Unentangled Bit Commitment and the Clifton-Bub-Halvorson (CBH) Theorem

M. S. Leifer

Institute for Quantum Computing
University of Waterloo

Perimeter Institute for Theoretical Physics

Dec. 18th 2007/Pavia Mini-Workshop

Outline

The Brassard-Fuchs Speculation

In ≈2000, Brassard and Fuchs speculated that the basic Hilbert Space structures of quantum theory might be uniquely determined by two cryptographic constraints:

- The Possibility of Secure Key Distribution
- The Impossibility of Bit Commitment

This was to be viewed as analogous to Einstein's derivation of the kinematics for special relativity from the two postulates:

- The laws of physics are invariant under changes of inertial frame.
- The speed of light in vacuo is constant in all inertial frames.

The Brassard-Fuchs Speculation

In $\approx$2000, Brassard and Fuchs speculated that the basic Hilbert Space structures of quantum theory might be uniquely determined by two cryptographic constraints:

- The Possibility of Secure Key Distribution
- The Impossibility of Bit Commitment

This was to be viewed as analogous to Einstein's derivation of the kinematics for special relativity from the two postulates:

- The laws of physics are invariant under changes of inertial frame.
- The speed of light in vacuo is constant in all inertial frames.

The Brassard-Fuchs Speculation

This derivation has to be done within a precise mathematical framework for physical theories, which must be:

- Narrow enough to convert the axioms into precise mathematical constraints.
- Broad enough that the work is being done by the postulates rather than the framework assumptions.

We are allowed to import definitions and concepts from existing physical frameworks, just as Einstein did.

The Brassard-Fuchs Speculation

This derivation has to be done within a precise mathematical framework for physical theories, which must be:

- Narrow enough to convert the axioms into precise mathematical constraints.
- Broad enough that the work is being done by the postulates rather than the framework assumptions.

We are allowed to import definitions and concepts from existing physical frameworks, just as Einstein did.

The Brassard-Fuchs Speculation

This derivation has to be done within a precise mathematical framework for physical theories, which must be:

- Narrow enough to convert the axioms into precise mathematical constraints.
- Broad enough that the work is being done by the postulates rather than the framework assumptions.

We are allowed to import definitions and concepts from existing physical frameworks, just as Einstein did.

The CBH Theorem

In 2003, Clifton, Bub and Halvorson "derived quantum theory" from:

- The impossibility of superluminal information transfer between two physical systems by performing measurements on one of them.
- The impossibility of perfectly broadcasting the information contained in an unknown physical state.
- The impossibility of unconditionally secure bit commitment.

The mathematical framework chosen was C^*-algebraic theories.

The CBH Theorem

CBH don't arrive exactly at quantum theory, but intend their theorem to be read as follows:

1. No signalling $\Rightarrow$ Separate systems correspond to commuting algebras of observables.
2. No broadcasting $\Rightarrow$ Algebras corresponding to individual systems are nonabelian.
3. No bit commitment $\Rightarrow$ Bipartite systems can occupy entangled states.

There is some debate about whether 3 is independent of 1 and 2.

The CBH Theorem

CBH don't arrive exactly at quantum theory, but intend their theorem to be read as follows:

1. No signalling $\Rightarrow$ Separate systems correspond to commuting algebras of observables.
2. No broadcasting $\Rightarrow$ Algebras corresponding to individual systems are nonabelian.
3. No bit commitment $\Rightarrow$ Bipartite systems can occupy entangled states.

There is some debate about whether 3 is independent of 1 and 2.

The CBH Theorem

CBH don't arrive exactly at quantum theory, but intend their theorem to be read as follows:

1. No signalling $\Rightarrow$ Separate systems correspond to commuting algebras of observables.
2. No broadcasting $\Rightarrow$ Algebras corresponding to individual systems are nonabelian.
3. No bit commitment $\Rightarrow$ Bipartite systems can occupy entangled states.

There is some debate about whether 3 is independent of 1 and 2.

