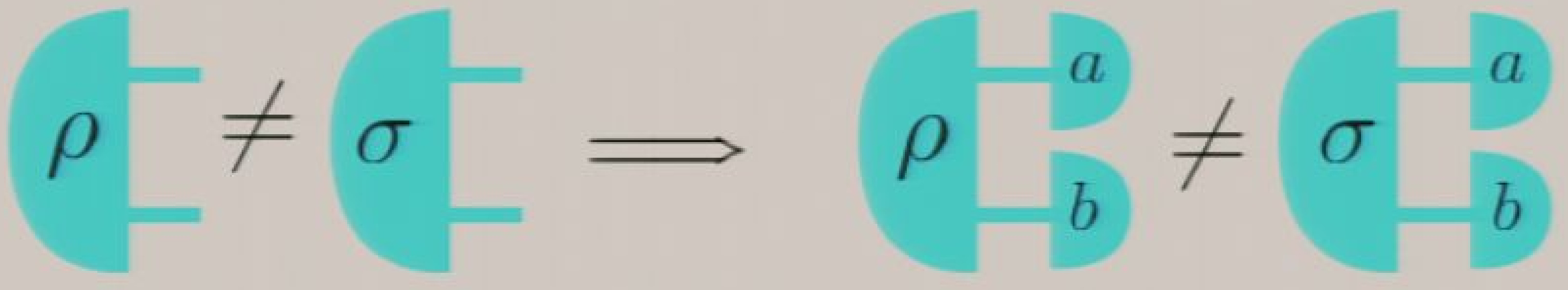
$$\rho^{A} = (1-p)\,\sigma^{A} + p\,\tau^{A} \longrightarrow \sigma \in D_\rho$$

(in QM: states with support contained in the support of ρ)

Internal state: ρ is internal if D_ρ contains all states
(in QM: internal state = full rank density matrix)

THEORIES WITH LOCAL DISCRIMINABILITY

LOCAL DISCRIMINABILITY



If two states are distinguishable,
they are distinguishable locally (with error prob less than $1/2$)

LD is equivalent to the possibility of making state tomography with only local devices.

GENERALIZATIONS

Convexity and local discriminability
are not essential for most of the results presented in the following.

(e.g. most result hold for QM on real Hilbert spaces)

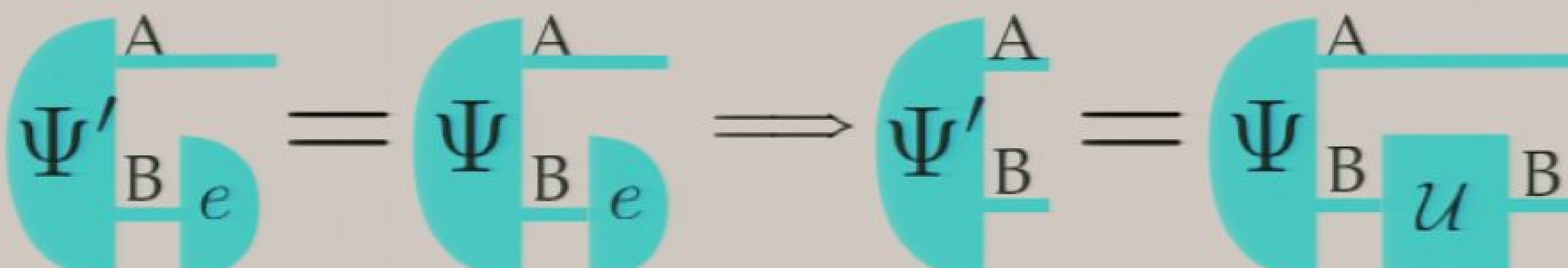
In this presentation, however, I will stick to the simplest scenario and assume both.

THEORIES WITH PURIFICATION

THE PURIFICATION AXIOM

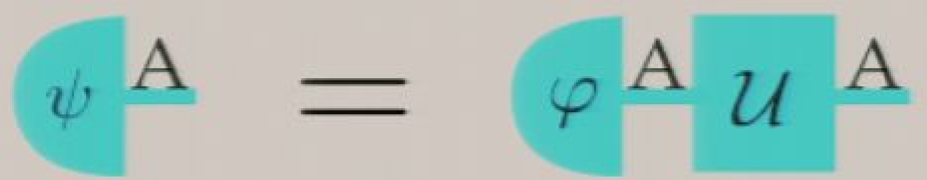
- Existence: For every state ρ of A
  there is a system B and a pure state Ψ_ρ of AB
  such that

- Uniqueness up to (reversible) transformations on the purifying system:



FIRST CONSEQUENCES

- There are entangled states
- Every couple of pure states is connected by a reversible transformation



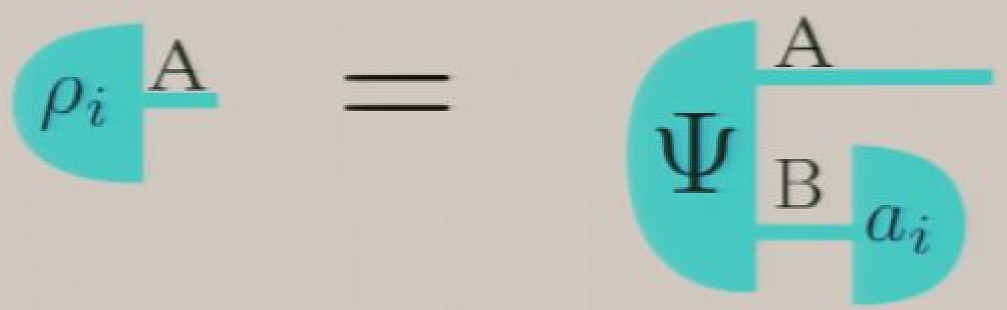
- Unique invariant state for every system:

