A COMPLETE SET OF INFORMATIONAL PRINCIPLES FOR QUANTUM THEORY

Giulio Chiribella
Perimeter Institute for Theoretical Physics

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

Colloquium, March 7 2011, Institute for Quantum Computing

OUTLINE

- Motivation and statement of the result
- The framework: circuits with probabilities
- Five basic axioms on information-processing
- The purification principle

MOTIVATION

SUCCESSFUL, YES, BUT MYSTERIOUS, TOO

Quantum theory is a very successful theory.
It is the core of atomic, molecular and particle physics, explains the structure of matter, chemistry, computer technology.

“Successful, yes, but mysterious, too. Balancing the glory of quantum achievements, we have the shame of not knowing "how come." Why does the quantum exist?”

J. A. Wheeler (The New York Times, Dec 12 2000)

MATHEMATICAL VS PHYSICAL PRINCIPLES

Since von Neumann's 1932 classic,
the standard textbook presentations of QM are
descriptions of its mathematical framework:

cf. "Each physical system is associated with a Hilbert space H. Unit rays in H describe the pure states of the system."

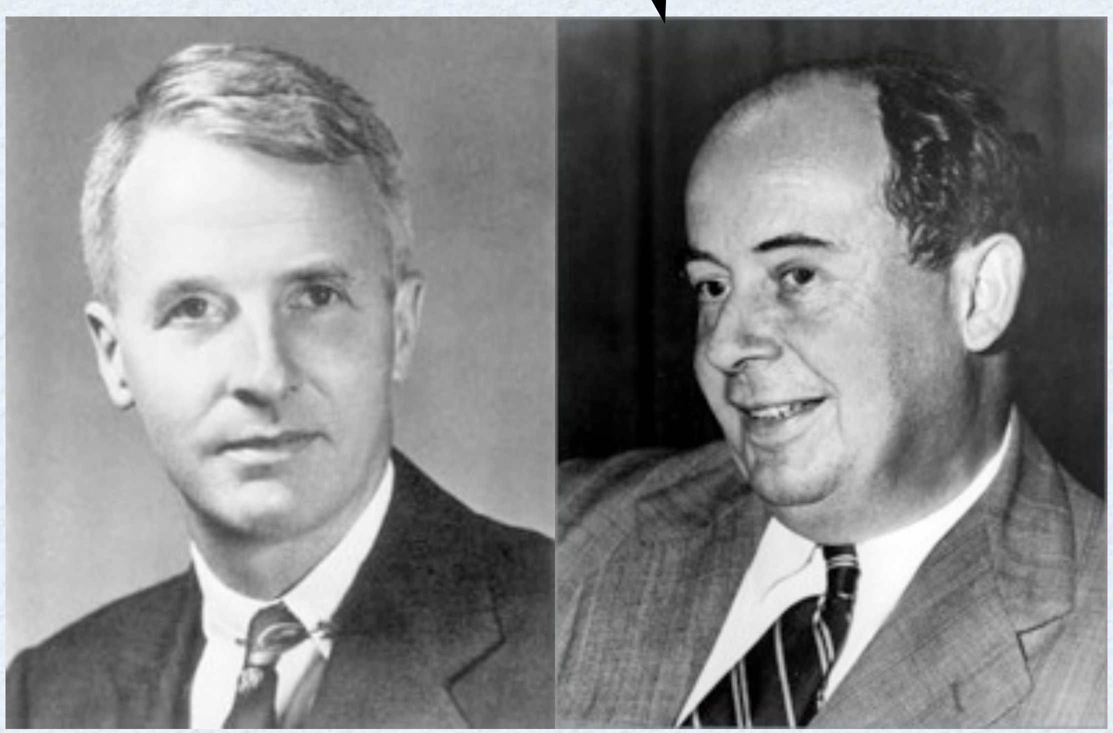
or: "Physical quantities are represented by self-adjoint operators on H".

Is it possible to describe QM through physical principles?

FORM LOGICS TO INFORMATION-PROCESSING

Birkhoff and von Neumann (1936)

QM should be understood as a new form of logics.



Wheeler (1990)

It from bit. All things physical are information-theoretic in origin

INFORMATIONAL AXIOMS FOR QM

Quantum information $\longrightarrow$ huge number of operational consequences of QT

Idea: promote some operational consequences to axioms and derive the math of QT from them

Previous works in this direction:

- Hardy, Brukner and Dakic, Masanes and Mueller
- Abramsky and Coecke, Coecke
- Barnum, Barrett, Leifer, Short, Wilce
- Fuchs and Schack
- D'Ariano
- Pawlowski, Paterek, Kaszlikowski, Scarani, Winter, Zukowski

THIS WORK

Main result:

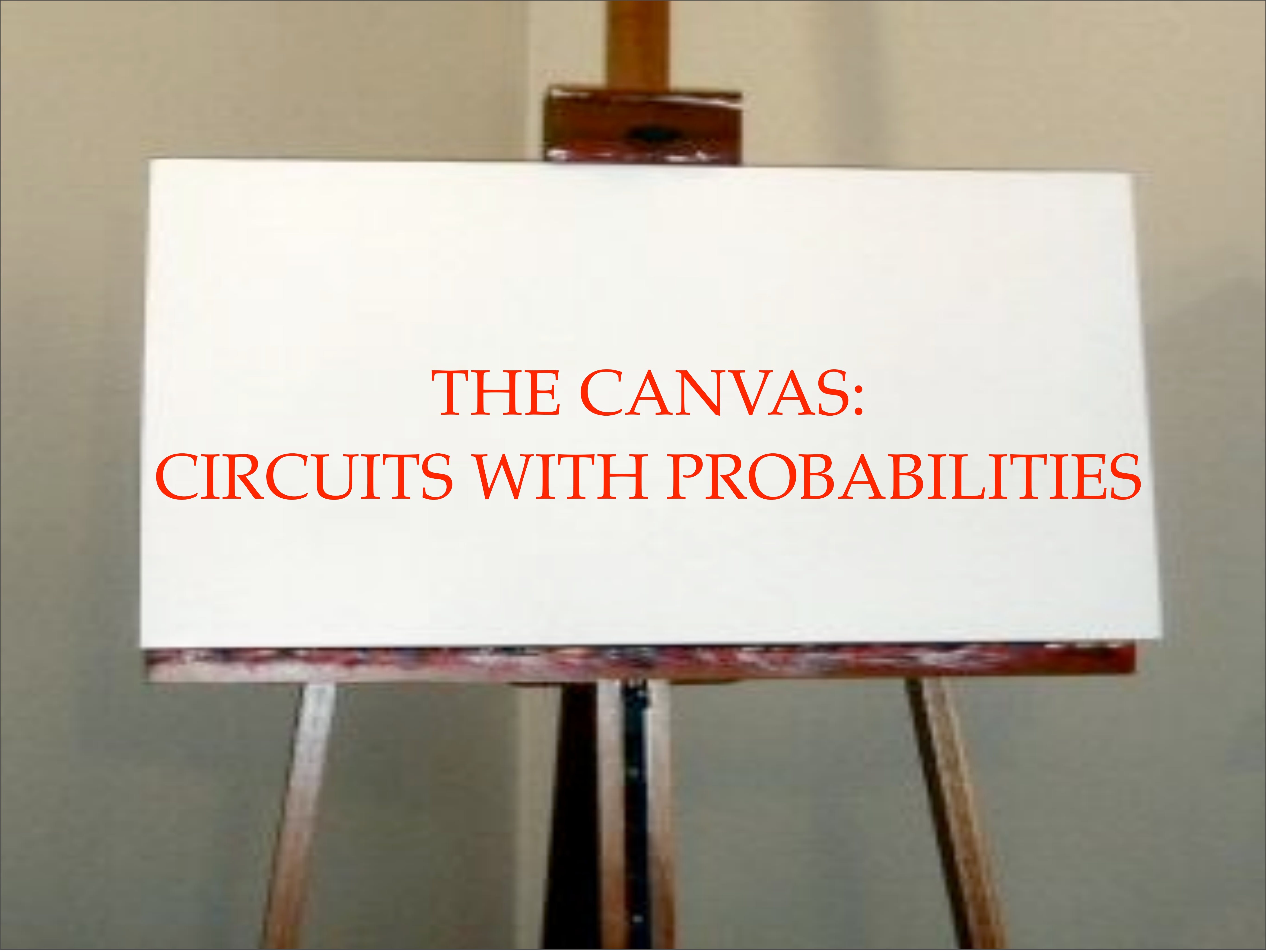
- QT can be completely characterized as a theory of information processing

- Among a standard set of theories of information processing, QT is uniquely identified by the purification principle

By-products:

- simpler proofs of existing quantum results

- less hypotheses needed
(less than the full QT, typically)

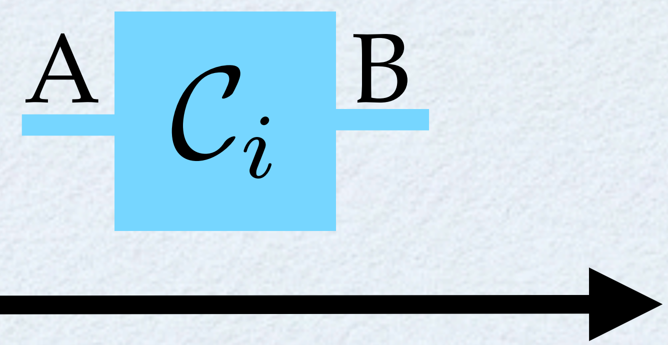

THE CANVAS:
CIRCUITS WITH PROBABILITIES

CIRCUITS

SYSTEMS AND TESTS

-Systems: A, B, C, ...