The CBH Theorem

CBH don't arrive exactly at quantum theory, but intend their theorem to be read as follows:

1. No signalling $\Rightarrow$ Separate systems correspond to commuting algebras of observables.
2. No broadcasting $\Rightarrow$ Algebras corresponding to individual systems are nonabelian.
3. No bit commitment $\Rightarrow$ Bipartite systems can occupy entangled states.

There is some debate about whether 3 is independent of 1 and 2.

Why C^*-algebras?

We are not in the business of rigorous axiomatization, so CBH say:

> *...it suffices for present purposes simply to observe that all physical theories that have been found empirically successful – not just phase space and Hilbert space theories but also theories based on a manifold – fall under this framework*

They should have added: AND THAT'S IT!

Why C^*-algebras?

We are not in the business of rigorous axiomatization, so CBH say:

> *...it suffices for present purposes simply to observe that all physical theories that have been found empirically successful – not just phase space and Hilbert space theories but also theories based on a manifold – fall under this framework*

They should have added: AND THAT'S IT!

Why C^*-algebras?

We are not in the business of rigorous axiomatization, so CBH say:

> *...it suffices for present purposes simply to observe that all physical theories that have been found empirically successful – not just phase space and Hilbert space theories but also theories based on a manifold – fall under this framework*

They should have added: AND THAT'S IT!

C^*-algebras: Reasons to be skeptical

- C^*-algebras were invented to do a Hilbert's 10th job on quantum theory – particularly QFT and quantum stat. mech.
- Every C^*-algebra has a faithful Hilbert space representation (GNS theorem).
- In finite dimensions we only have classical probability, quantum theory and quantum theory with superselection rules.
- In infinite dimensions it's essentially the same story.

It is pretty easy to derive quantum theory if you assume quantum theory at the outset.

C^*-algebras: Reasons to be skeptical

- C^*-algebras were invented to do a Hilbert's 10th job on quantum theory – particularly QFT and quantum stat. mech.
- Every C^*-algebra has a faithful Hilbert space representation (GNS theorem).
- In finite dimensions we only have classical probability, quantum theory and quantum theory with superselection rules.
- In infinite dimensions it's essentially the same story.

It is pretty easy to derive quantum theory if you assume quantum theory at the outset.

C^*-algebras: Reasons to be skeptical

- C^*-algebras were invented to do a Hilbert's 10th job on quantum theory – particularly QFT and quantum stat. mech.
- Every C^*-algebra has a faithful Hilbert space representation (GNS theorem).
- In finite dimensions we only have classical probability, quantum theory and quantum theory with superselection rules.
- In infinite dimensions it's essentially the same story.

It is pretty easy to derive quantum theory if you assume quantum theory at the outset.

C^*-algebras: Reasons to be skeptical

- C^*-algebras were invented to do a Hilbert's 10th job on quantum theory – particularly QFT and quantum stat. mech.
- Every C^*-algebra has a faithful Hilbert space representation (GNS theorem).
- In finite dimensions we only have classical probability, quantum theory and quantum theory with superselection rules.
- In infinite dimensions it's essentially the same story.