- Purity $\Longrightarrow$ independence from the rest of the world

PURIFICATION OF ENSEMBLES

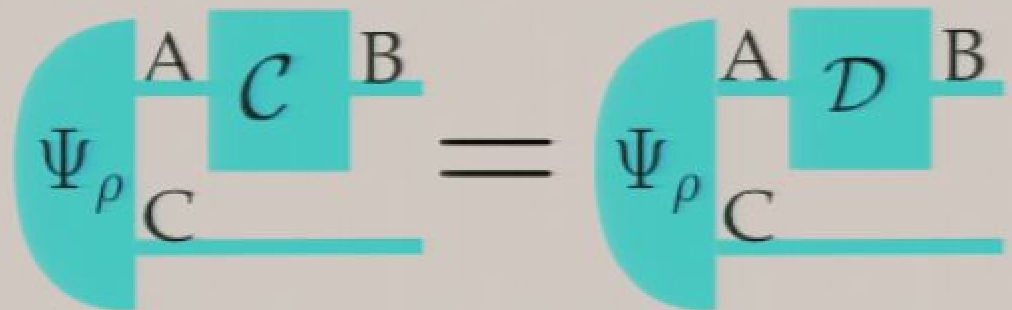
Purification of states $\longrightarrow$ purification of ensembles

Theorem:
For every preparation-test $\{\rho_i\}_{i\in X}$ of A
there is a system B,
a pure state Ψ of AB
and an observation-test $\{a_i\}_{i\in X}$ of B
such that

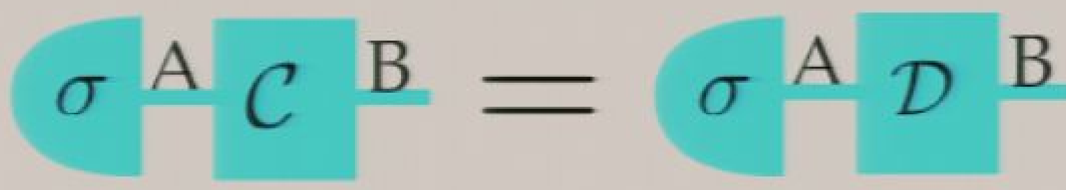


EQUALITY UPON INPUT OF ρ

Ψ_ρ = purification of ρ

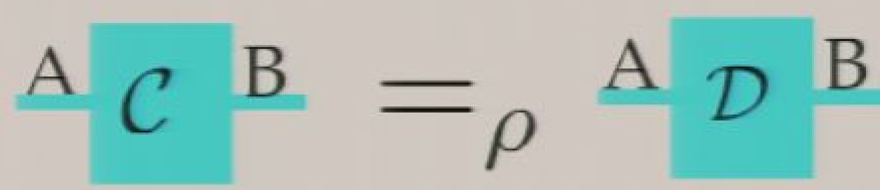


$\Longleftrightarrow$



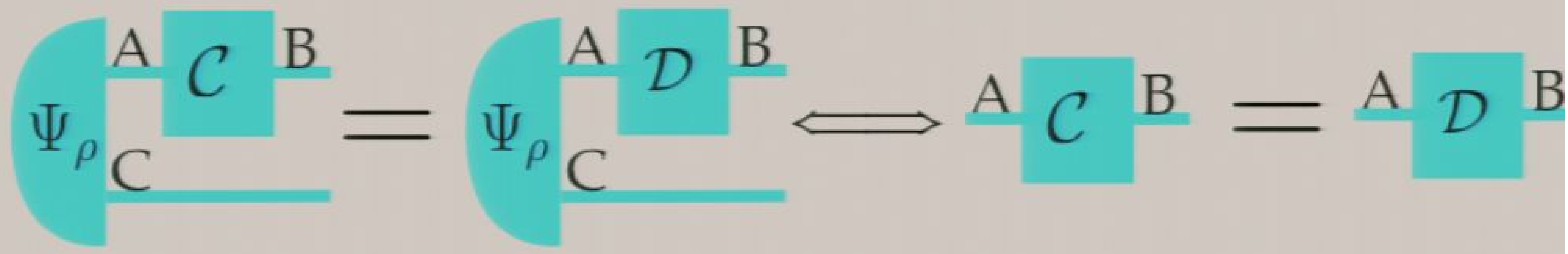
$\forall \sigma \in D_\rho$

$\overset{\text{def}}{\Longleftrightarrow}$



ANCILLA -ASSISTED PROCESS TOMOGRAPHY

ρ internal $\Longrightarrow$ Ψ_ρ allows for process tomography



Pure faithful state $\Longrightarrow$ • no information without disturbance

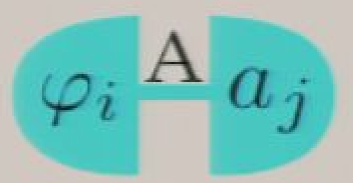
• no cloning of pure states

NO CLONING OF PURE STATES

Perfect cloning $\Longrightarrow$ perfect discrimination

Barnum, Barret, Leifer, Wilce, Phys. Rev. Lett. 99,240501 (2007)
[see also GC, D'Ariano, Perinotti, Phys. Rev. Lett. 101, 180504 (2008)]

Discriminabiliy
+ finite dimension $\Longrightarrow$ finite number of pure states $\{\varphi_i\}_{i\in X}$



