Title: Information Processing in Convex Operational Theories: Toward a characterization of quantum mechanics

Date: Oct 15, 2008 04:00 PM

URL: http://pirsa.org/08100037

Abstract: The rise of quantum information science has been paralleled by the development of a vigorous research program aimed at obtaining an informational characterization or reconstruction of the quantum formalism, in a broad framework for stochastic theories that encompasses quantum and classical theory, but also a wide variety of other theories that can serve as foils to them. Such a reconstruction, at its most ambitious, is envisioned as playing a role in quantum physics similar to Einstein\'s reconstruction of the dynamics and kinetics of macroscopic bodies, and later of their gravitational interactions, on the basis of simple principles with clear operational meanings and experimental consequences. But short of such an ambitious goal, it could still lead to a principled understanding of the features of quantum mechanics that account for its greater-than-classical information-processing power, an understanding which could help guide the search for new quantum algorithms and protocols. I will summarize a convex operational framework for possible physical theories, and present results from a project to characterize quantum mechanics in terms of principles tightly linked to the possibility or impossibility of various information processing protocols. Previous results identified properties, like the existence of information-disturbance tradeoffs and restrictions on cloning and broadcasting, common to all nonclassical theories. In this talk I will focus on recent results involving protocols that are less generic. These are: the existence of exponentially secure bit commitment in non-classical theories without entanglement, the consequences for theories of the existence of a conclusive teleportation scheme, and sufficient conditions for the existence of a deterministic teleportation scheme. I\'ll also discuss sufficient conditions for \'remote steering\' of ensembles using entanglement, rendering insecure bit commitment protocols of the form shown to be secure in the unentangled case. Connections to the category-theoretic approach of Coecke and Abramsky, Selinger, Baez, and collaborators may be touched on if time permits. Joint work with various groups of collaborators including Jonathan Barrett, Matthew Leifer, Alexander Wilce, Oscar Dahlsten, and Ben Toner.

Information processing in convex operational theories

Howard Barnum

Los Alamos National Laboratory

Oct. 2008 / Perimeter Institute

Information Sciences Group/CCS-3
Los Alamos National Laboratory
barnum@lanl.gov

Primary collaboration: H.B.; J. Barrett, DAMTP, Cambridge; M. Leifer, CQC, U. Waterloo; A. Wilce, U. Susquehanna
Bit commitment collaboration: H.B.; M. Leifer; B. Toner, CWI, Amsterdam; O. Dahlsten, ETH Zürich

Information processing in convex operational theories

Howard Barnum

Los Alamos National Laboratory

Oct. 2008 / Perimeter Institute

Information Sciences Group/CCS-3
Los Alamos National Laboratory
barnum@lanl.gov

Primary collaboration: H.B.; J. Barrett, DAMTP, Cambridge; M. Leifer, CQC, U. Waterloo; A. Wilce, U. Susquehanna
Bit commitment collaboration: H.B.; M. Leifer; B. Toner, CWI, Amsterdam; O. Dahlsten, ETH Zürich

Research program: study information processing in general probabilistic theories

What?

Characterize quantum and classical theories within broad framework of “foil theories”...

...in terms of flow and processing of information.

Research program: study information processing in general probabilistic theories

What?

Characterize quantum and classical theories within broad framework of "foil theories"...
...in terms of flow and processing of information.

Why?

From pragmatism...

- *Conceptual* understanding of info processing: principles $\leftrightarrow$ tasks
  - ...help develop protocols
  - ...understand *limits* to QIP ...
  - ...model info in other complex / concurrent systems?

...to hubris

- Information the essence of quantum physics? ...analogue of Einstein's principle-based accounts of spec/gen relativity?

Research program: study information processing in general probabilistic theories

What?

Characterize quantum and classical theories within broad framework of "foil theories"...
...in terms of flow and processing of information.

Research program: study information processing in general probabilistic theories

What?

Characterize quantum and classical theories within broad framework of "foil theories"...
...in terms of flow and processing of information.

Why?

From pragmatism...

- *Conceptual* understanding of info processing: principles $\leftrightarrow$ tasks
  - ...help develop protocols
  - ...understand *limits* to QIP ...
  - ...model info in other complex / concurrent systems?

...to hubris

- Information the essence of quantum physics? ...analogue of Einstein's principle-based accounts of spec/gen relativity?

Birth of quantum mechanics: an informational break with classical physics

Radical principles underlying quantum information processing recognized by QM's founders

- Measurement disturbs state (Bohr, Heisenberg)
- Entanglement (Schrödinger: "The best possible knowledge of a total system does not necessarily include total knowledge of all its parts, not even when these are fully separated from each other and at the moment are not influencing each other at all.")

Same principles now viewed as underlying QIP's power (e.g. QKD)

Possibly, *many* illuminating characterizations/axiomatizations. Existing characterizations or partial characterizations

- Hardy 2001, D'Ariano recently, Araki 1980, Quantum logical

Rough overview of convex operational formalism

- Systems A, B, C...
- Convex set Ω_A, Ω_B... of states (for each system)
- Convex sets of measurement outcomes $[0, u_A]$.
- Bilinear map: states $\times$ outcomes $\rightarrow$ *probabilities*.
- Convex set of allowable dynamics taking states to states, $\mathscr{D}_A$.
- Way(s) of making "composite" systems, or of recognizing compositeness: $C = A \otimes B$

Main Results

- A set of states is clonable (independent copies) if and only if the states are perfectly distinguishable. (BBLW)
- A set of states is broadcastable (possibly correlated copies) iff it is in the convex hull of a set of clonable states, i.e. in a *classical subset* of states. (BBLW)
- The only information that can be obtained without disturbance is *intrinsically classical* information (information about which "superselection sector" a state is in). (BBLW)
- Necessary conditions for conclusive teleportation (BBLW)
- Sufficient conditions for deterministic teleportation (BBLW)
- Exponentially secure bit commitment is possible in any non-classical theory that does not have entanglement. (BDLT)
- Conditions for "ensemble steering" (generalized Hughston-Jozsa-Wootters Theorem)