-Tests: a test represents one use of a physical device



input-output arrow

A : input system

B : output system

i: outcome, in some outcome set X

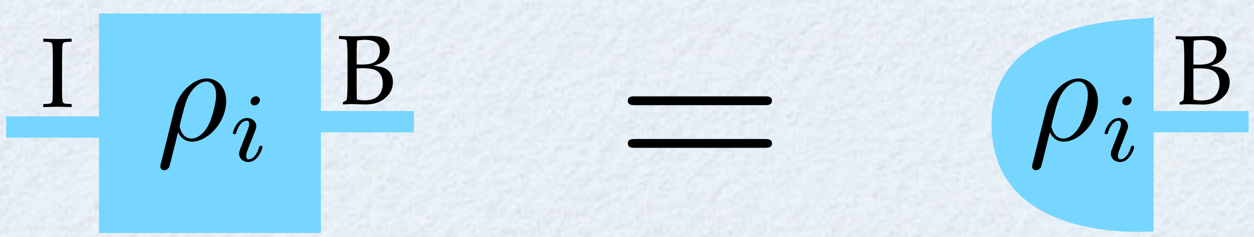
$\mathcal{C}_i$: event

PREPARATIONS AND MEASUREMENTS

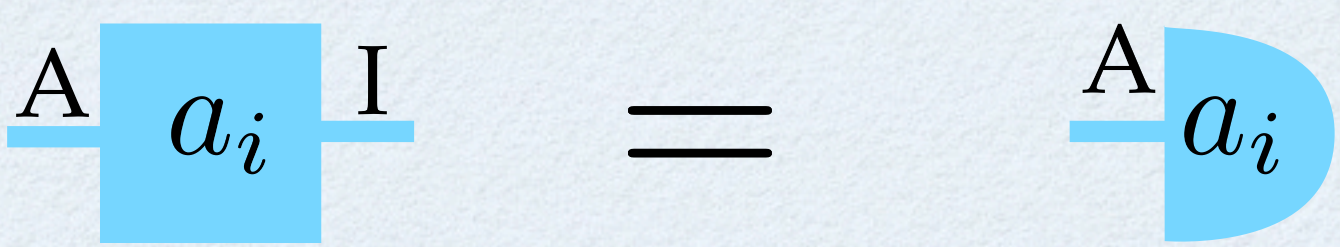
Trivial system (nothing), denoted by I

Special cases of tests:

- trivial input: preparation, ρ_i : state

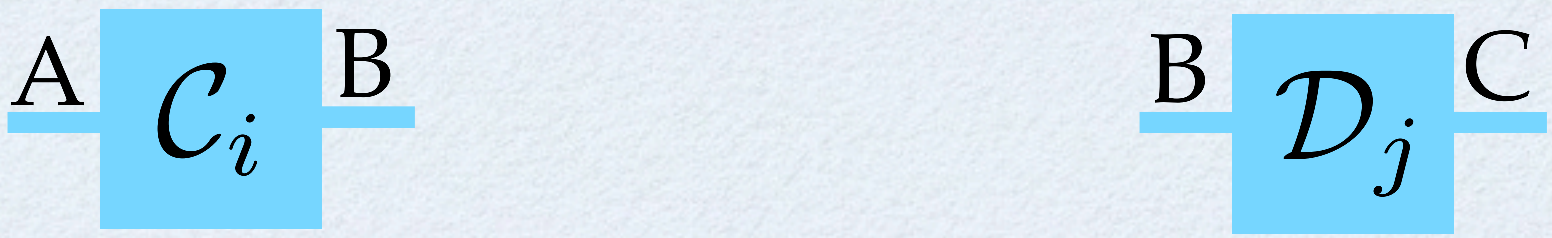


- trivial output: measurement a_i : effect

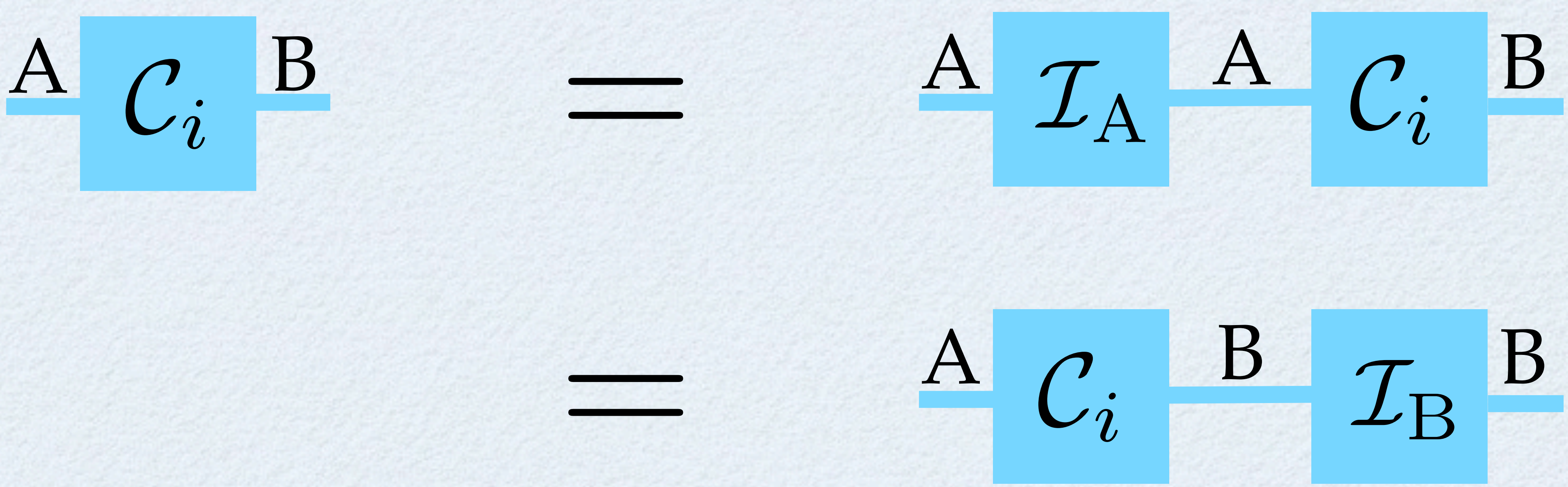


COMPOSITION IN SERIES

-Cascades of tests:



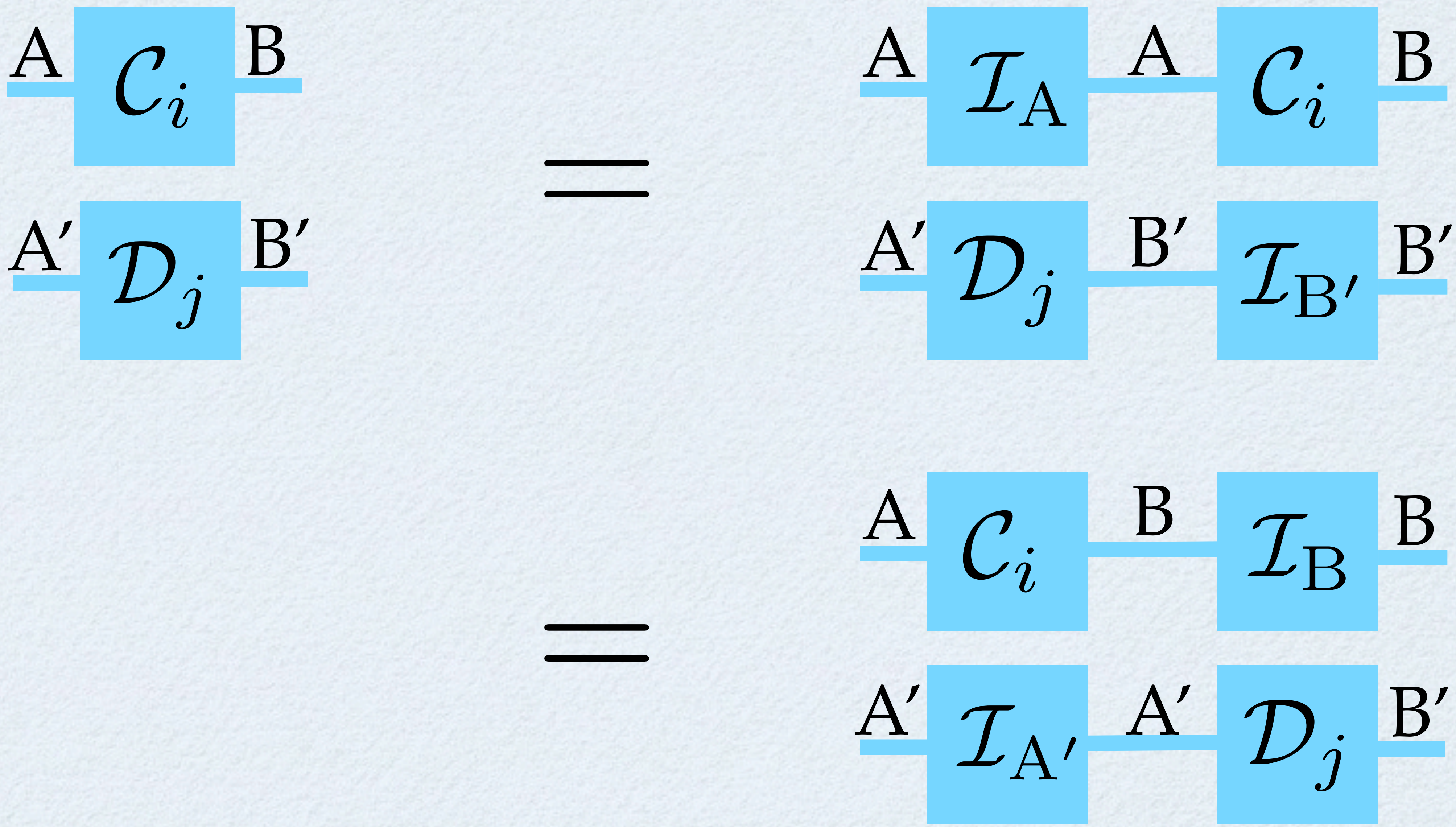
-Identity tests:



COMPOSITION IN PARALLEL

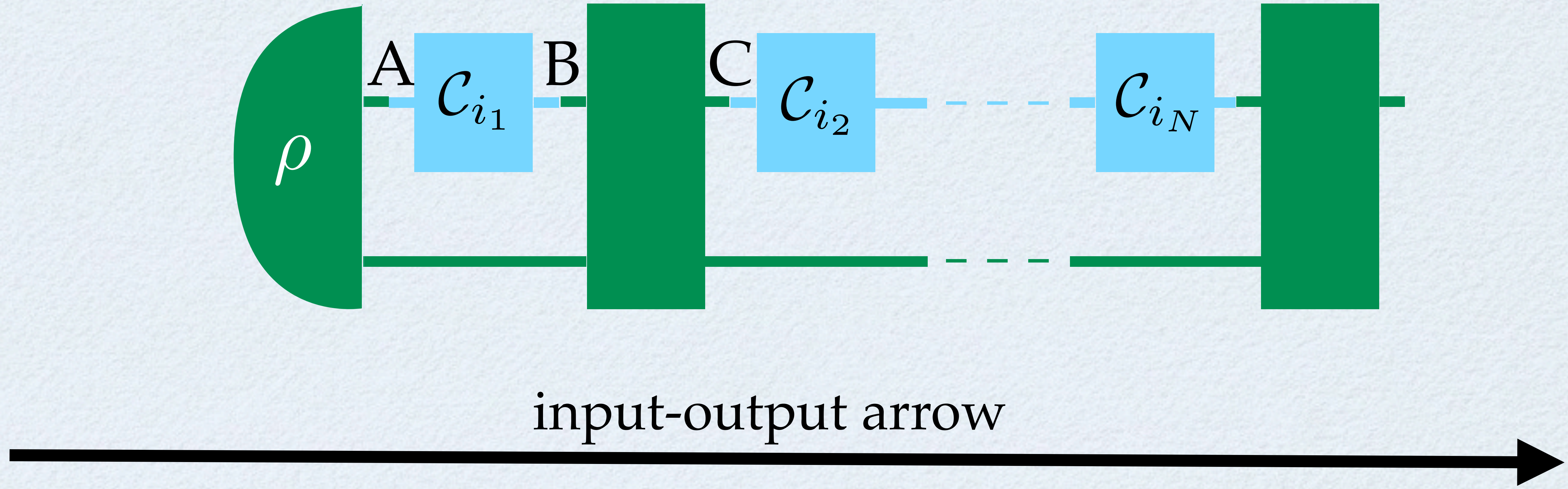
-Composite systems: AB, ABC (trivial composition: A=AI=IA)

-Composite tests:



CIRCUITS

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

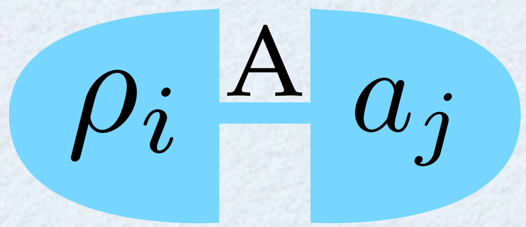


An operational theory is a language, and its words are well-formed circuits.