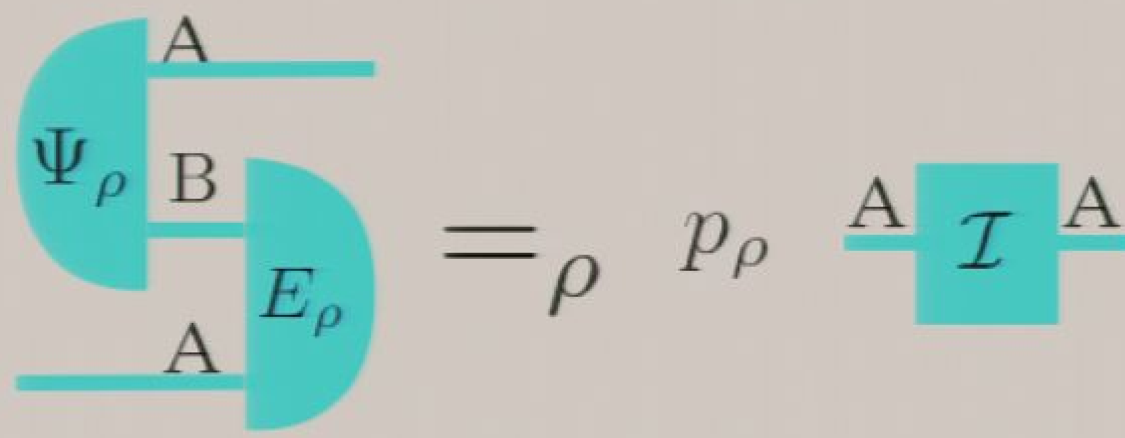
$= \delta_{ij} \Longrightarrow$

Cloning $\Longrightarrow$ non-disturbing test
with non-zero information $\Longrightarrow$ absurd

TELEPORTATION, STORING & RETRIVING, AND THE CHOI-JAMIOLKOWSKI ISOMORPHISM

PROBABILISTIC TELEPORTATION

Theorem: for every state ρ on A
there is an effect E_ρ on AB such that



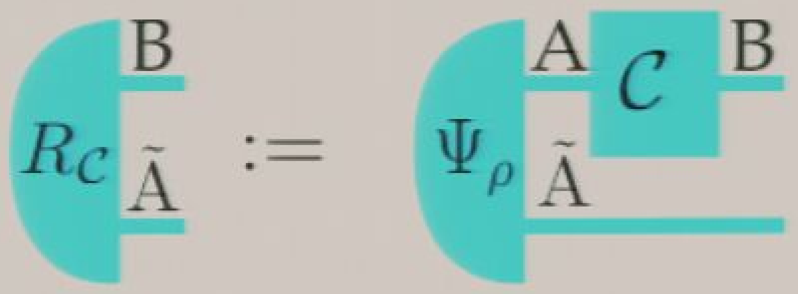
for internal states: ordinary teleportation

cf. Coecke's approach, where the above diagram is the main axiom

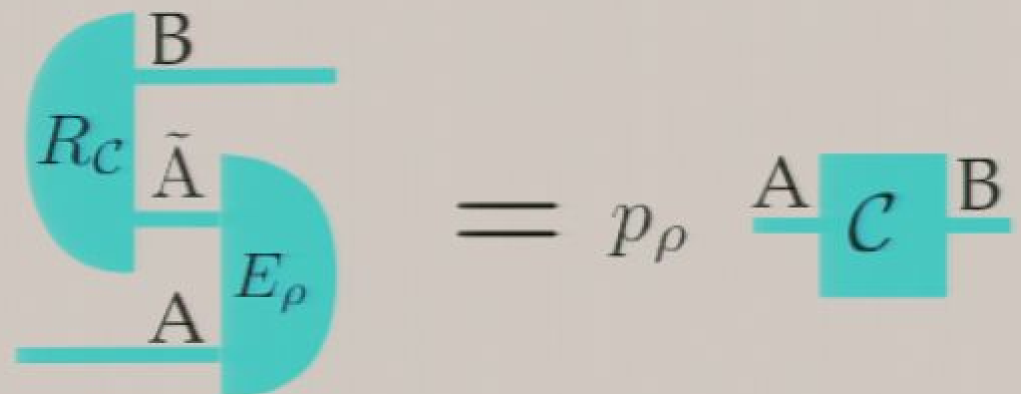
General bound: $$p_\rho \leq \frac{1}{\dim(\mathrm{St}(A))}$$

STORING AND PROBABILISTIC RETRIEVING

"Choi-Jamiolkowski" state (storing a channel in the state of a physical system)



Probabilistic retrieving:



ENTANGLEMENT BREAKING CHANNELS

- Channel $\mathcal{C}$ is entanglement breaking (upon input of ρ)

$\Longleftrightarrow$ it is measure-and-prepare (upon input of ρ)

$\Longleftrightarrow$ CJ state (defined by a purification of ρ) is separable

cf. Horodecki, Shor, and Ruskai for QM

COMPLETENESS OF THEORIES WITH PURIFICATION

Theorem: a theory with purification is completely identified once we declared the state space of every system.

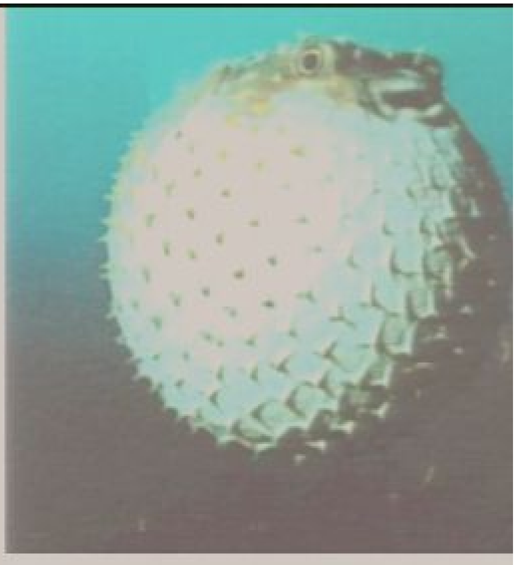
Every mathematically admissible map MUST be a physical transformation allowed by the theory.

COMPLETENESS OF THEORIES WITH PURIFICATION

Theorem: a theory with purification is completely identified once we declared the state space of every system.