1. Abstract State Spaces

Definition

A **cone** in a real vector space A is a set $K \subseteq A$ such that

(a) $a \in K, \lambda \geq 0 \Rightarrow \lambda a \in K$

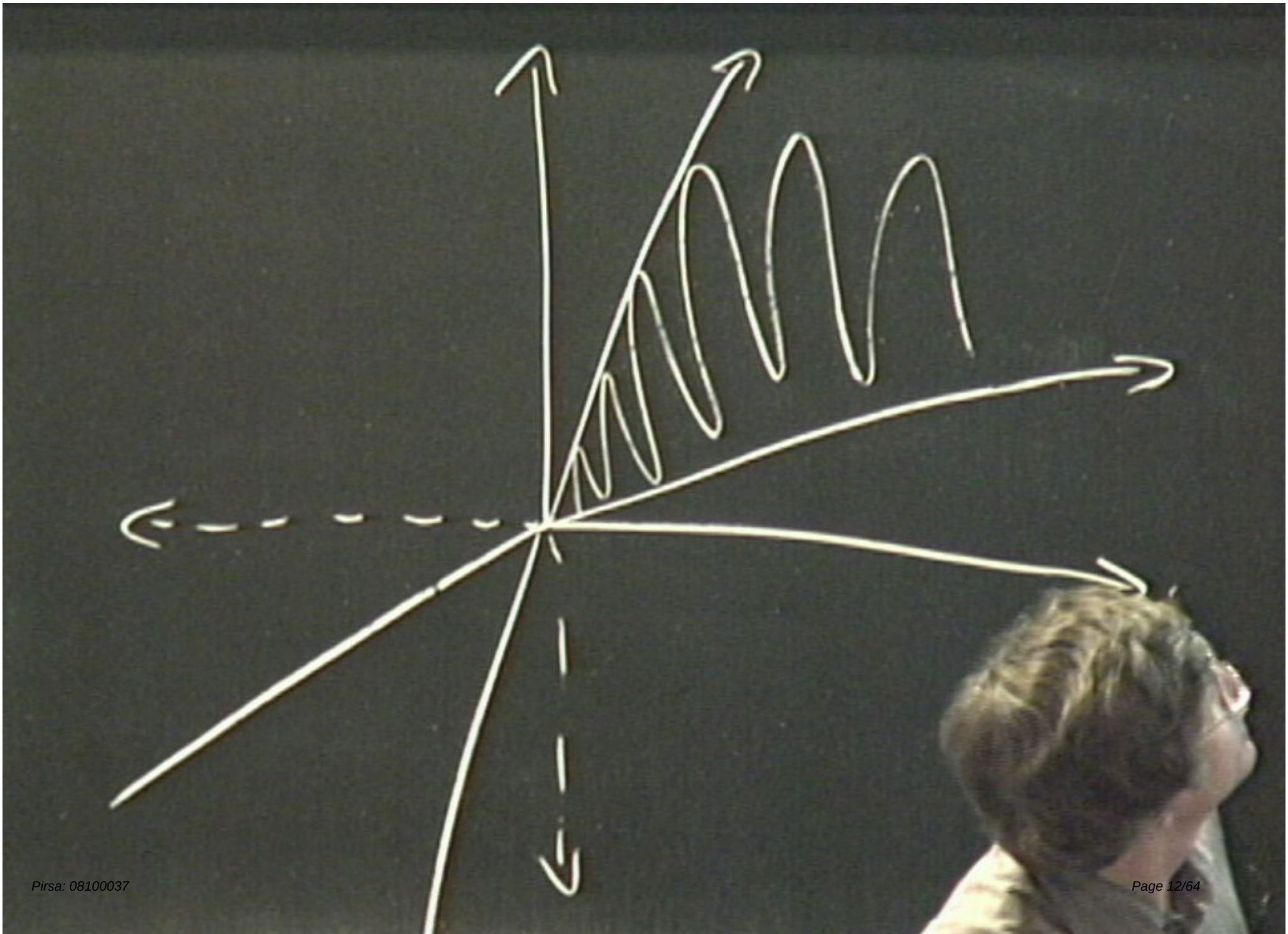
(b) $a, b \in K \Rightarrow a + b \in K$

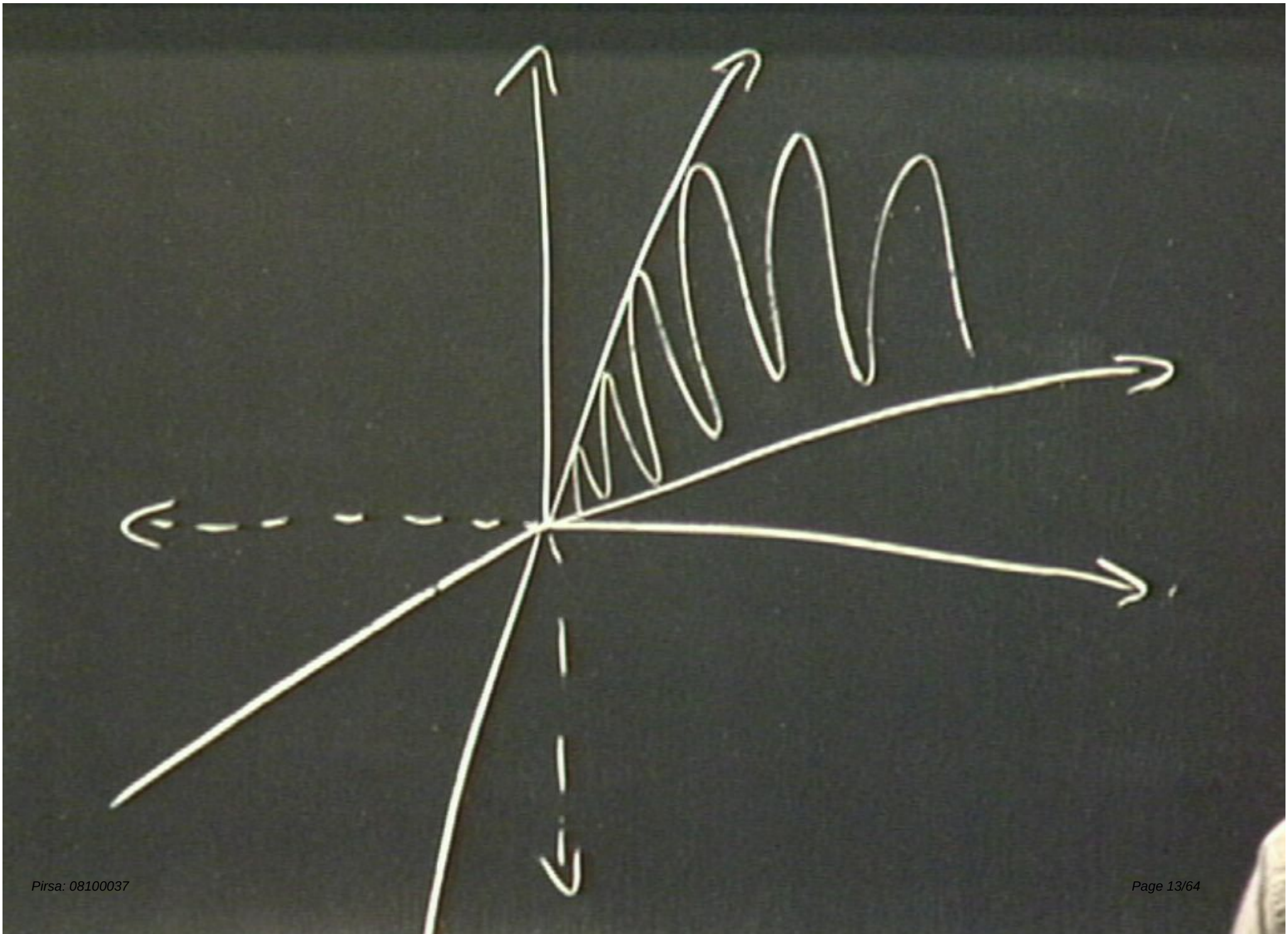
(c) $K \cap -K = \{0\}$. (i.e. **pointed**: contains no non-null subspace.)