PROBABILITIES

PROBABILISTIC STRUCTURE (I)

- Preparation + measurement = probability distribution



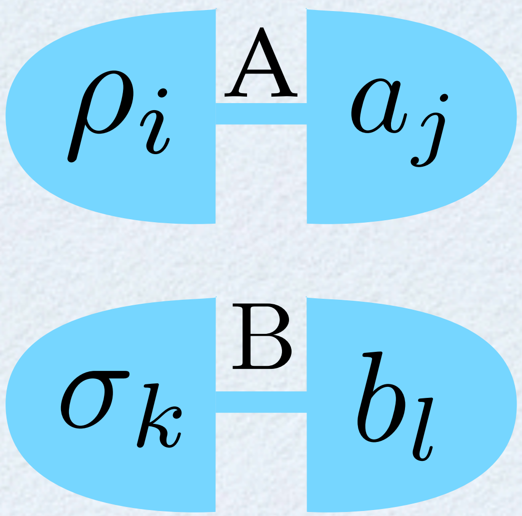
$$= p(a_j, \rho_i)$$

$$\begin{cases} p(a_j, \rho_i) \geq 0 \\ \\ \displaystyle\sum_{i \in X} \sum_{j \in Y} p(a_j, \rho_i) = 1 \end{cases}$$

Consequence: states and effects form vector spaces (here state spaces are assumed to be finite dimensional and closed)

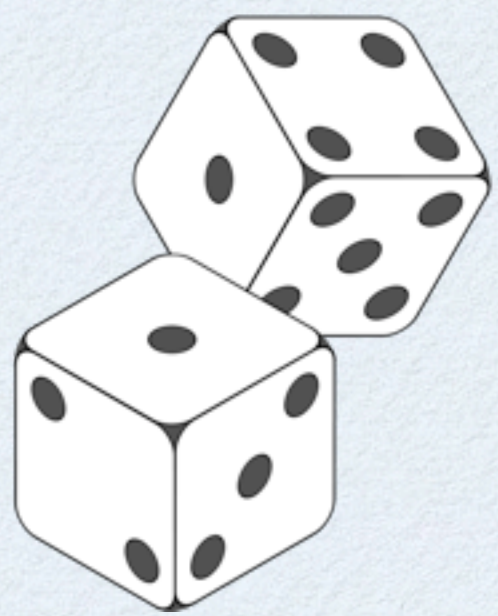
PROBABILISTIC STRUCTURE (II)

Experiments performed in parallel are statistically independent:



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

e.g. the roll of two dice



BASIC NOTIONS IN THE OPERATIONAL-PROBABILISTIC FRAMEWORK

COARSE-GRAINING

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

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

Atomic transformations: $\mathcal{C}$ is atomic if it cannot be obtained from a (non-trivial) coarse-graining

$$\mathcal{C} = \sum_{i \in X} \mathcal{C}_i \implies \mathcal{C}_i \propto \mathcal{C} \;\forall i \in X$$

e.g. in roll of a dice, ask if the outcome is even or odd:

$$p'_{even} = p_2 + p_4 + p_6$$

the event "even" is the coarse graining of the atomic events 2,4,6

PURE VS MIXED STATES (I)

Mixed states: a state is mixed if it is a coarse-graining of some random preparation

$$\rho = \sum_{i \in X} \rho_i$$

Pure states: a state is pure if it is atomic

$$\rho = \sum_{i \in X} \rho_i \implies \rho_i \propto \rho \quad \forall i \in X$$

PURE VS MIXED STATES (II)

Pure states: maximal knowledge about the preparation

in classical information: pure state = point in phase space
mixed state = probability distribution

in quantum information: pure state = unit vector in Hilbert space
mixed state = density matrix

ATOMIC MEASUREMENTS

Atomic effect: not a coarse-graining

$$a = \sum_i a_i \quad \Longrightarrow a_i \propto a \quad \forall i$$

Atomic measurement: measurement consisting of atomic effects

Atomic measurement are “maximally informative”, in the sense that they provide maximal resolution.

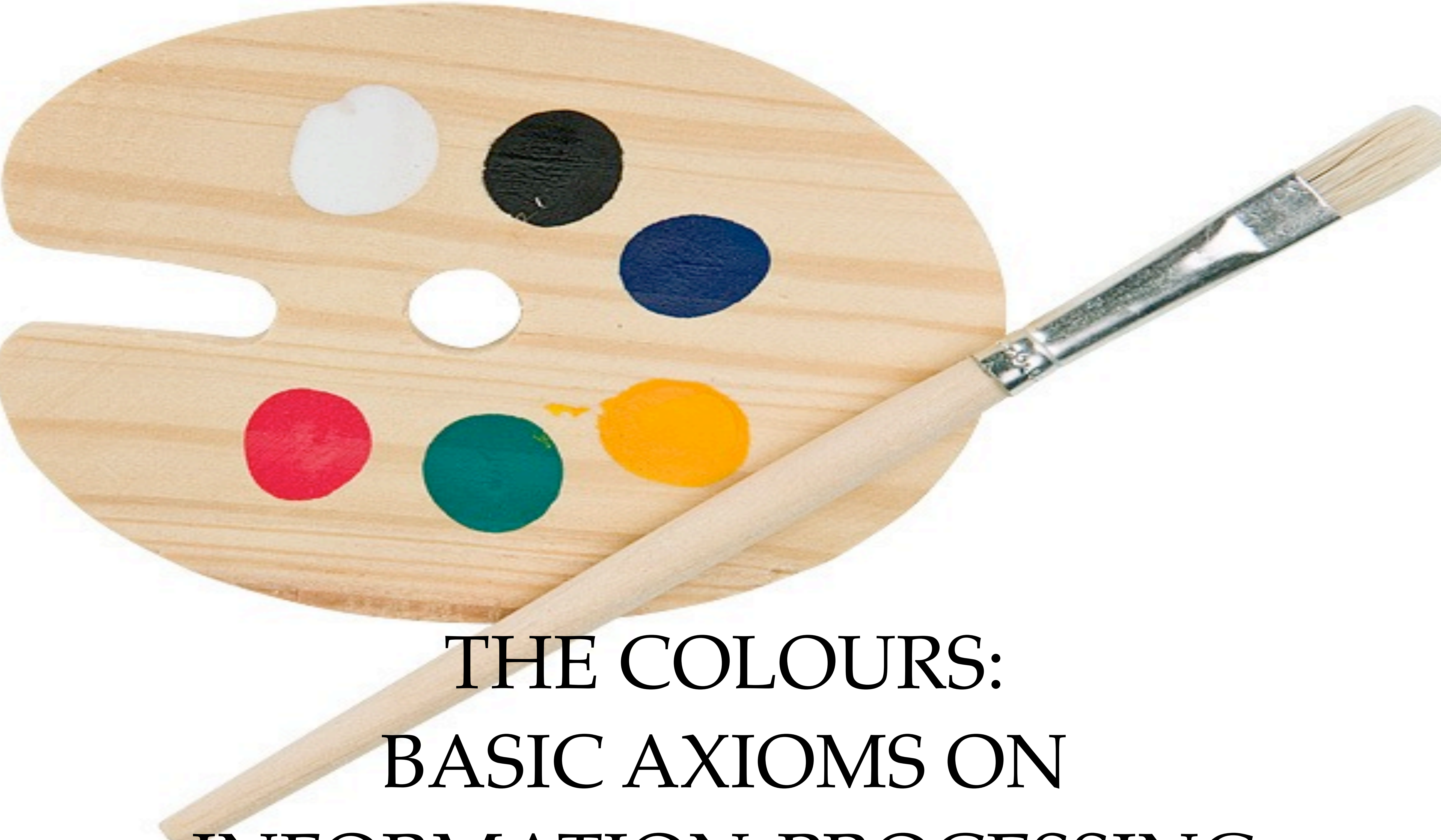
e.g. in QT: rank-one POVMs are atomic
non rank-one POVM non-atomic

WHAT IS AN "OPERATIONAL" AXIOM?

An axiom is operational if it can be expressed using only

- the basic notions: system, state, effect, transformation
- their specifications: atomic, pure, mixed, completely mixed
- composite notions obtained from the above
  (e.g. "reversible transformation")

In the following: complete set of operational axioms for QT!
(five basic axioms + purification)



THE COLOURS: BASIC AXIOMS ON INFORMATION-PROCESSING

STANDARD MODEL OF INFORMATION PROCESSING

Five properties are common to both classical and quantum information:

- Causality
- Perfect distinguishability
- Local distinguishability
- Ideal compression
- Pure conditioning

→ axioms for a standard model of information processing

CAUSALITY

CAUSALITY AXIOM

A1 The probability of outcomes for a test at a certain time is independent of the choice of tests performed at later times.

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

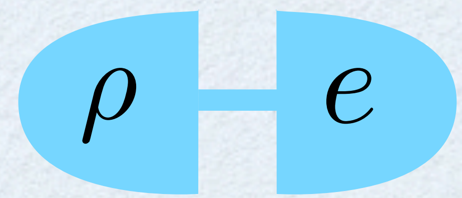
In other words, the choice of a test can only affect the outcome probabilities of tests that happen "later".