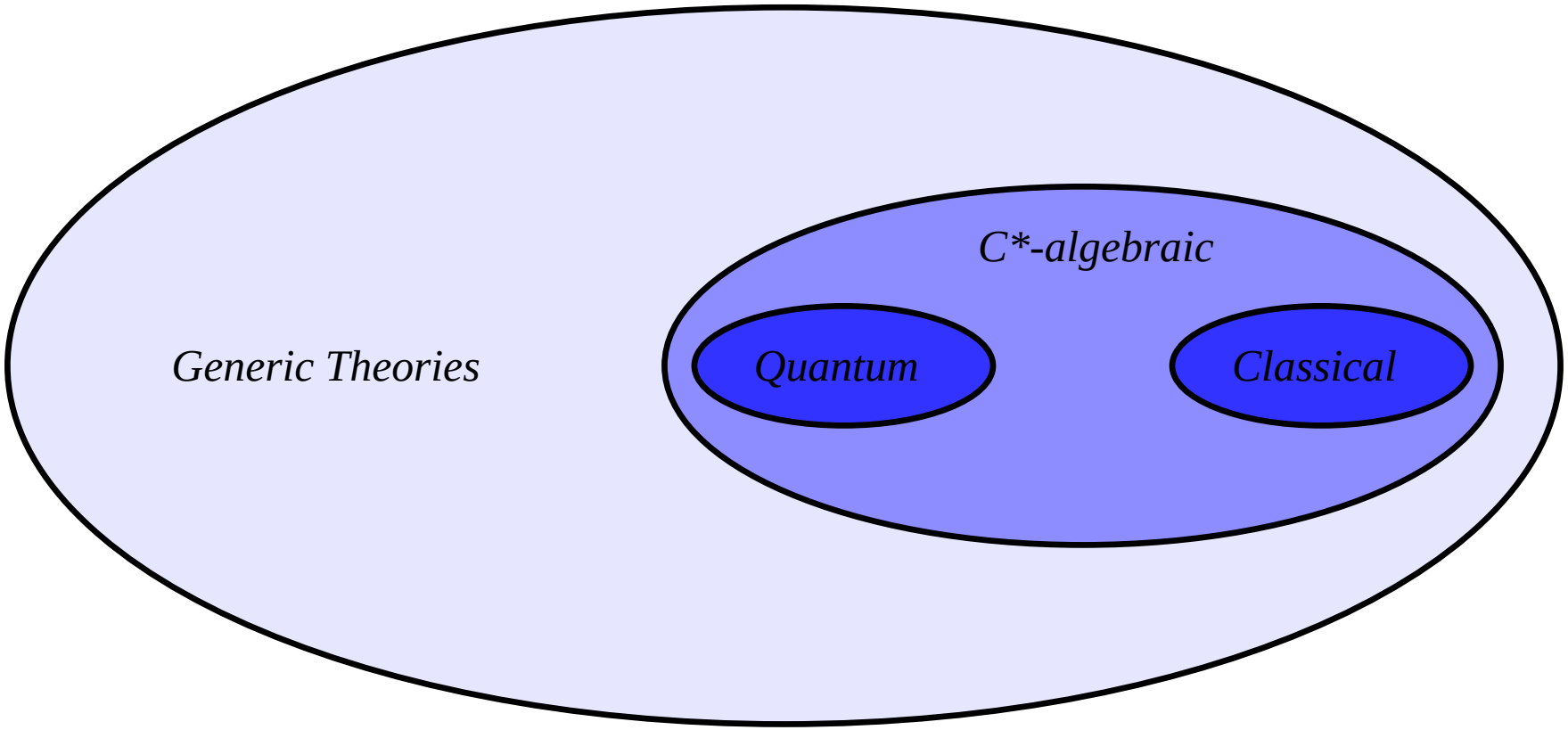
It is pretty easy to derive quantum theory if you assume quantum theory at the outset.