Any cone induces a partial order on A, defined by $a \leq b$ iff $b - a \in K$, satisfying $a \leq b \Rightarrow a + c \leq b + c$ for all $a, b, c \in A$, and $a \leq b \Rightarrow \lambda a \leq \lambda b$ for all $\lambda \geq 0$. Conversely, given such an order $K = \{a \in A | a \geq 0\}$ is a cone inducing the order.

A cone K is **generating** iff $A = K - K = \{a - b | a, b \in K\}$.

Henceforth **cone** means generating, topologically closed [pointed, convex] cone, in a finite-dimensional vector space.





1. Abstract State Spaces

Definition

A **cone** in a real vector space A is a set $K \subseteq A$ such that

(a) $a \in K, \lambda \geq 0 \Rightarrow \lambda a \in K$

(b) $a, b \in K \Rightarrow a + b \in K$

(c) $K \cap -K = \{0\}$. (i.e. **pointed**: contains no non-null subspace.)

Any cone induces a partial order on A, defined by $a \leq b$ iff $b - a \in K$, satisfying $a \leq b \Rightarrow a + c \leq b + c$ for all $a, b, c \in A$, and $a \leq b \Rightarrow \lambda a \leq \lambda b$ for all $\lambda \geq 0$. Conversely, given such an order $K = \{a \in A | a \geq 0\}$ is a cone inducing the order.

A cone K is **generating** iff $A = K - K = \{a - b | a, b \in K\}$.

Henceforth **cone** means generating, topologically closed [pointed, convex] cone, in a finite-dimensional vector space.

Abstract State Spaces

Definition

An **abstract state space** is a pair (A, u) where

(i) A is an ordered real vector space with positive cone A_+ and

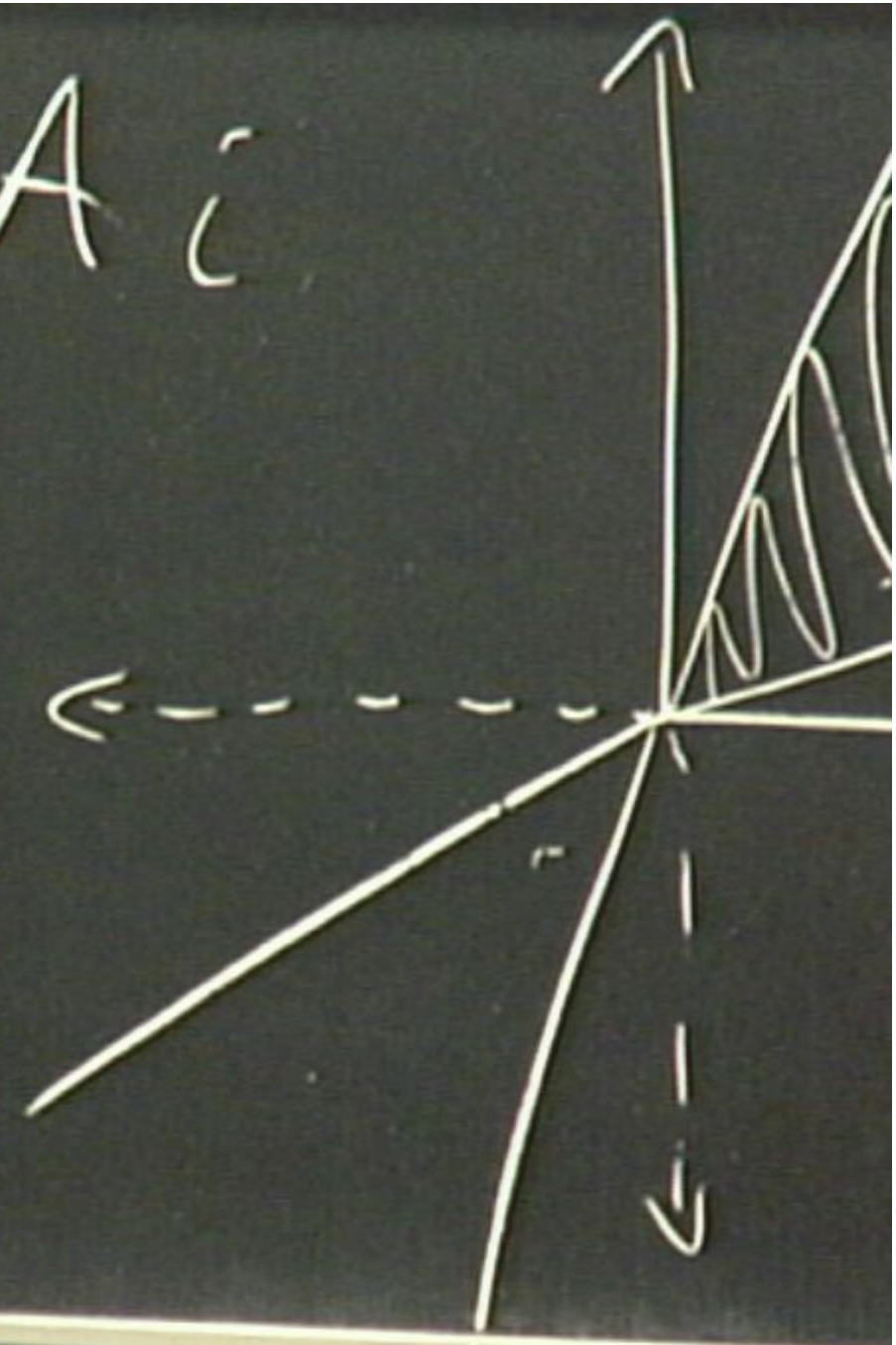
(ii) u is a fixed positive linear functional, called the *order unit*, picking out a set of *normalized states* $\Omega_A = u^{-1}(1)$.

(In fact, any compact convex set has the form Ω_A for a canonical (A, u): Take $A = \mathrm{Aff}(\Omega)^*$).

If $A \simeq \mathbf{R}^d$ as a vector space, Ω_A has affine dimension $d - 1$.

$$K - K = A\,i$$

$$-i$$



Abstract State Spaces

Definition

An **abstract state space** is a pair (A, u) where

(i) A is an ordered real vector space with positive cone A_+ and

(ii) u is a fixed positive linear functional, called the *order unit*, picking out a set of *normalized states* $\Omega_A = u^{-1}(1)$.