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

EQUIVALENT CONDITION

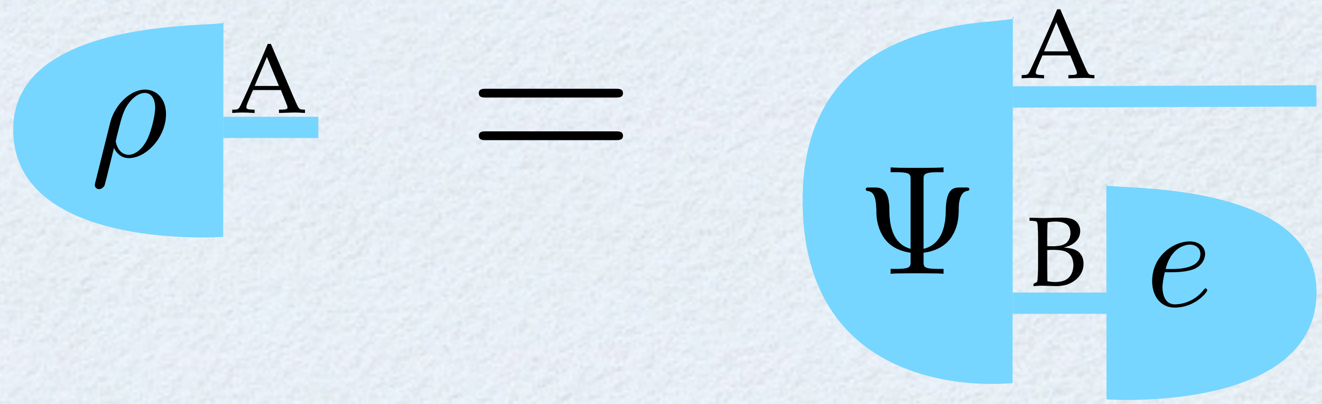
Equivalent condition: there is a unique deterministic effect e

$$\sum_{i \in \mathrm{X}} a_i = e$$

e.g. in quantum mechanics: 

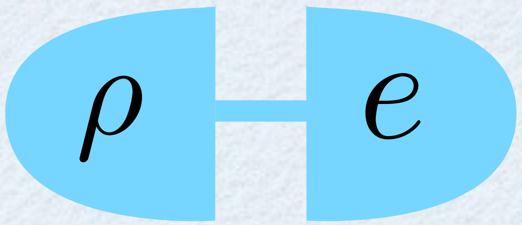
$= \mathrm{Tr}[\rho]$

Consequence:
marginal states are uniquely defined



Causality implies the impossibility of superluminal signalling

NORMALIZED STATES

A state ρ is normalized if 

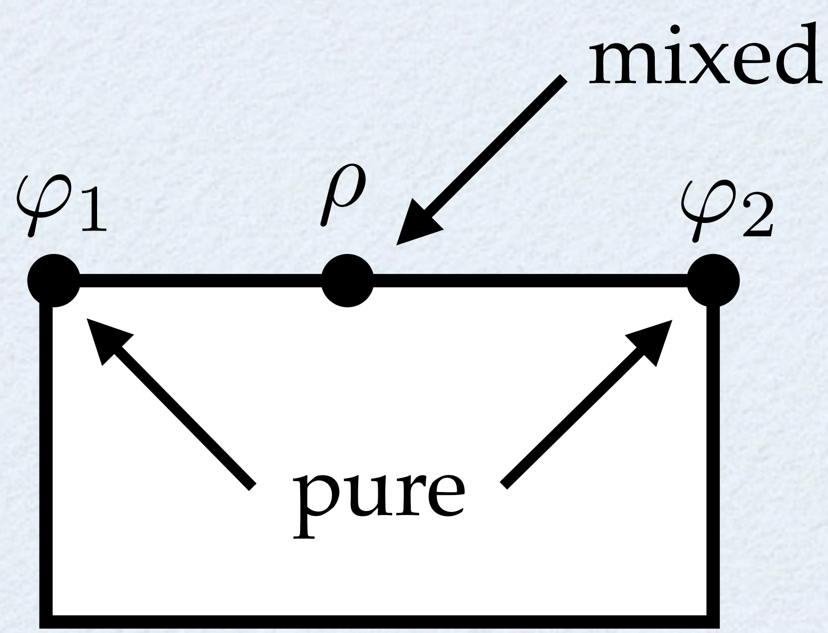
$= 1$

Normalized states form a convex set:

$$\rho, \sigma \text{ normalized} \Rightarrow p\rho + (1-p)\sigma \text{ normalized } \forall p, 0 \le p \le 1$$

Pure states $=$ extreme points of the convex set

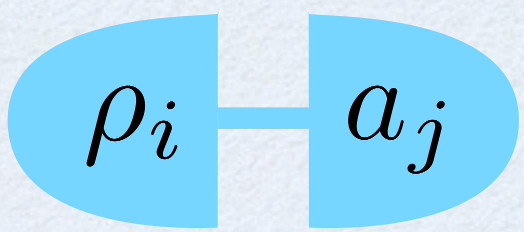
Example:



PERFECT DISTINGUISHABILITY

PERFECTLY DISTINGUISHABLE STATES

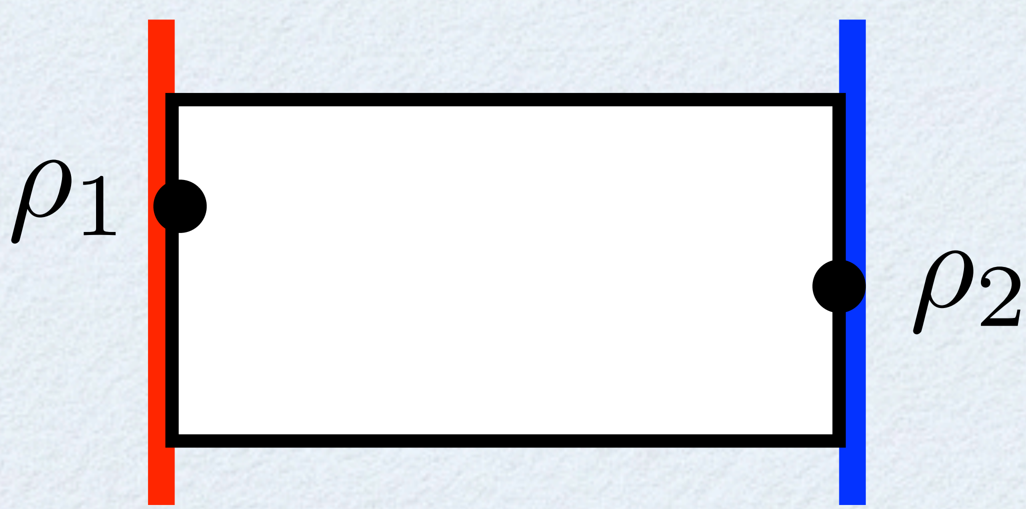
The (normalized) states $\rho_1, \ldots, \rho_N$
are perfectly distinguishable if there is a measurement $\{a_i\}_{i=1}^N$
such that



$= \delta_{ij}$

Example 1: in QM, two orthogonal states

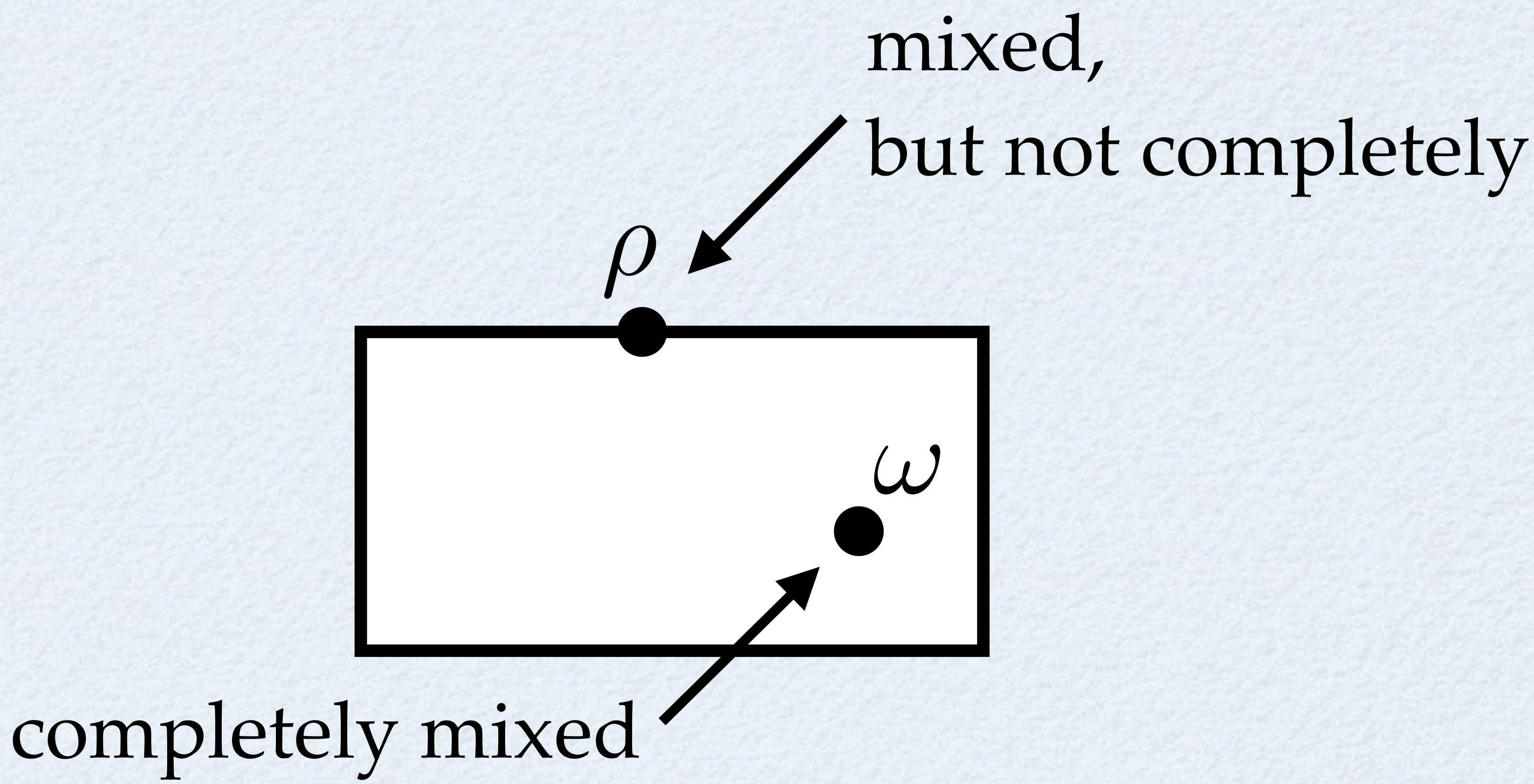
Example 2:



COMPLETELY MIXED STATES

A state is completely mixed if any state can stay in its convex decomposition,
Equivalently, if the state is in the interior of the convex set.