C^*-algebras: Reasons to be skeptical

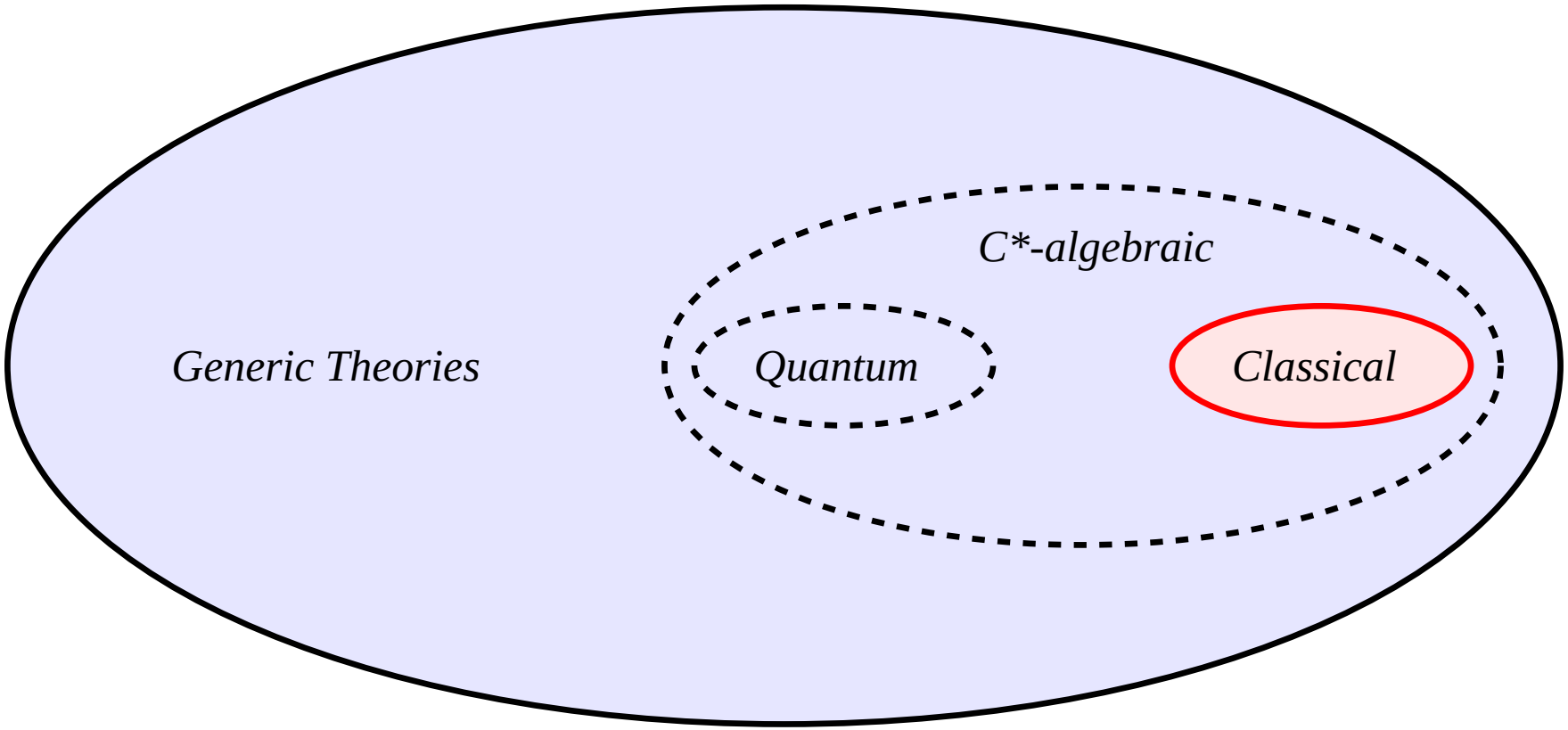
- C^*-algebras were invented to do a Hilbert's 10th job on quantum theory – particularly QFT and quantum stat. mech.
- Every C^*-algebra has a faithful Hilbert space representation (GNS theorem).
- In finite dimensions we only have classical probability, quantum theory and quantum theory with superselection rules.
- In infinite dimensions it's essentially the same story.

It is pretty easy to derive quantum theory if you assume quantum theory at the outset.