(In fact, any compact convex set has the form Ω_A for a canonical (A, u): Take $A = \mathrm{Aff}(\Omega)^*$).

If $A \simeq \mathbf{R}^d$ as a vector space, Ω_A has affine dimension $d - 1$.

Abstract State Spaces

Examples

Classical: $A = \mathbb{R}^X$ (all real functions on a finite set X); $u(f) = \sum_{x \in X} f(x)$. Then Ω_A is the set of probability weights on X. (Note: A has this form iff Ω_A is a simplex.)

Quantum: $A = \mathscr{B}_h(\mathbf{H})$ = self-adjoint operators on complex (f.d.) Hilbert space $\mathbf{H}$; $u(A) = \mathrm{Tr}(A)$. Then Ω_A = density operators.

Neither: $A = n \times n$ matrices with column sums = constant; $u(a)$ = column sum; Ω_A = stochastic matrices. (In 2×2 case, a square.)

Classical State Spaces

Base, Ω, is a d-vertex *simplex* in $\mathbf{R}^d$.

Definition

A **simplex** in $\mathbf{R}^d$ is the affine hull of $d+1$ or fewer affinely independent points.

An equivalent definition is that it is a convex set $\Omega \subset \mathbf{R}^d$ such that every point $x \in \Omega$ has a *unique* convex decomposition $x = \sum_i p_i x_i$ into extreme points x_i.

Measurement outcomes

Measurement outcomes, or **effects**, f are *linear* (in order to preserve convex combination) functionals that are positive on states, i.e. belong to the cone *dual* to A.

$f(\omega)$ interpreted as probability of obtaining outcome f in a measurement when state is ω.

Definition (Dual cone)

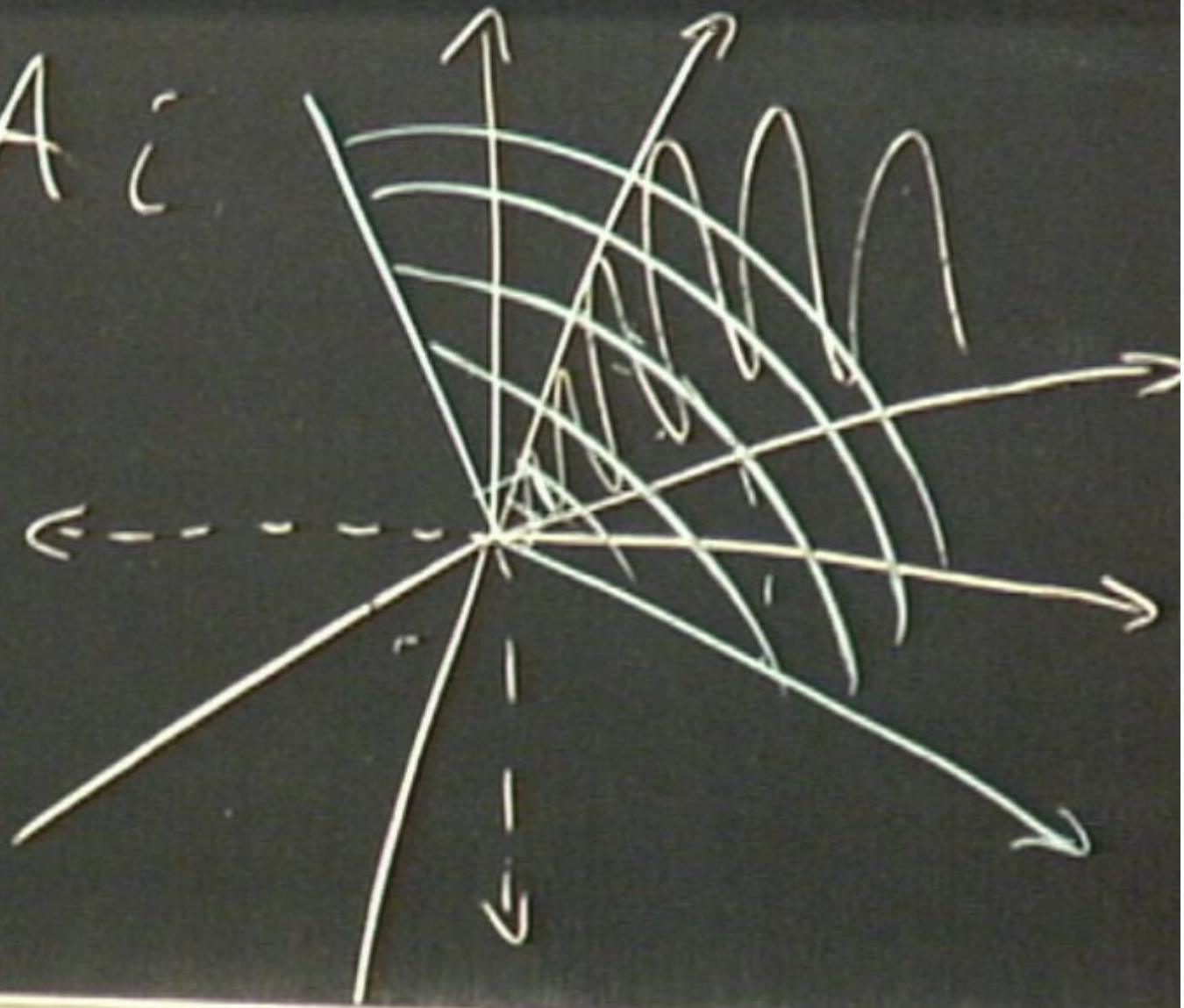
Let A_+ be a cone in A.

$$A_+^* := \{f \in A^* : \forall \omega \in A_+ \; f(\omega) \geq 0\} \tag{1}$$

Effects f also satisfy $\forall \omega \in \Omega, f(\omega) \leq 1$. I.e. $f \leq u$.

I.e., the (normalized) effects are elements the elements of the interval $[0, u]$ in A^*.

$$K - K = A\,i$$



Maximal vs. nonmaximal operational models

In a *maximal* abstract state space, the effects are the unit interval in A^*.
In a *nonmaximal* theory, they are $[0, u_A]$ in some *subcone* $A^\sharp \subset A^*$ containing u_A.
Category-theoretic generalization of this notion... maximal *theory*.

Maximal vs. nonmaximal operational models

In a *maximal* abstract state space, the effects are the unit interval in A^*.
In a *nonmaximal* theory, they are $[0, u_A]$ in some *subcone* $A^\sharp \subset A^*$ containing u_A.
Category-theoretic generalization of this notion... maximal *theory*.

Measurements

Discrete: *resolutions of the unit* into elements of $[0, u]$:

$$\sum_i f_i = u$$

enforces $\sum_i f_i(\omega) = 1$.