Every mathematically admissible map MUST be a physical transformation allowed by the theory.

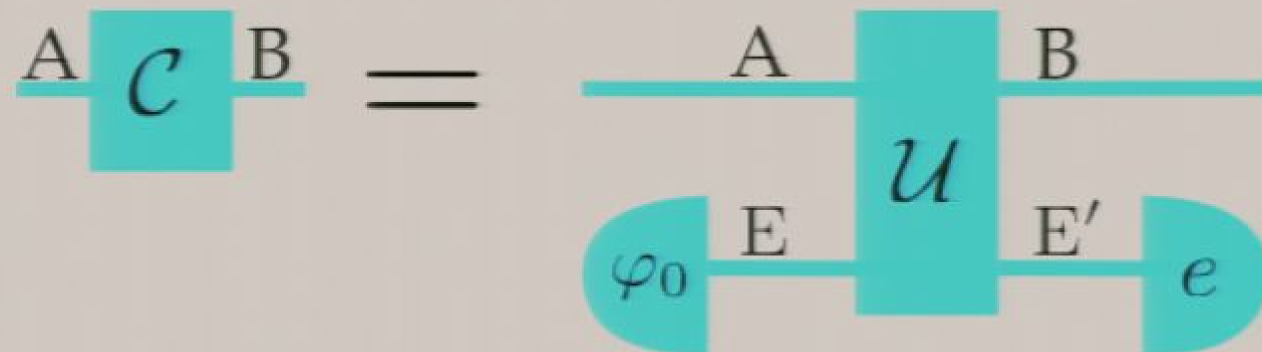
This explains why it is so difficult to invent new examples of theories with purification.



REVERSIBLE DILATIONS

DILATION OF CHANNELS

Theorem: For every channel $\mathcal{C}$ from A to B
there exist two systems E and E′ ,
a pure state φ_0 of E ,
and a reversible channel $\mathcal{U}$ from AE to BE′ such that

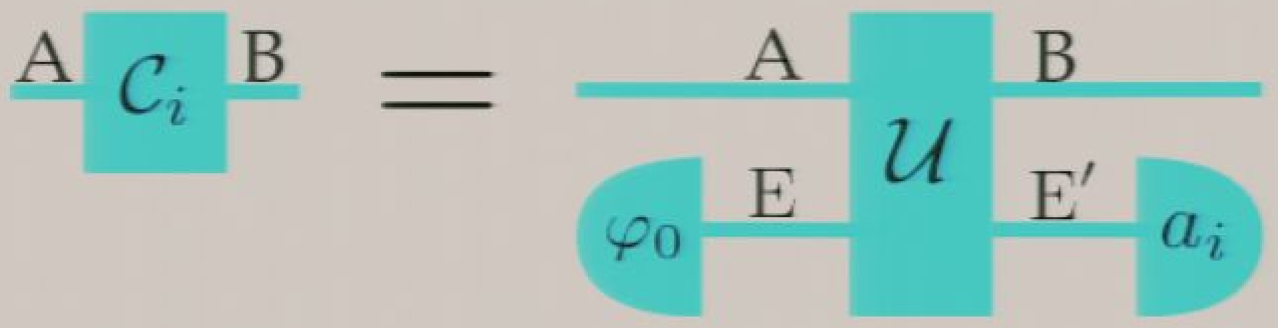


The dilation is unique up to reversible channels on E′
(cf Stinespring theorem in QM)

Irreversibility can be always thought as arising from
→ the loss of control over some system.
Information cannot be erased, it can only be discarded.

DILATION OF TESTS

Theorem: For any test $\{\mathcal{C}_i\}_{i\in X}$ from A to B
there exist a pure state φ_0 on E
a reversible channel $\mathcal{U}$ from AE to BE′
and an observation-test $\{a_i\}_{i\in X}$ on E′
such that

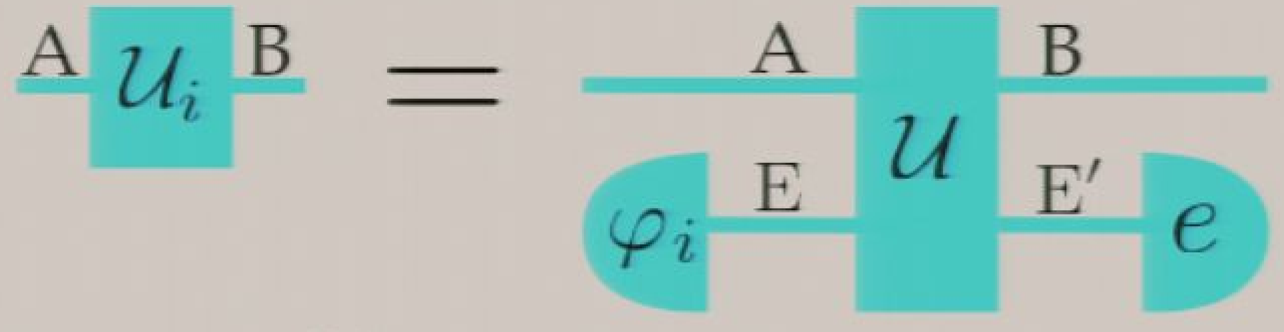


By adding extra-ancillae, $\{a_i\}_{i\in X}$ can be made to be a discriminating test (in QM, an orthogonal measurement)