Generalized Probabilistic Frameworks

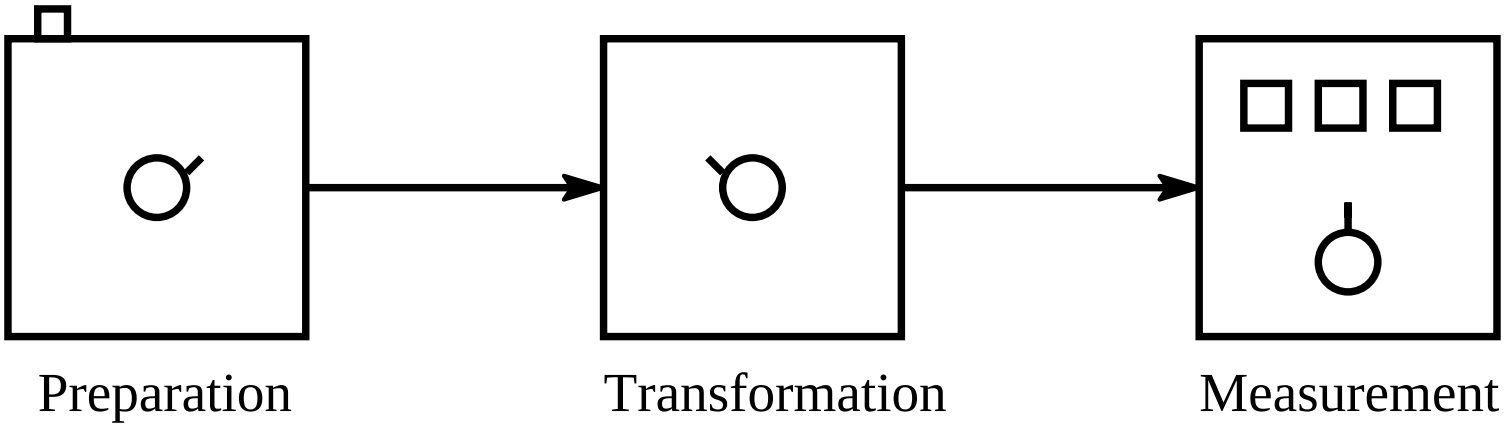


The End Result



The Convex Sets Framework

- A traditional operational framework.



- Goal: Predict Prob(outcome|Choice of P, T and M)

Preparations $\longrightarrow$ States

Definition

The set Ω of normalized states is a compact, closed, convex set.

- Convex: If $\omega, \mu \in \Omega$ and $p \in [0,1]$ then $p\omega + (1-p)\mu \in \Omega$.
- Extreme points of Ω are called pure states.
- Note: Every convex subset of a locally convex topological vector space is affinely homeomorphic to the set of all states on a test space (F. W. Shultz, *Journal of Combinatorial Theory A* 17, 317 (1974)).

Preparations $\longrightarrow$ States

Definition

The set Ω of normalized states is a compact, closed, convex set.

- Convex: If $\omega, \mu \in \Omega$ and $p \in [0, 1]$ then $p\omega + (1 - p)\mu \in \Omega$.
- Extreme points of Ω are called pure states.
- Note: Every convex subset of a locally convex topological vector space is affinely homeomorphic to the set of all states on a test space (F. W. Shultz, *Journal of Combinatorial Theory A* 17, 317 (1974)).

Preparations → States

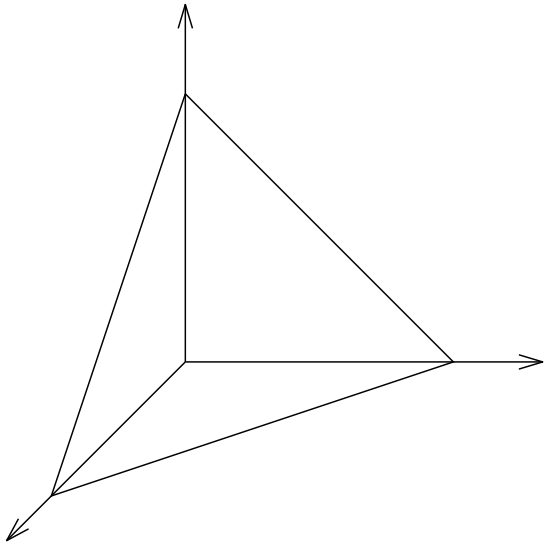
Definition

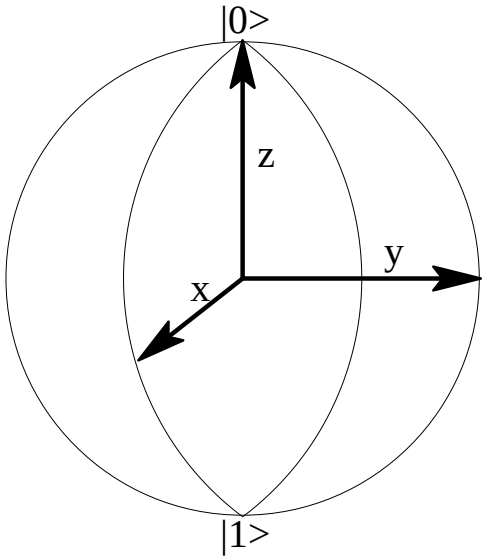
The set Ω of normalized states is a compact, closed, convex set.