Informationally complete if the f_i span V^* (probabilities for $\{f_i\}$'s outcomes in a state determine the state).

Continuously indexed measurements: effect-valued measure $\int d\mu_\alpha f_\alpha = u$.

Maximal vs. nonmaximal operational models

In a *maximal* abstract state space, the effects are the unit interval in A^*.
In a *nonmaximal* theory, they are $[0, u_A]$ in some *subcone* $A^\sharp \subset A^*$ containing u_A.
Category-theoretic generalization of this notion... maximal *theory*.

Measurements

Discrete: *resolutions of the unit* into elements of $[0, u]$:

$$\sum_i f_i = u$$

enforces $\sum_i f_i(\omega) = 1$.

Informationally complete if the f_i span V^* (probabilities for $\{f_i\}$'s outcomes in a state determine the state).

Continuously indexed measurements: effect-valued measure $\int d\mu_\alpha f_\alpha = u$.

Positive Maps and Dynamics

Definition (Positive map $\phi : V \to W$)

Linear map $\phi : V \to W$ such that $\phi(V_+). \subseteq W_+$ Equivalently, preserves order.

A positive map is an *order-isomorphism* (we will just say isomorphism) if it is one-to-one and takes V_+ *onto* W_+. Equivalently: invertible, has positive inverse. If there is an isomorphism from V_+ to W_+, we say V_+ (or V) and W_+ (or W) are isomorphic, $V \simeq W$. *Automorphism*: isomorphism from OLS V to V. $Aut(V)$ a group.

Definition (Dynamics)

A *dynamics* $\mathscr{D}_A$ for an abstract state space (A, u_A) is a cone of positive maps from A to itself, closed under composition and containing id.

$\mathrm{Hom}(A, A)$ anyone?

Measurements

Discrete: *resolutions of the unit* into elements of $[0, u]$:

$$\sum_i f_i = u$$

enforces $\sum_i f_i(\omega) = 1$.

Informationally complete if the f_i span V^* (probabilities for $\{f_i\}$'s outcomes in a state determine the state).

Continuously indexed measurements: effect-valued measure $\int d\mu_\alpha f_\alpha = u$.

Maximal vs. nonmaximal operational models

In a *maximal* abstract state space, the effects are the unit interval in A^*.
In a *nonmaximal* theory, they are $[0, u_A]$ in some *subcone* $A^\sharp \subset A^*$ containing u_A.
Category-theoretic generalization of this notion... maximal *theory*.

Measurements

Discrete: *resolutions of the unit* into elements of $[0, u]$:

$$\sum_i f_i = u$$

enforces $\sum_i f_i(\omega) = 1$.

Informationally complete if the f_i span V^* (probabilities for $\{f_i\}$'s outcomes in a state determine the state).

Continuously indexed measurements: effect-valued measure $\int d\mu_\alpha f_\alpha = u$.

Positive Maps and Dynamics

Definition (Positive map $\phi : V \to W$)

Linear map $\phi : V \to W$ such that $\phi(V_+). \subseteq W_+$ Equivalently, preserves order.

A positive map is an *order-isomorphism* (we will just say isomorphism) if it is one-to-one and takes V_+ *onto* W_+. Equivalently: invertible, has positive inverse. If there is an isomorphism from V_+ to W_+, we say V_+ (or V) and W_+ (or W) are isomorphic, $V \simeq W$. *Automorphism*: isomorphism from OLS V to V. $Aut(V)$ a group.

Definition (Dynamics)

A *dynamics* $\mathscr{D}_A$ for an abstract state space (A, u_A) is a cone of positive maps from A to itself, closed under composition and containing id.

$\mathrm{Hom}(A, A)$ anyone?

Positive Maps and Dynamics

Definition (Positive map $\phi : V \to W$)

Linear map $\phi : V \to W$ such that $\phi(V_+). \subseteq W_+$ Equivalently, preserves order.

A positive map is an *order-isomorphism* (we will just say isomorphism) if it is one-to-one and takes V_+ *onto* W_+. Equivalently: invertible, has positive inverse. If there is an isomorphism from V_+ to W_+, we say V_+ (or V) and W_+ (or W) are isomorphic, $V \simeq W$. *Automorphism*: isomorphism from OLS V to V. $Aut(V)$ a group.

Definition (Dynamics)

A *dynamics* $\mathscr{D}_A$ for an abstract state space (A, u_A) is a cone of positive maps from A to itself, closed under composition and containing id.

$\mathrm{Hom}(A, A)$ anyone?

Category-theoretic version, I

Convexity of the state space and the dynamics are instances of a general principle in the convex operational approach: whatever can happen/be done to a system, can happen or be done conditioned on the outcome of a coin toss. Motivates *enrichment* in the following:

Concrete categories $\mathscr{C}$ of state spaces and positive maps

- Objects: abstract state spaces
- Morphisms: positive maps between state spaces A, B.
- Assumption: $\mathscr{C}(A, B)$ is a cone. (Category is *enriched over ordered linear spaces.*)

Caution: A^* is not necessarily in $\mathscr{C}$.

Definition (Operation)

Norm-nonincreasing positive map ϕ such that $u(\phi(\omega)) \leq u(\omega)$

Definition (Instrument)

Set of norm-nonincreasing maps ϕ_i summing to a norm-preserving one.

Continuously indexed analogues, "operation-valued measures" can also be defined.

Interpretation: ϕ_i "conditional dynamics"; $u(\phi_i)$ probability of process (operation) ϕ_i; map $\omega \mapsto u(\phi_i(\omega))$ is the associated effect.

Internal duals and self-duality

Pick any isomorphism $L : A \to A^*$. Inner product $\langle x, y \rangle := L(x)[y]$ represents functional evaluation "internally".
Quantum case: $\langle X, Y \rangle := \mathrm{tr}\, XY$.

- *Internal dual* of A_+ in such a representation is $A_+^{*int} := \{y \in A : \forall x \in A_+ \langle y, x \rangle \geq 0\}$ isomorphic to A_+^*.
- When there is such a representation L with $A_+^{*int} = A_+$, A is *self-dual*.
- Quantum and classical theory are self-dual!