cf. Ozawa and Naimark theorems in QM

NO PROGRAMMING THEOREM

Problem: Given N reversible gates,
find N program states such that



for some $\mathcal{U}$

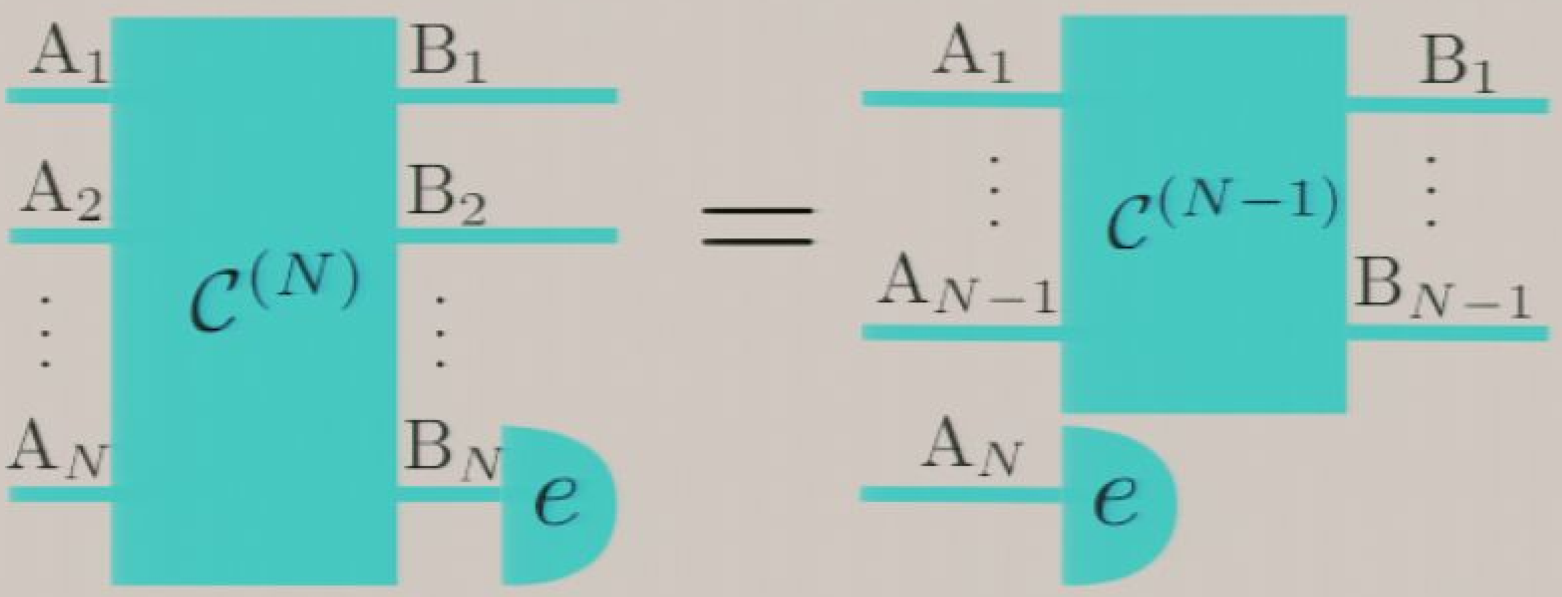
Theorem: to do this you need N perfectly distinguishable states

Corollary: it is impossible to program every reversible gate with a finite-dimensional ancilla

cf. Nielsen-Chuang no-programming for QM

CAUSALLY ORDERED CHANNELS

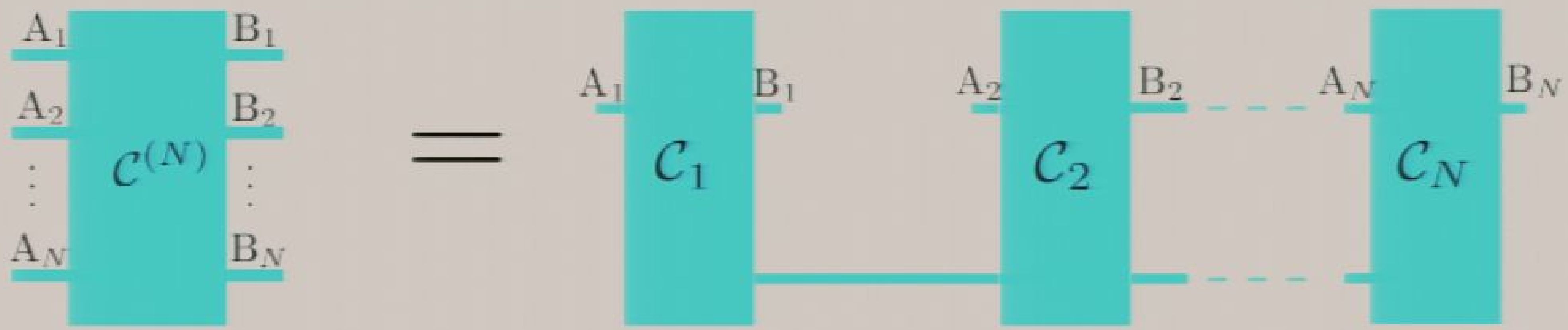
An N-partite channel $\mathcal{C}^{(N)}$ is causally ordered if