Example:

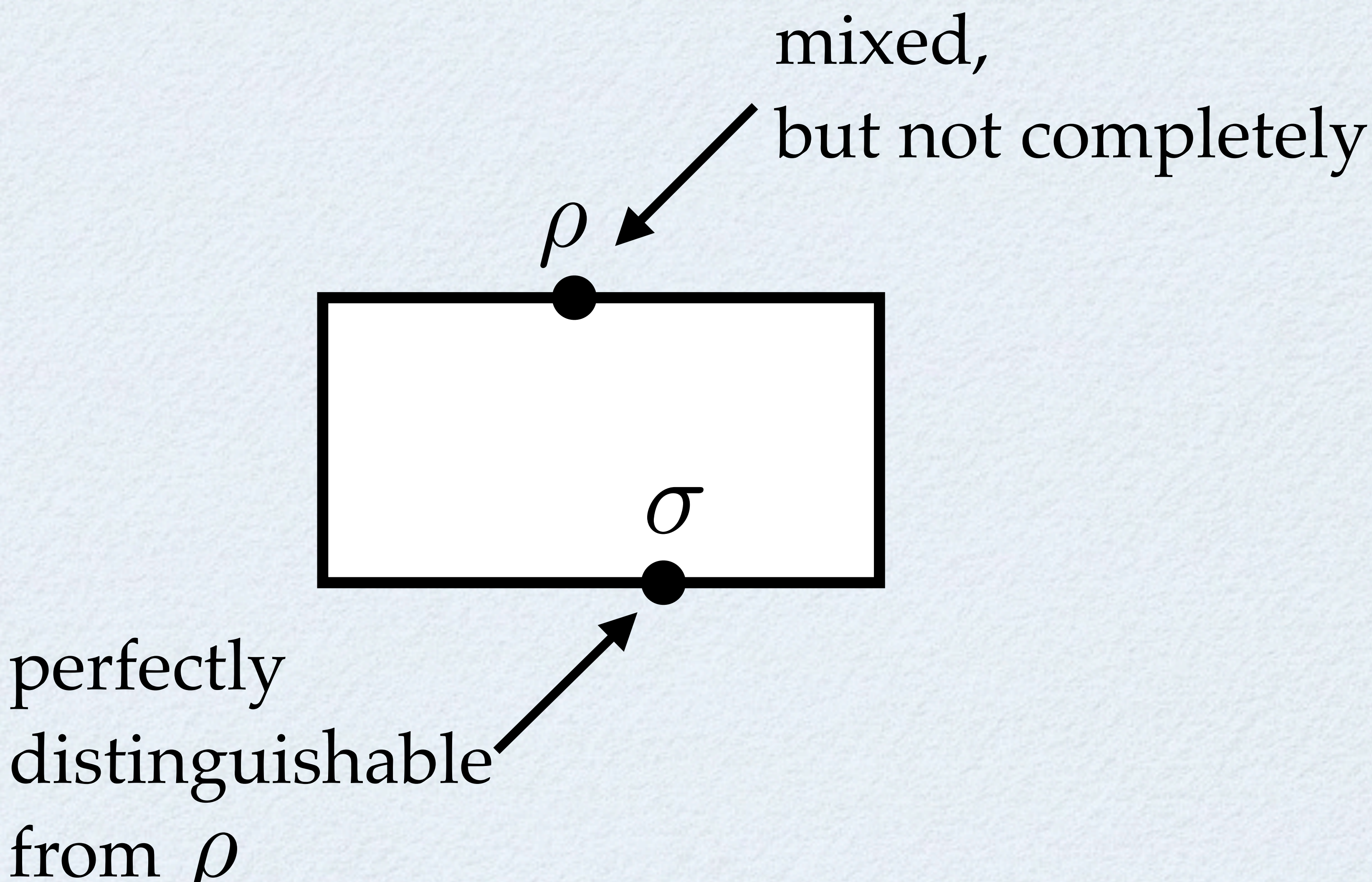


Property: no state can be perfectly distinguished from a completely mixed state

PERFECT DISTINGUISHABILITY AXIOM

A2 If a state is not completely mixed,
then it is perfectly distinguishable from some other state.

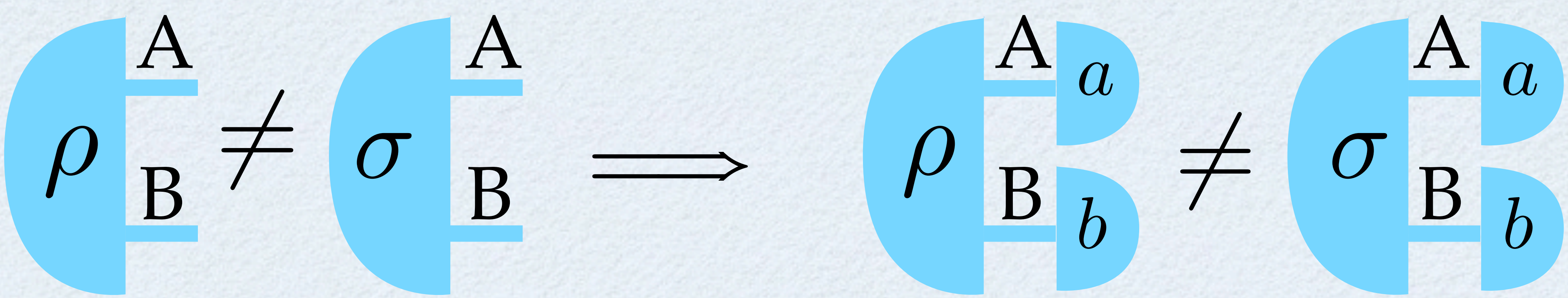
Example:



LOCAL DISTINGUISHABILITY

LOCAL DISTINGUISHABILITY AXIOM

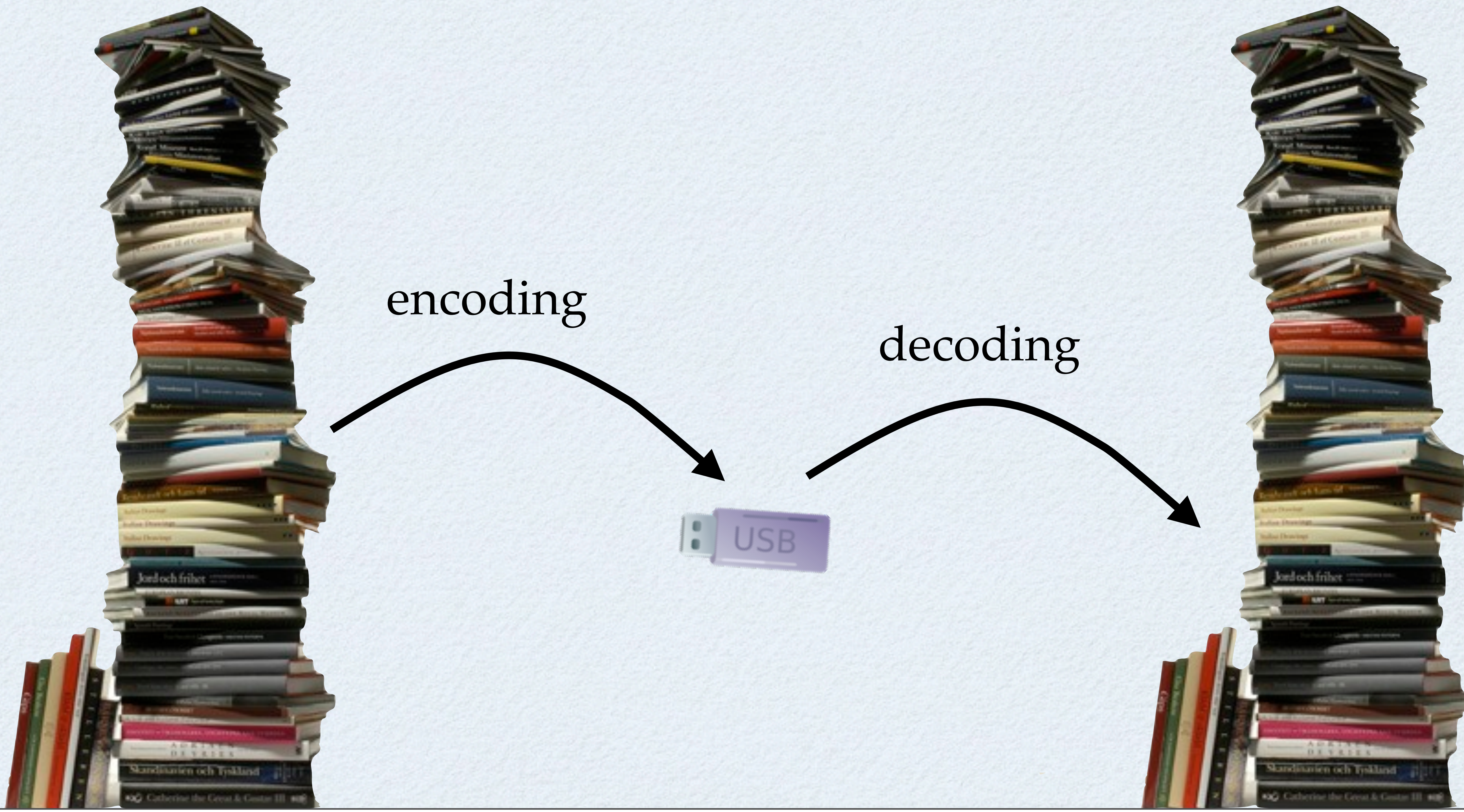
A3 If two states are distinguishable,
they are distinguishable from the statistics of local experiments.