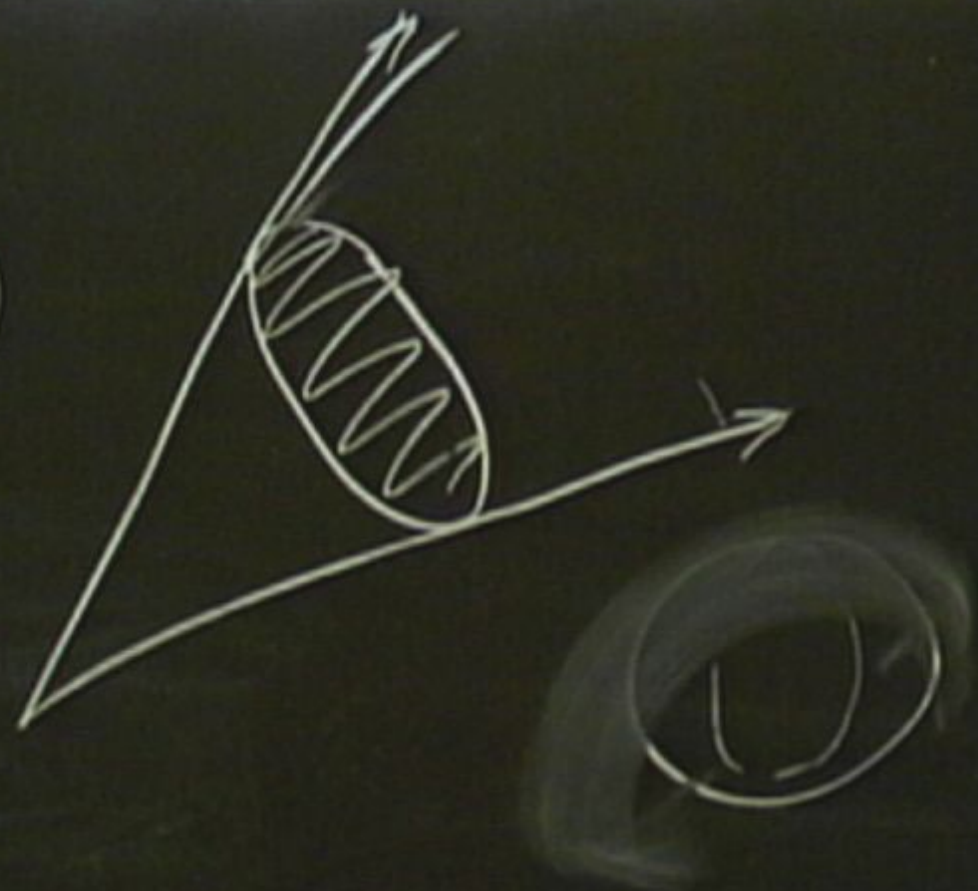
State space characterization

Theorem (Koecher 1958, Vinberg 1960)

Let A be an irreducible, finite-dimensional, self-dual state space, and suppose the group of affine automorphisms of A_+ acts transitively on the interior of A_+. Then Ω is affinely isomorphic to one of the following: (1) The set of density operators on an n-dimensional Hilbert space (so A is quantum); (2) a ball; (3) the set of positive 3×3 trace-one matrices over the octonions.

I.e., state spaces of (finite-dimensional) formally real Jordan algebras.

$$C = \bigoplus_i C_i$$



State space characterization

Theorem (Koecher 1958, Vinberg 1960)

Let A be an irreducible, finite-dimensional, self-dual state space, and suppose the group of affine automorphisms of A_+ acts transitively on the interior of A_+. Then Ω is affinely isomorphic to one of the following: (1) The set of density operators on an n-dimensional Hilbert space (so A is quantum); (2) a ball; (3) the set of positive 3×3 trace-one matrices over the octonions.

I.e., state spaces of (finite-dimensional) formally real Jordan algebras.

Weak self-duality

A weaker condition is simply that there exist an order-isomorphism $\eta : A^* \simeq A$. If this is the case, we shall say that A is *weakly self-dual*.

Example: Let Ω be a square, and let $A = V(\Omega)$. A_+ is weakly self-dual, but not self-dual.

Weak self-duality

A weaker condition is simply that there exist an order-isomorphism $\eta : A^* \simeq A$. If this is the case, we shall say that A is *weakly self-dual*.

Example: Let Ω be a square, and let $A = V(\Omega)$. A_+ is weakly self-dual, but not self-dual.

Composite systems: tensor products

Definition

A **tensor product** of state spaces A and B is a state space $AB = A \otimes B$, ordered by any cone of states that are *positive on product effects* and that contains all pure product states, equipped with order unit $u_{AB} = u_A \otimes u_B$.

Composites II

Examples

(a) The *minimal tensor product*, $A \otimes_{\min} B$, contains *only* convex combinations of product states.

(b) The *maximal tensor product*, $A \otimes_{\max} B$, consists of *all* states positive on product effects. I.e. $A \otimes_{\max} B = (A^* \otimes_{\min} B^*)^*$

(c) If $A = B = \mathscr{B}_h(\mathbf{H})$, then the positive cone on $\mathscr{B}_h(\mathbf{H} \otimes \mathbf{H})$, with its usual ordering, lies properly between the max. and min. cones.

- Definition: States in $A \otimes_{\max} B$ but not in $A \otimes_{\min} B$ are **entangled**; similarly for effects.
- Any state $\omega \in A \otimes B$ has **marginal** or **reduced** states $\omega_A \in A$, $\omega_B \in B$, given by $\omega_A(f) := \omega(f, u_B)$ and $\omega(B)(g) = \omega(u_A, g)$. As in QM (cf. Schrödinger quote above), pure entangled states have mixed marginals, while pure unentangled states do not.

Composites III

This notion of compositeness *embodies* two nontrival assumptions:
(1) No signalling between subsystems (arguably should be part of *definition* of "subsystem".
(2) Local observability (Barrett calls it "global state assumption".) State determinable by local tomography & classical communication.
Local observability violated by real QM w/ natural notion of composite system.
We can define tripartite composites by *direct generalization* of the bipartite definition, or *recursively* from it, but in either case we need a further nontrivial requirement of "regularity", roughly:
Regularity: Conditioning on products of effects in some slots, gives valid local states of the composite in the others.
Nontriviality from example: $(A \otimes_{\min} A) \otimes_{\max} (A \otimes_{\min} A)$ is not regular

Composite systems: tensor products

Definition

A **tensor product** of state spaces A and B is a state space $AB = A \otimes B$, ordered by any cone of states that are *positive on product effects* and that contains all pure product states, equipped with order unit $u_{AB} = u_A \otimes u_B$.

Composites II

Examples

(a) The *minimal tensor product*, $A \otimes_{\min} B$, contains *only* convex combinations of product states.

(b) The *maximal tensor product*, $A \otimes_{\max} B$, consists of *all* states positive on product effects. I.e. $A \otimes_{\max} B = (A^* \otimes_{\min} B^*)^*$

(c) If $A = B = \mathscr{B}_h(\mathbf{H})$, then the positive cone on $\mathscr{B}_h(\mathbf{H} \otimes \mathbf{H})$, with its usual ordering, lies properly between the max. and min. cones.

- Definition: States in $A \otimes_{\max} B$ but not in $A \otimes_{\min} B$ are **entangled**; similarly for effects.
- Any state $\omega \in A \otimes B$ has **marginal** or **reduced** states $\omega_A \in A$, $\omega_B \in B$, given by $\omega_A(f) := \omega(f, u_B)$ and $\omega(B)(g) = \omega(u_A, g)$. As in QM (cf. Schrödinger quote above), pure entangled states have mixed marginals, while pure unentangled states do not.