for some (N-1)-partite causally ordered channel $\mathcal{C}^{(N-1)}$

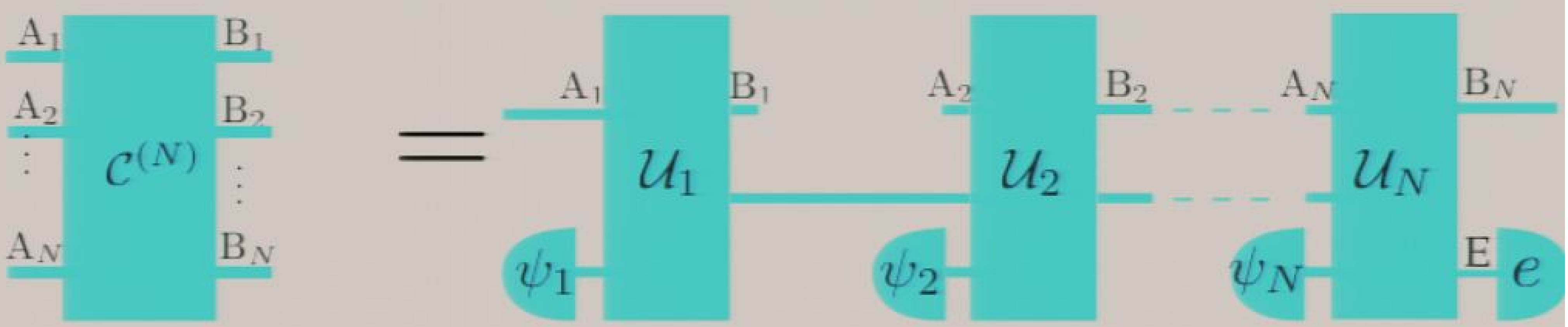
CHANNELS WITH MEMORY

Theorem: any causally ordered channel can be realized as a sequence of channels with memory.



cf. Beckmann, Gottesmann, Nielsen, and Preskill;
Eggeling, Schlingemann, and Werner (N=2);
Kretschmann and Werner (general N);
for QM

DILATION OF CAUSAL CHANNELS



Uniqueness: two dilations of the same channel only differ for a local channel on the last memory system E

→ no perfect bit-commitment:

-single-party strategies = sequences of memory channels

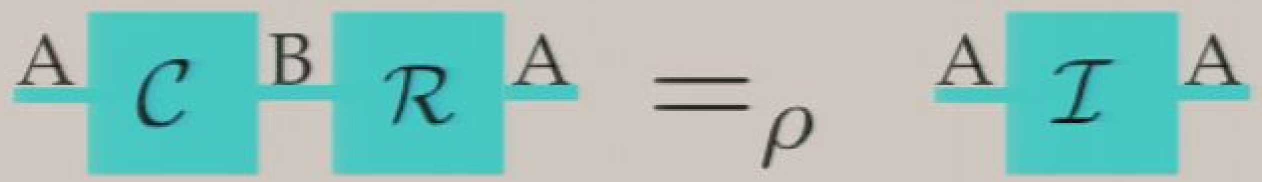
-a protocol is concealing if Alice's strategies for 0 and 1 are indistinguishable by Bob up to the end of the commitment