Equivalently: a state is fully characterized from the statistics of local experiments (local tomography)

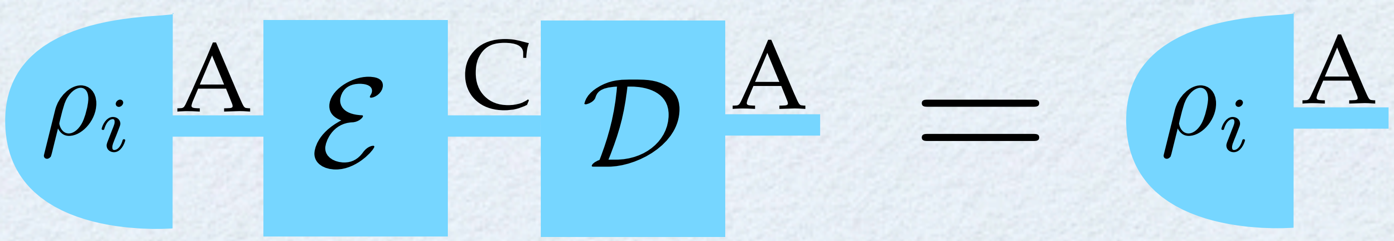
IDEAL COMPRESSION

INTUITIVE IDEA



LOSSLESS ENCODING

Let $\{p_i\, \rho_i\}_{i \in X}$ be an information source for system A.
A transformation $\mathcal{E}$ from A to C is a lossless encoding if there is a decoding transformation $\mathcal{D}$ from C to A such that



$\forall i \in X$

$\mathcal{E}$ is a lossless encoding for ρ if it is lossless for every information source such that

$$\sum_{i \in X} p_i\, \rho_i = \rho$$

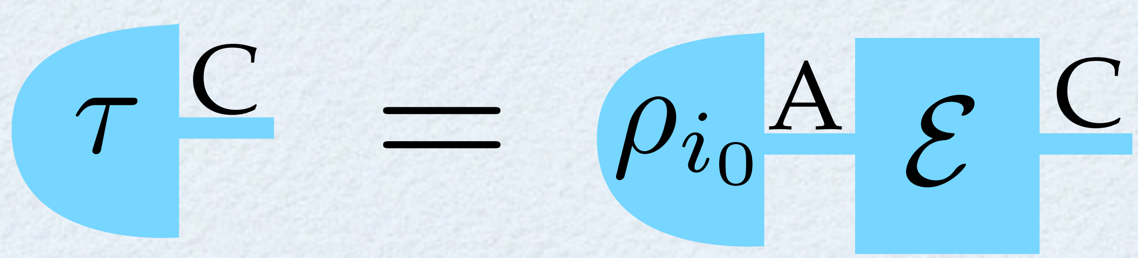
MAXIMALLY EFFICIENT ENCODING

The encoding $\mathcal{E}$ is maximally efficient for ρ if every state in C represents some state in the convex decomposition of ρ ,

that is, if for every state τ in C there is an information source such that $\{p_i \ \rho_i\}_{i\in X}$

$$\sum_{i\in X} \rho_i = \rho$$

and an outcome $i_0 \in X$ such that

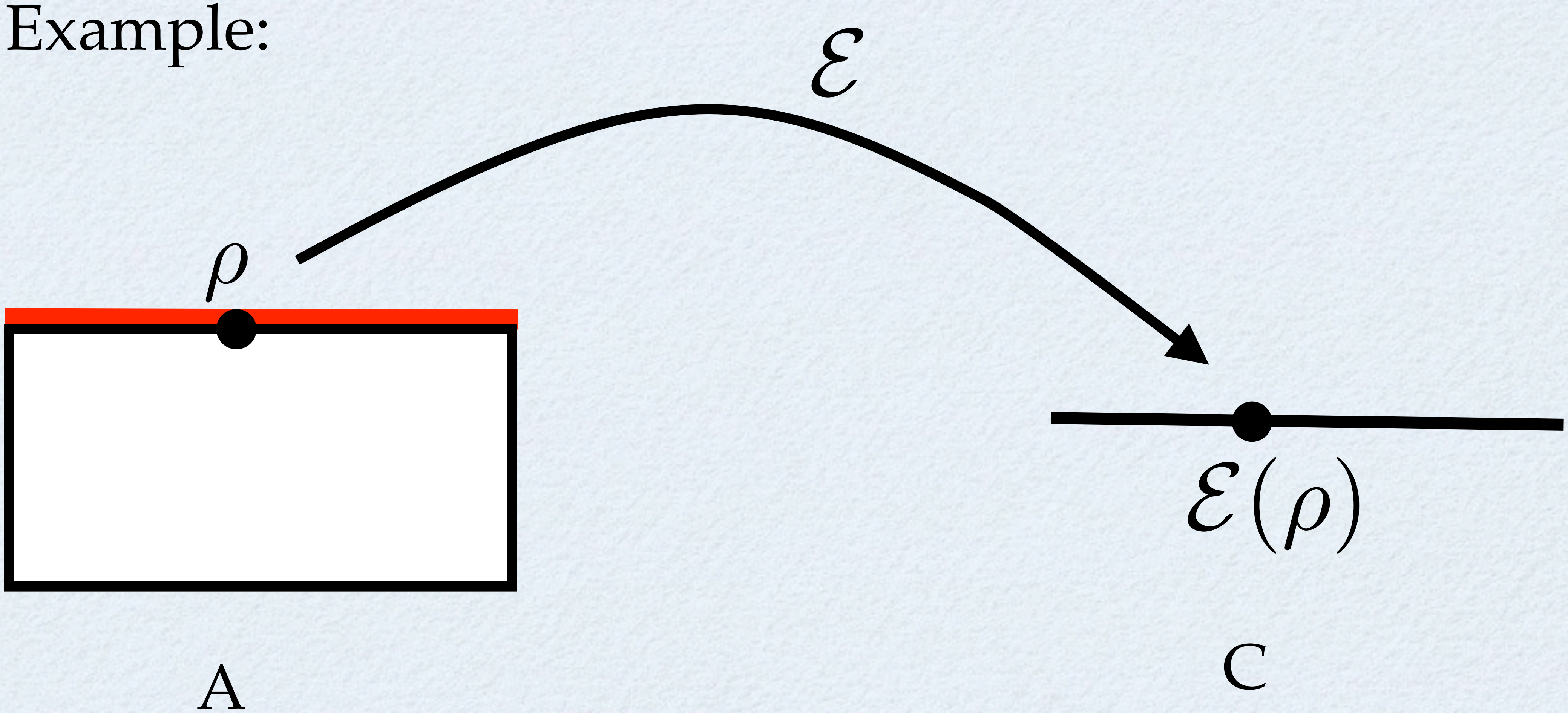


IDEAL COMPRESSION AXIOM

An encoding that is lossless and maximally efficient is an ideal compression.

A4 For every state there is an ideal compression.

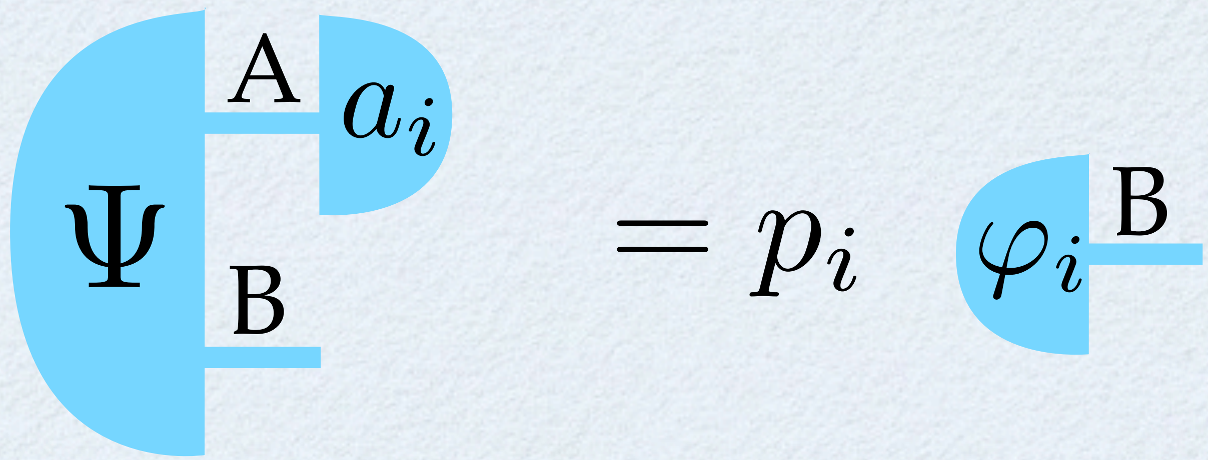
Example:



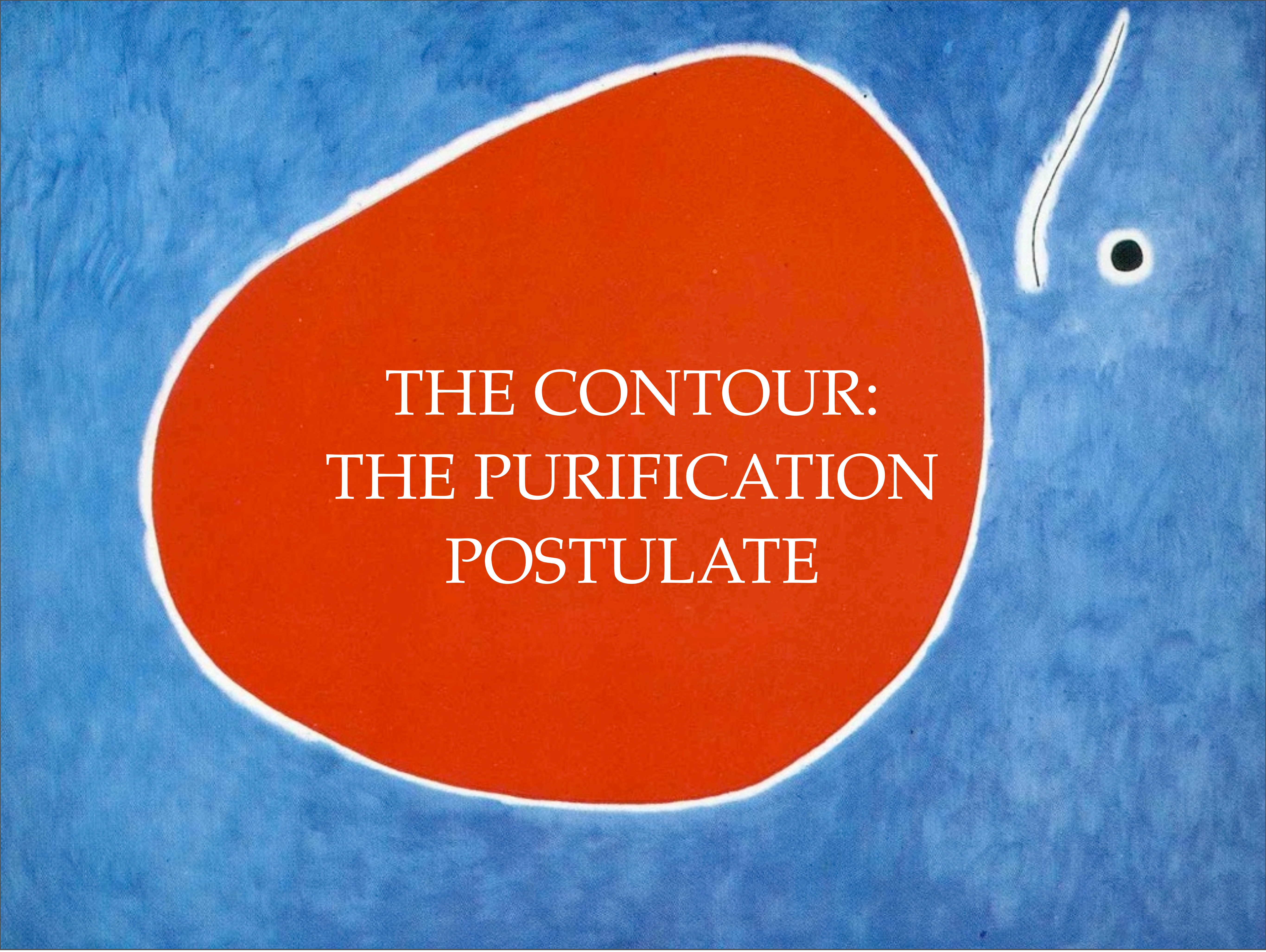
PURE CONDITIONING

PURE CONDITIONING AXIOM

A5 Each outcome of an atomic measurements on one side of a bipartite pure state induces a pure state on the other side.