Composites III

This notion of compositeness *embodies* two nontrival assumptions:
(1) No signalling between subsystems (arguably should be part of *definition* of "subsystem".
(2) Local observability (Barrett calls it "global state assumption".) State determinable by local tomography & classical communication.
Local observability violated by real QM w/ natural notion of composite system.
We can define tripartite composites by *direct generalization* of the bipartite definition, or *recursively* from it, but in either case we need a further nontrivial requirement of "regularity", roughly:
Regularity: Conditioning on products of effects in some slots, gives valid local states of the composite in the others.
Nontriviality from example: $(A \otimes_{\min} A) \otimes_{\max} (A \otimes_{\min} A)$ is not regular

Classicality in the convex framework

Many properties sometimes thought of as "peculiarly quantum" are generically nonclassical, e.g.:

- Impossibility of universal pure-state cloning
- Impossibility of universal mixed-state broadcasting
- Ability to extract full information about an unknown pure state in a theory without disturbing it

Demonstrated in some of our earlier work, and sharpened to characterize broadcastable sets of states (classical subsets) and information obtainable without disturbance (*intrinsically* classical information).
Here I will emphasize things not common to all nonclassical theories, in particular the existence of **teleportation** and **bit commitment** protocols.

Composites III

This notion of compositeness *embodies* two nontrival assumptions:
(1) No signalling between subsystems (arguably should be part of *definition* of "subsystem".
(2) Local observability (Barrett calls it "global state assumption".) State determinable by local tomography & classical communication.
Local observability violated by real QM w/ natural notion of composite system.
We can define tripartite composites by *direct generalization* of the bipartite definition, or *recursively* from it, but in either case we need a further nontrivial requirement of "regularity", roughly:
Regularity: Conditioning on products of effects in some slots, gives valid local states of the composite in the others.
Nontriviality from example: $(A \otimes_{\min} A) \otimes_{\max} (A \otimes_{\min} A)$ is not regular

Composites III

This notion of compositeness *embodies* two nontrival assumptions:
(1) No signalling between subsystems (arguably should be part of *definition* of "subsystem".
(2) Local observability (Barrett calls it "global state assumption".) State determinable by local tomography & classical communication.
Local observability violated by real QM w/ natural notion of composite system.
We can define tripartite composites by *direct generalization* of the bipartite definition, or *recursively* from it, but in either case we need a further nontrivial requirement of "regularity", roughly:
Regularity: Conditioning on products of effects in some slots, gives valid local states of the composite in the others.
Nontriviality from example: $(A \otimes_{\min} A) \otimes_{\max} (A \otimes_{\min} A)$ is not regular

Classicality in the convex framework

Many properties sometimes thought of as "peculiarly quantum" are generically nonclassical, e.g.:

- Impossibility of universal pure-state cloning
- Impossibility of universal mixed-state broadcasting
- Ability to extract full information about an unknown pure state in a theory without disturbing it

Demonstrated in some of our earlier work, and sharpened to characterize broadcastable sets of states (classical subsets) and information obtainable without disturbance (*intrinsically* classical information).
Here I will emphasize things not common to all nonclassical theories, in particular the existence of **teleportation** and **bit commitment** protocols.

Marginals, Cloning and Broadcasting Skip

Definition (Marginal state and map)

For $\omega \in (A \otimes B)_+$, its *marginal state* ω_A is defined by $\omega_A : f \mapsto \omega(f \otimes u_B)$. For $T : V \to (A \otimes B)$, its *marginal map* T_A is defined by $T_A : \omega \mapsto (T(\omega))_A$.

Definition (Cloning)

$T : V \to V \otimes V$ *clones* α if $T(\alpha) = \alpha \otimes \alpha$. T *clones* $S \subseteq \Omega$ if it clones every state in S. S is *clonable* if there is a positive map T that clones it.

Definition (Broadcasting)

$T : V \to V \otimes V$ *broadcasts* α if $T_A(\alpha) = T_B(\alpha) = \alpha$. T *broadcasts* $S \subseteq \Omega$ if it broadcasts every state in S. S is *broadcastable* if there is a positive map T that clones it.

Direct sums of cones

Definition (Direct sum of cones)

Cone C is a *direct sum* of disjoint-except-for-0 cones $C_i \subseteq C$, written $C = \oplus_i C_i$, if every element of C is a convex combination of elements of the C_i.

- There are no "coherent superpositions" of elements of different C_i's, only mixtures. So the answer to "which summand" is *intrinsically classical* information.
- Every cone (recall finite d!) is uniquely a finite direct sum of cones, $C = \oplus_i C_i$.
- A simplex (classical system) is a direct sum of copies of the one-dimensional cone.

Only intrinsically classical information can be obtained without disturbance (Skip)

Definition (Operation nondisturbing to a pure state)

An operation T *does not disturb* a pure state ω if $T(\omega) = c\omega$ for some $c \geq 0$.

Definition (Operation nondisturbing to a state)

An operation T *does not disturb* a state ω if it does not disturb any pure state that can appear in a convex decomposition of ω.

Theorem (Information-Disturbance)

An operation T is nondisturbing to all states in Ω iff it can be written:

$$T = \oplus_i c_i \mathrm{id}_i \tag{2}$$

where $c_i \geq 0$, $V(\Omega)_+ = \oplus_i C_i$, and id_i is the identity on the direct summand C_i.

Remote Evaluation

Given a bipartite state $\omega \in A \otimes_{\max} B$, we can **condition** on the occurrence of an effect $f \in A^*$, defining $\omega_f \in B$ by

$$\omega_f(g) = \omega(f \otimes g).$$

(We are dealing with un-normalized states; normalizing yields the usual conditional state.)

Lemma (Remote Evaluation)

Let $f \in (A \otimes B)^*$ and $\omega \in B \otimes C$. Then, for any $\alpha \in A$,

$$(\alpha \otimes \omega)_f = \hat{\omega}(\hat{f}(\alpha)). \tag{3}$$

If the tripartite system $A \otimes_{\min} (B \otimes_{\max} C)$ is in state $\alpha \otimes \omega$, α unknown, then conditional on securing measurement outcome f on $A \otimes B$, the state of C is a *known function of* α.

Conclusive teleportation

If $C \simeq A$ and $\tau = \hat{\omega} \circ \hat{f}$ is *physically reversible* (invertible with norm non-increasing inverse), then performing the operation τ^{-1} at C reproduces α. This is *conclusive (one-outcome post-selected) teleportation*. When this is possible, we say that B *teleports* A. [Teleportation in a *given* composite requires that f and ω belong to $(A \otimes B)^*, (B \otimes C)$ respectively.]