-Alice can decide at the end to change the value of the bit

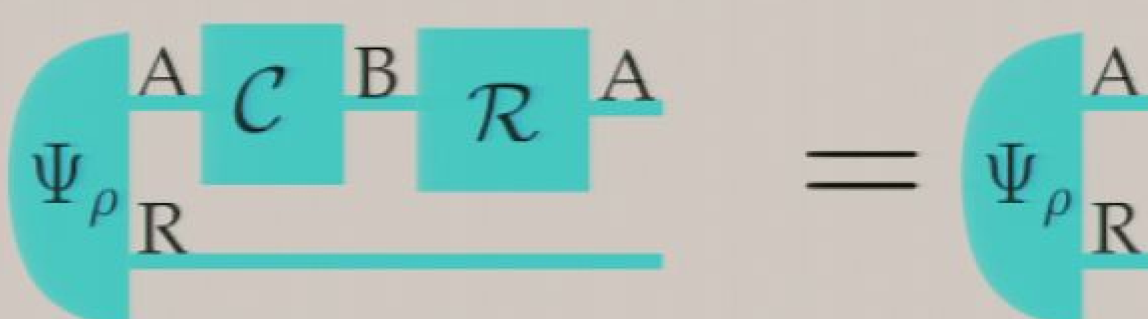
CONDITIONS FOR ERROR CORRECTION

CORRECTABLE CHANNELS

$\mathcal{C}$ correctable upon input ρ if there is a recovery channel

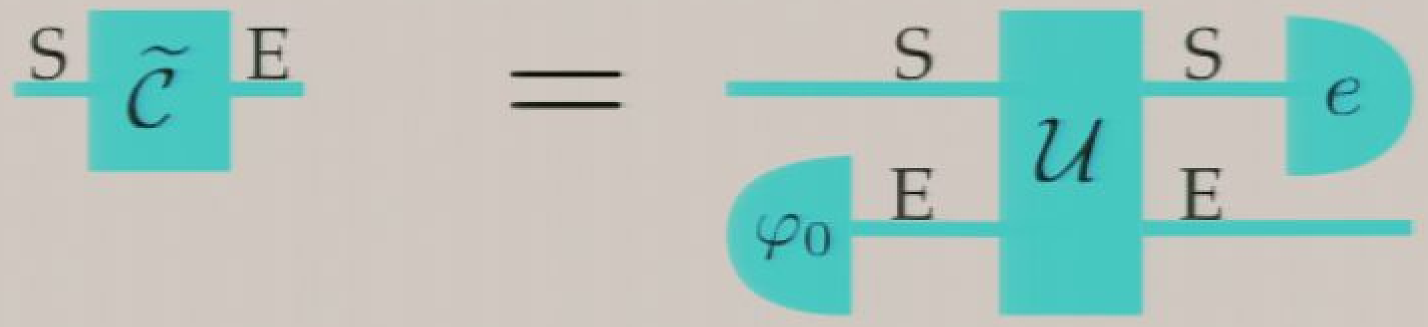


Equivalently,



COMPLEMENTARY CHANNELS

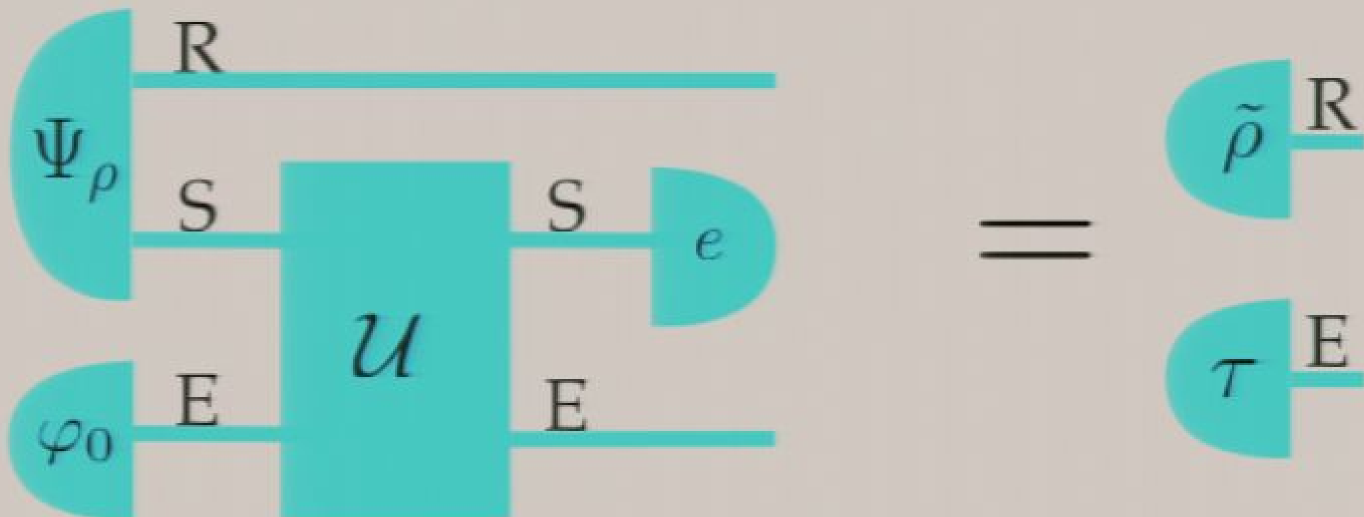
- Complementary channel: take dilation and discard the output system



(it is unique up to reversible channels on E)

CONDITIONS FOR ERROR CORRECTION

Theorem: a channel is correctable iff in any reversible dilation environment and reference factorize:

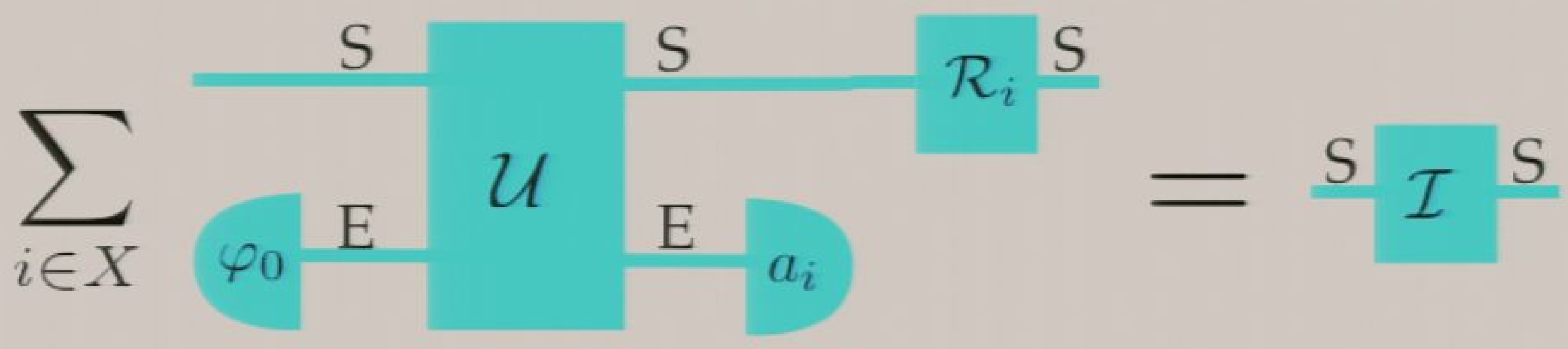


Equivalently: $\mathcal{C}$ correctable upon input of ρ

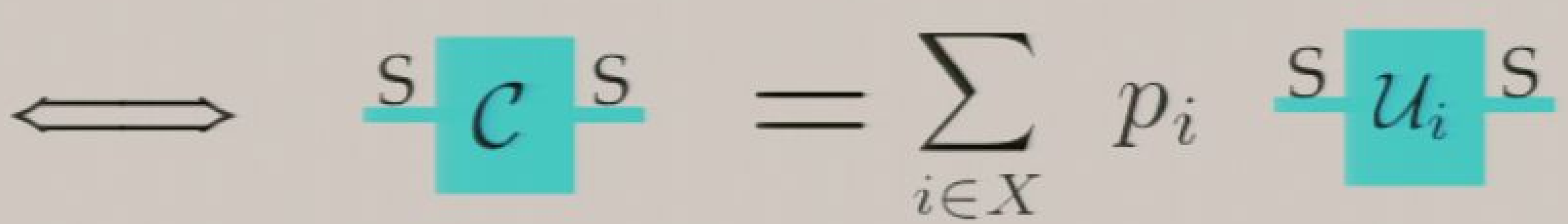
$\Longleftrightarrow$

ERROR CORRECTION WITH FEED-FORWARD

A channel correctable with 1-way classical communication from the environment if



Theorem: $\mathcal{C}$ correctable with 1-way CC from E



cf. Gregoratti and Werner in QM

CONJUGATE PURIFYING SYSTEMS, DETERMINISTIC TELEPORTATION

PURIFICATION WITH CONJUGATE SYSTEMS

Stronger form of the purification axiom:

for every system A, there is a conjugate system $\tilde{\mathrm{A}}$
such that every state of A has a purification in $\mathrm{A}\tilde{\mathrm{A}}$.