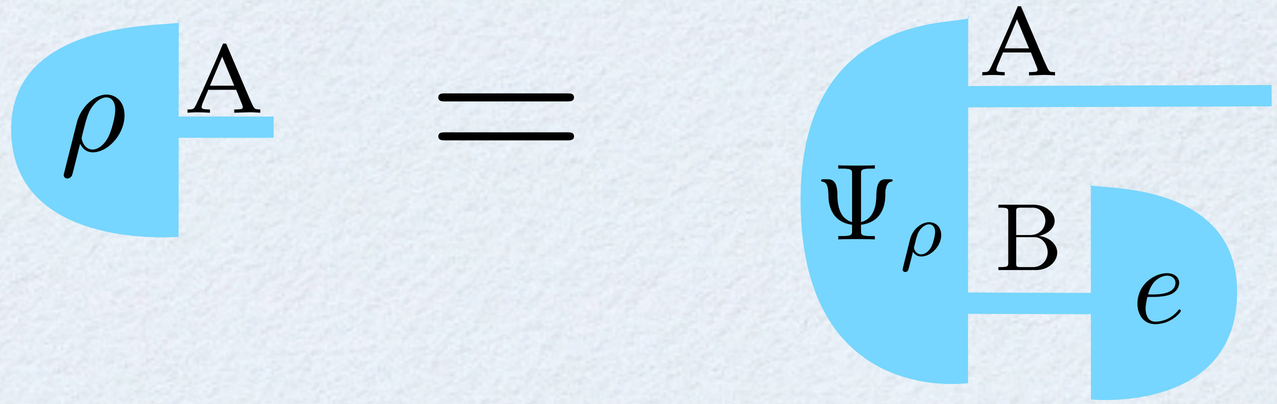


$$\Psi \text{ pure } + \ a_i \text{ atomic} \Longrightarrow \varphi_i \text{ pure}$$

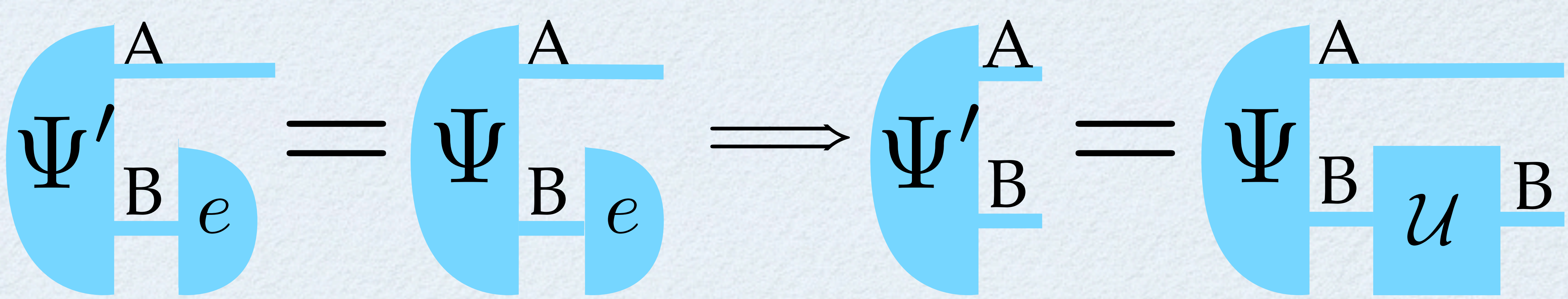

THE CONTOUR:
THE PURIFICATION
POSTULATE

THE PURIFICATION POSTULATE

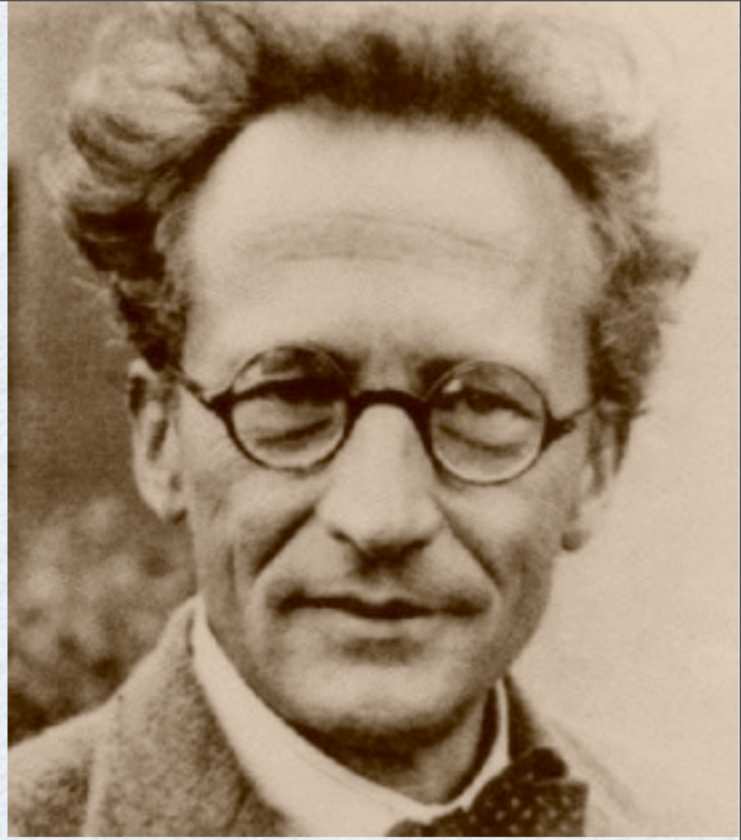
- **Existence:** For every state ρ of A
  there is a system B and a pure state Ψ_ρ of AB
  such that



- **Uniqueness** up to reversible transformations on the purifying system:



ON THE EXISTENCE OF PURIFICATION



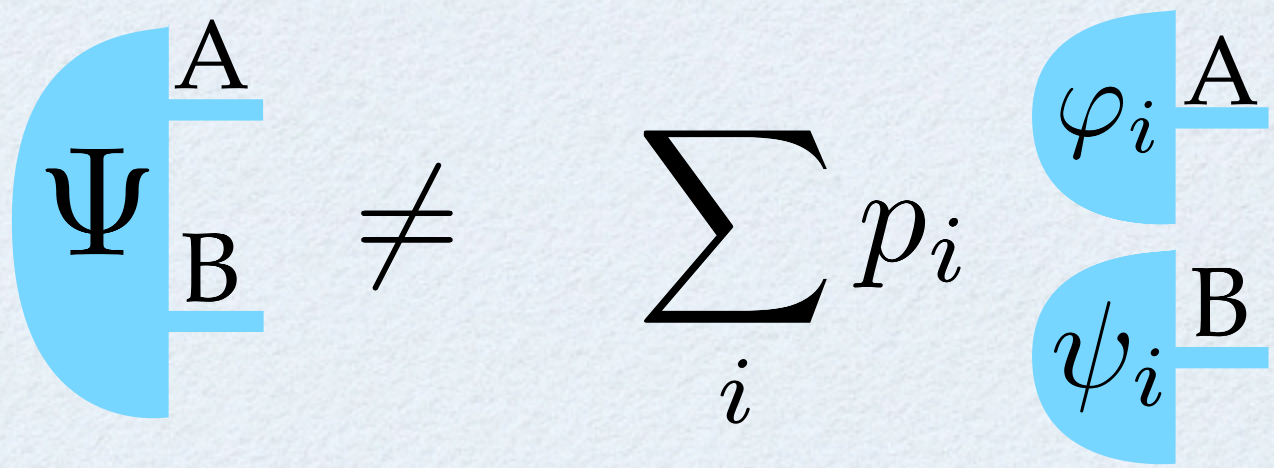
"the best possible knowledge of a *whole* does not necessarily include the best possible knowledge of all its *parts*, even though they may be entirely separate and therefore virtually capable of being 'best possibly known'."

"I would not call that *one* but rather *the* characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought."

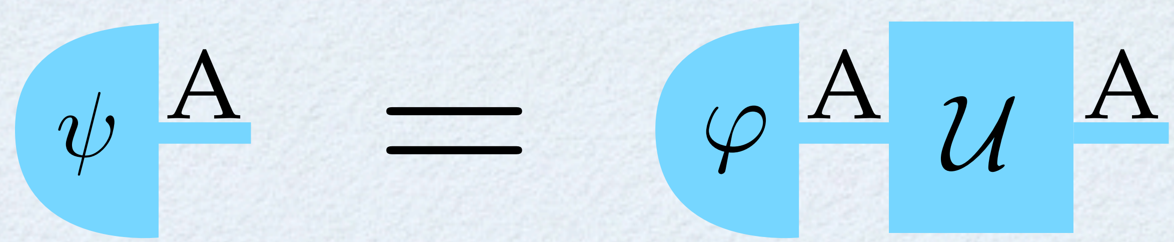
Schrödinger, E. (1935) "Discussion of Probability Relations Between Separated Systems," *Proceedings of the Cambridge Philosophical Society* **31**, 555 (1935)

A FEW CONSEQUENCES OF PURIFICATION

- There are entangled states (no classical probability theory)



- Every couple of pure states is connected by a reversible transformation (no PR boxes)



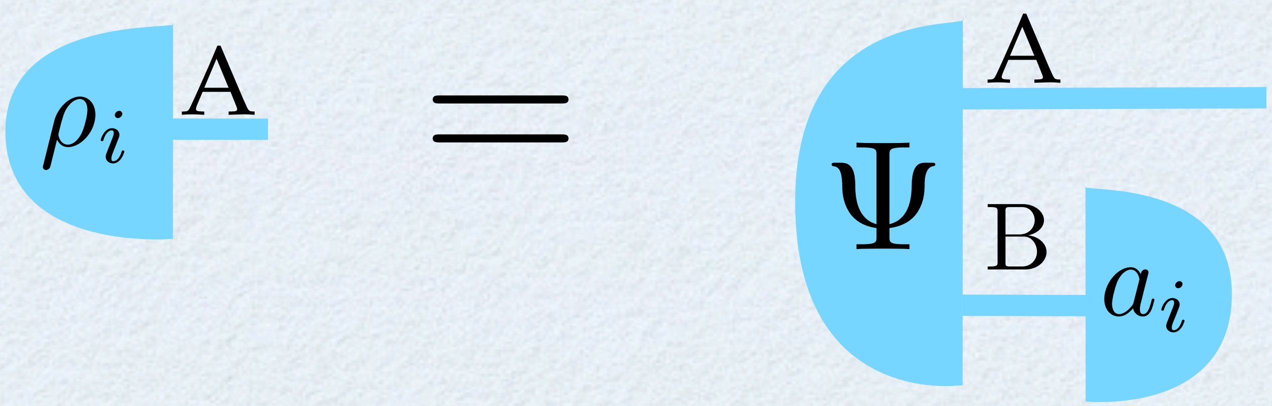
PURIFICATION OF INFORMATION SOURCES

Purification of states $\longrightarrow$ purification of information sources

$\longrightarrow$ Schroedinger's "steering"