Theorem (Conclusive Teleportation)

A teleports through B iff there exist a positive embedding $i : A \to B^*$, and a positive idempotent (projection) $P : B^* \to B^*$ with range $i(A)$.

When $B \simeq A^*$, A teleports through B.
When $B \simeq A$, the existence of the embedding i is *weak self-duality*.
If $B \simeq A$, when can we teleport with a *uniform* tensor product.

Remote Evaluation

Given a bipartite state $\omega \in A \otimes_{\max} B$, we can **condition** on the occurrence of an effect $f \in A^*$, defining $\omega_f \in B$ by

$$\omega_f(g) = \omega(f \otimes g).$$

(We are dealing with un-normalized states; normalizing yields the usual conditional state.)

Lemma (Remote Evaluation)

Let $f \in (A \otimes B)^*$ and $\omega \in B \otimes C$. Then, for any $\alpha \in A$,

$$(\alpha \otimes \omega)_f = \hat{\omega}(\hat{f}(\alpha)). \tag{3}$$

If the tripartite system $A \otimes_{\min} (B \otimes_{\max} C)$ is in state $\alpha \otimes \omega$, α unknown, then conditional on securing measurement outcome f on $A \otimes B$, the state of C is a *known function of* α.

Conclusive teleportation

If $C \simeq A$ and $\tau = \hat{\omega} \circ \hat{f}$ is *physically reversible* (invertible with norm non-increasing inverse), then performing the operation τ^{-1} at C reproduces α. This is *conclusive (one-outcome post-selected) teleportation*. When this is possible, we say that B *teleports* A. [Teleportation in a *given* composite requires that f and ω belong to $(A \otimes B)^*, (B \otimes C)$ respectively.]

Theorem (Conclusive Teleportation)

A teleports through B iff there exist a positive embedding $i : A \to B^*$, and a positive idempotent (projection) $P : B^* \to B^*$ with range $i(A)$.

When $B \simeq A^*$, A teleports through B.
When $B \simeq A$, the existence of the embedding i is *weak self-duality*.
If $B \simeq A$, when can we teleport with a *uniform* tensor product.

$$\alpha \qquad A \otimes \underbrace{B \otimes C}_{\omega^{BC}}$$

$$\underbrace{\qquad}_{f^{AB}} \qquad \hat{\omega} : f \longmapsto \omega_f$$

$$\hat{f} : A \to B^* \qquad A^* \longrightarrow B$$

Conclusive teleportation

If $C \simeq A$ and $\tau = \hat{\omega} \circ \hat{f}$ is *physically reversible* (invertible with norm non-increasing inverse), then performing the operation τ^{-1} at C reproduces α. This is *conclusive (one-outcome post-selected) teleportation*. When this is possible, we say that B *teleports* A. [Teleportation in a *given* composite requires that f and ω belong to $(A \otimes B)^*, (B \otimes C)$ respectively.]

Theorem (Conclusive Teleportation)

A teleports through B iff there exist a positive embedding $i : A \to B^*$, and a positive idempotent (projection) $P : B^* \to B^*$ with range $i(A)$.

When $B \simeq A^*$, A teleports through B.
When $B \simeq A$, the existence of the embedding i is *weak self-duality*.
If $B \simeq A$, when can we teleport with a *uniform* tensor product.

Theorem (Deterministic Teleportation)

Let $A \simeq B$. If there exist
(1) A finite, norm-preserving subgroup G of $Aut(A)$ with a unique invariant state ω_0, and
(2) an isomorphism $\hat{f} : A \to B^*$ such that $\hat{f}(\omega_0) = u_B$,
then there's a composite $A \otimes (B \otimes C)$ with a deterministic teleportation scheme.

Proof uses group-averaging,

A sufficient condition for the existence of ω_0 is that G act transitively on the normalized pure states of A.
Also, note that, given the existence of ω_0, any G-equivariant isomorphism from A to B^* will satisfy (2).
For details, see BBLW08

Theorem (Deterministic Teleportation)

Let $A \simeq B$. If there exist
(1) A finite, norm-preserving subgroup G of $Aut(A)$ with a unique invariant state ω_0, and
(2) an isomorphism $\hat{f} : A \to B^*$ such that $\hat{f}(\omega_0) = u_B$,
then there's a composite $A \otimes (B \otimes C)$ with a deterministic teleportation scheme.

Proof uses group-averaging,

A sufficient condition for the existence of ω_0 is that G act transitively on the normalized pure states of A.
Also, note that, given the existence of ω_0, any G-equivariant isomorphism from A to B^* will satisfy (2).
For details, see BBLW08

Bit Commitment

Definition: In a **bit commitment protocol**, Alice commits to a bit value, 0 or 1, in a way that is:

1. **Hiding:** until she reveals it, Bob gets no information about it
2. **Binding:** if she tries to change it after commiting, Bob's test will detect her attempt
3. **Sound:** if Alice and Bob honestly perform the protocol, Bob will know the bit after Alice reveals it, and won't falsely accuse Alice of cheating

- Important cryptographic primitive that enables many other tasks
- Classically, possible given assumptions about hardness of certain computations, but *not* possible with information-theoretic security.
- Also impossible in quantum mechanics (Mayers; Lo and Chau (1996)).

Conclusive teleportation

If $C \simeq A$ and $\tau = \hat{\omega} \circ \hat{f}$ is *physically reversible* (invertible with norm non-increasing inverse), then performing the operation τ^{-1} at C reproduces α. This is *conclusive (one-outcome post-selected) teleportation*. When this is possible, we say that B *teleports* A. [Teleportation in a *given* composite requires that f and ω belong to $(A \otimes B)^*, (B \otimes C)$ respectively.]

Theorem (Conclusive Teleportation)

A teleports through B iff there exist a positive embedding $i : A \to B^*$, and a positive idempotent (projection) $P : B^* \to B^*$ with range $i(A)$.

When $B \simeq A^*$, A teleports through B.
When $B \simeq A$, the existence of the embedding i is *weak self-duality*.
If $B \simeq A$, when can we teleport with a *uniform* tensor product.

Conclusive teleportation

If $C \simeq A$ and $\tau = \hat{\omega} \circ \hat{f}$ is *physically reversible* (invertible with norm non-increasing inverse), then performing the operation τ^{-1} at C reproduces α. This is *conclusive (one-outcome post-selected) teleportation*. When this is possible, we say that B *teleports* A. [Teleportation in a *given* composite requires that f and ω belong to $(A \otimes B)^*, (B \otimes C)$ respectively.]

Theorem (Conclusive Teleportation)

A teleports through B iff there exist a positive embedding $i : A \to B^*$, and a positive idempotent (projection) $P : B^* \to B^*$ with range $i(A)$.

When $B \simeq A^*$, A teleports through B.
When $B \simeq A$, the existence of the embedding i is *weak self-duality*.
If $B \simeq A$, when can we teleport with a *uniform* tensor product.