Moreover, one has

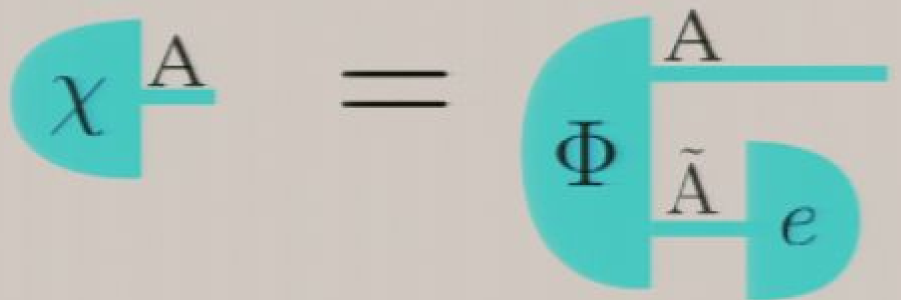
$$\tilde{\tilde{\mathrm{A}}} = \mathrm{A} \qquad \text{(symmetry)}$$

$$\widetilde{\mathrm{AB}} = \tilde{\mathrm{A}}\tilde{\mathrm{B}} \quad \text{(regularity under composition)}$$

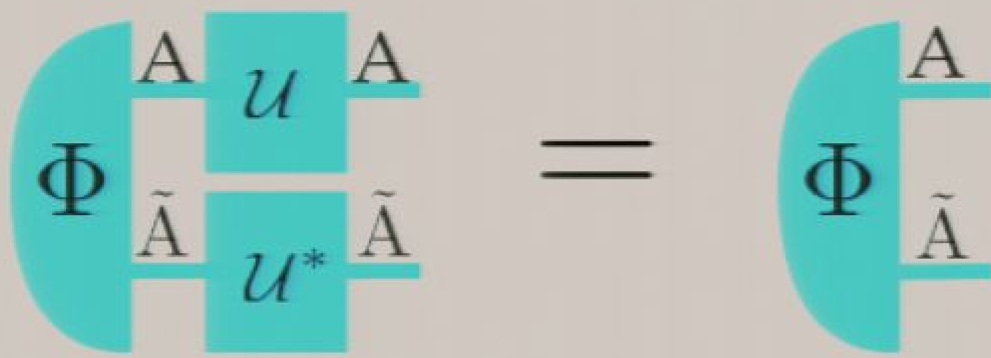
ISOTROPIC STATE

- Take the invariant state χ

Purification of χ :



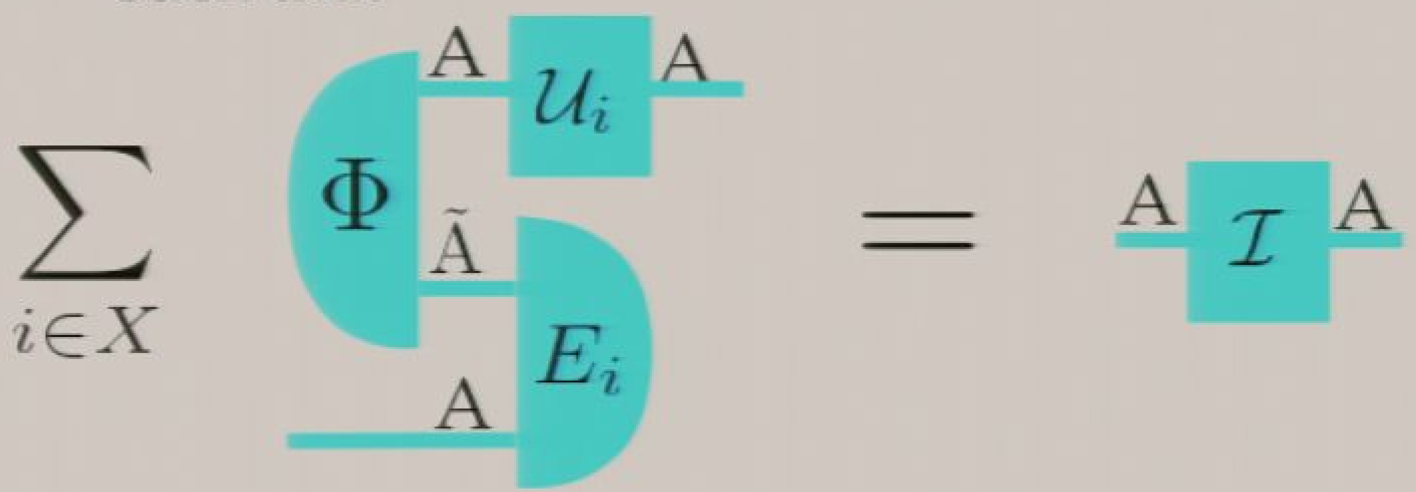
- $\forall\, \mathcal{U} \;\; \exists!\, \mathcal{U}^*$



$\longrightarrow$ one-to-one correspondence between reversible transformations of A and $\tilde{\mathrm{A}}$

DETERMINISTIC TELEPORTATION

Theorem: there exist an observation test $\{E_i\}_{i\in X}$
and a finite set of reversible channels $\{\mathcal{U}_i\}_{i\in X}$
such that



• Φ can be converted by LOCC in any bipartite state of $A\tilde{A}$

Moreover, Φ is the unique state (up to local reversible channels) allowing for deterministic teleportation

CONCLUSIONS AND FUTURE WORK

Purification is the key for deriving most of the diagrammatic features of QM:

- entanglement, no cloning, no info without disturbance
- teleportation, Choi-Jamiolkowski isomorphism,
- dilation theorems, causal channels, no bit commitment
- no programming
- conditions for error correction

However, an information-theoretic analysis is still missing: entropies and rates for compression, communication, entanglement concentration, and similar tasks.

Next step: treatment of info-theoretic tasks in theories with purification