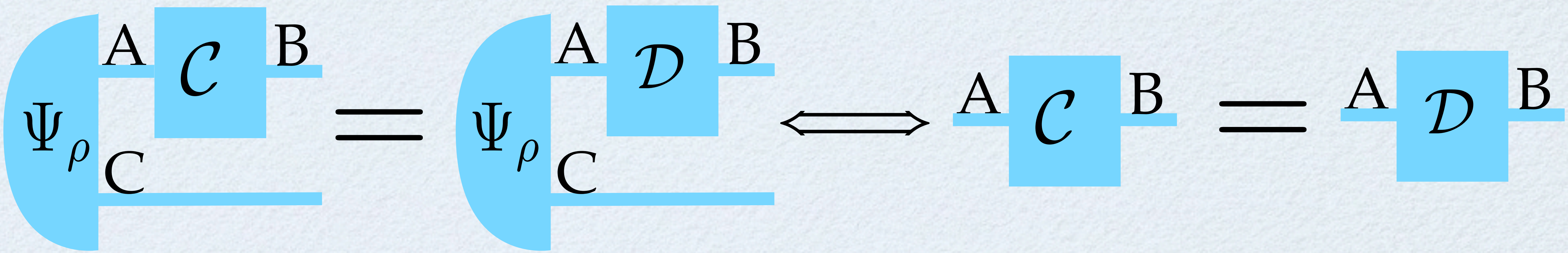
Theorem:

For every information source $\{\rho_i\}_{i\in X}$ of A
there is a system B,
a pure state Ψ of AB
and a measurement $\{a_i\}_{i\in X}$ of B
such that



PROCESS TOMOGRAPHY

ρ completely mixed $\Longrightarrow$ Ψ_ρ allows for process tomography

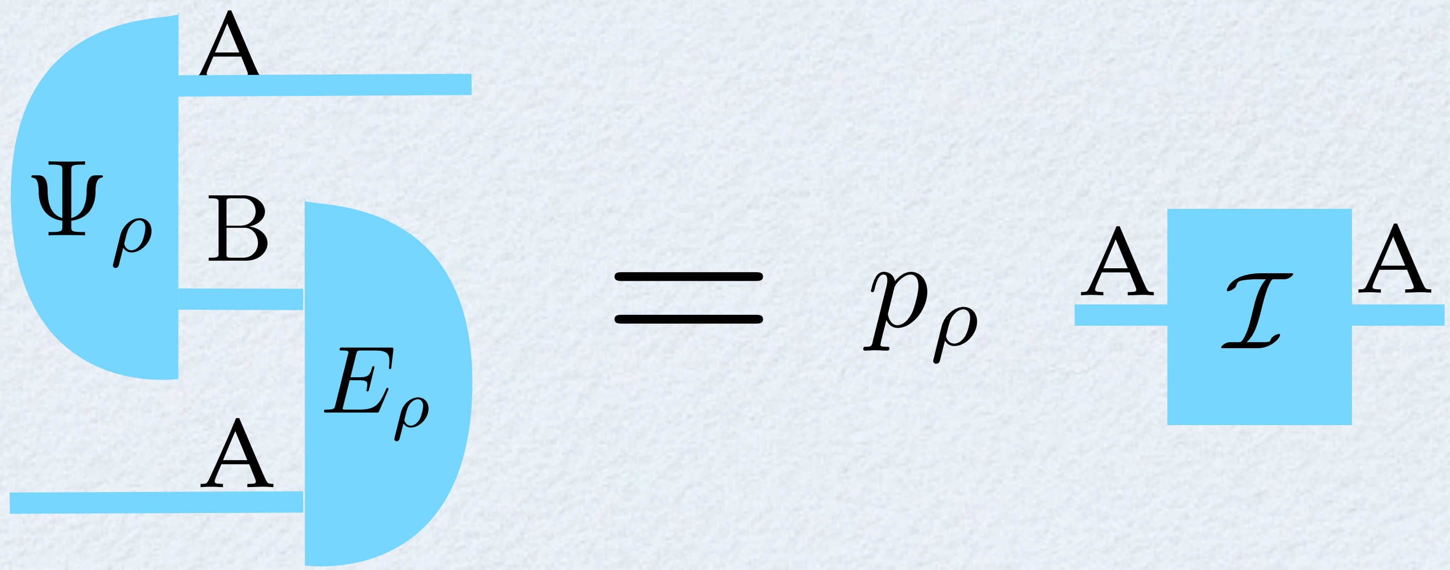


Ψ_ρ is pure $\Longrightarrow$

- no information without disturbance
- no cloning of pure states

PROBABILISTIC TELEPORTATION

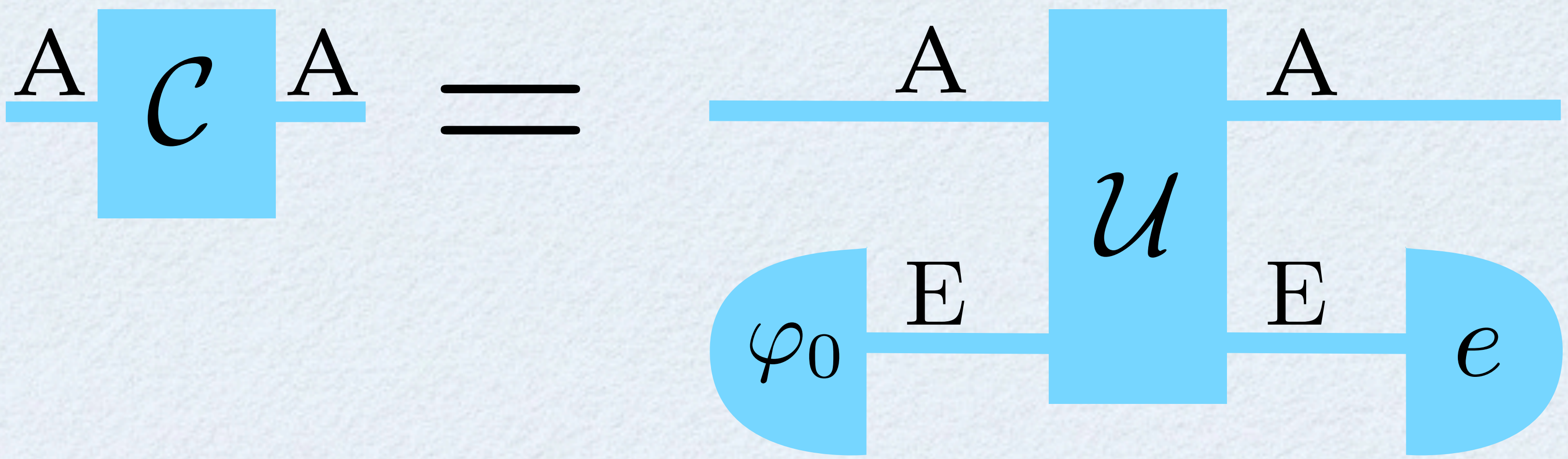
Theorem: for every completely mixed state ρ on A
there is an effect E_ρ on AB such that



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

IRREVERSIBILITY FROM REVERSIBILITY

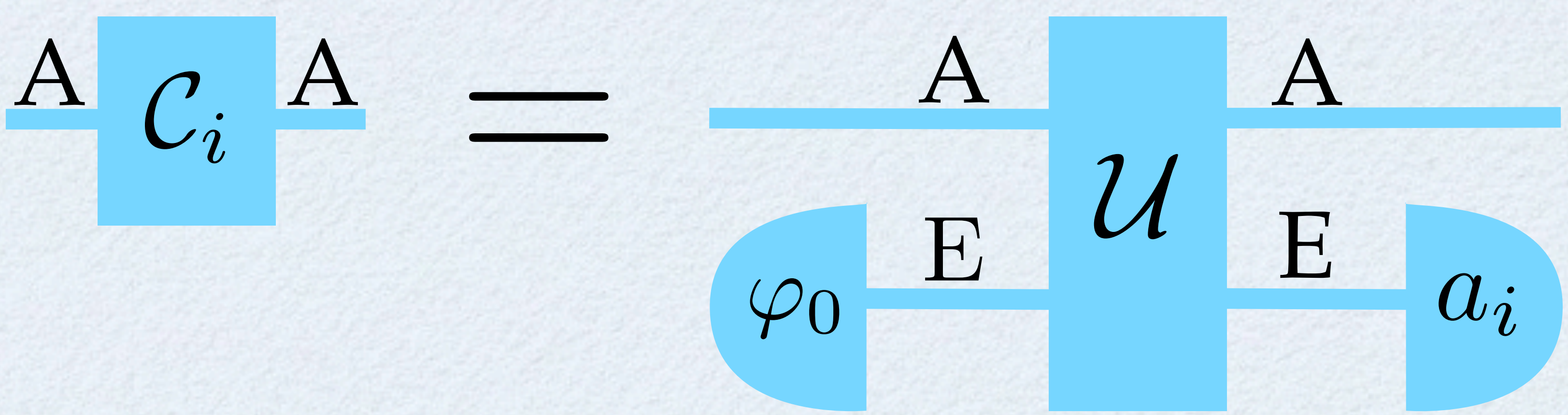
Theorem: For every channel $\mathcal{C}$ on system A
there exists an environment E,
a pure state φ_0 of E ,
and a reversible interaction $\mathcal{U}$ such that



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

SHIFTING VON NEUMANN'S CUT

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



→ Every measurement can be modelled as a reversible interaction with an apparatus, followed by a reading of the pointer.

CONCLUSIONS

CONCLUSIONS

- Quantum mechanics can be completely characterized as a theory of information processing.

- Within a standard class of theories of information-processing, QT is uniquely identified by the purification postulate.

- Directions for future work:

  -Extension to infinite dimensional systems
  (cf. continuous variable systems, field theory)

  -Extension of the results beyond causality and local
  distinguishability.

RELATED READINGS

J. A. Wheeler, ‘A Practical Tool,´ but Puzzling Too,
http://www.nytimes.com/2000/12/12/science/12ESSA.html

G Chiribella, GM D’Ariano, and P. Perinotti,
Informational derivation of quantum theory,
arXiv:1011.6451

G Chiribella, GM D’Ariano, and P. Perinotti,
Probabilistic theories with purification,
Phys. Rev. A 81, 062348 (2010), arXiv:0908.1583