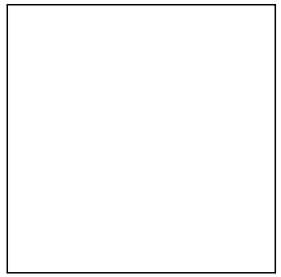
- Convex: If $\omega, \mu \in \Omega$ and $p \in [0, 1]$ then $p\omega + (1 - p)\mu \in \Omega$.
- Extreme points of Ω are called pure states.
- Note: Every convex subset of a locally convex topological vector space is affinely homeomorphic to the set of all states on a test space (F. W. Shultz, *Journal of Combinatorial Theory A* 17, 317 (1974)).

Examples

- Classical: $\Omega =$ Probability simplex.
- Quantum: $\Omega = \{$Denisty matrices$\}$.
- Polyhedral.







Measurement Outcomes → Effects

Definition

Let $A(\Omega)$ be the set of affine functionals $\Omega \to \mathbb{R}$ and $V(\Omega)$ be the set of positive affine functionals $\Omega \to \mathbb{R}^+$.

$$\forall p \in [0,1],\ f(p\omega + (1-p)\mu) = pf(\omega) + (1-p)f(\mu)$$

- $A(\Omega)$ is a vector space and $V(\Omega)$ is a convex cone.

$$(\alpha f + \beta g)(\omega) = \alpha f(\omega) + \beta g(\omega)$$

- $V(\Omega)$ spans $A(\Omega)$.
- Partial order on $A(\Omega)$: $f \leq g$ iff $\forall \omega \in \Omega,\ f(\omega) \leq g(\omega)$.
- Unit: $\forall \omega \in \Omega,\ \tilde{1}(\omega) = 1$. Zero: $\forall v \in V,\ \tilde{0}(v) = 0$.
- Normalized effects: $[\tilde{0}, \tilde{1}] = \{f \in V(\Omega) | \tilde{0} \leq f \leq \tilde{1}\}$.

Measurement Outcomes → Effects

Definition

Let $A(\Omega)$ be the set of affine functionals $\Omega \to \mathbb{R}$ and $V(\Omega)$ be the set of positive affine functionals $\Omega \to \mathbb{R}^+$.

$$\forall p \in [0,1],\ f(p\omega + (1-p)\mu) = pf(\omega) + (1-p)f(\mu)$$

- $A(\Omega)$ is a vector space and $V(\Omega)$ is a convex cone.

$$(\alpha f + \beta g)(\omega) = \alpha f(\omega) + \beta g(\omega)$$

- $V(\Omega)$ spans $A(\Omega)$.
- Partial order on $A(\Omega)$: $f \leq g$ iff $\forall \omega \in \Omega,\ f(\omega) \leq g(\omega)$.
- Unit: $\forall \omega \in \Omega,\ \tilde{1}(\omega) = 1$. Zero: $\forall v \in V,\ \tilde{0}(v) = 0$.
- Normalized effects: $[\tilde{0}, \tilde{1}] = \{f \in V(\Omega) | \tilde{0} \leq f \leq \tilde{1}\}$.

Measurement Outcomes → Effects

Definition

Let $A(\Omega)$ be the set of affine functionals $\Omega \to \mathbb{R}$ and $V(\Omega)$ be the set of positive affine functionals $\Omega \to \mathbb{R}^+$.

$$\forall p \in [0,1],\ f(p\omega + (1-p)\mu) = pf(\omega) + (1-p)f(\mu)$$

- $A(\Omega)$ is a vector space and $V(\Omega)$ is a convex cone.

$$(\alpha f + \beta g)(\omega) = \alpha f(\omega) + \beta g(\omega)$$

- $V(\Omega)$ spans $A(\Omega)$.
- Partial order on $A(\Omega)$: $f \leq g$ iff $\forall \omega \in \Omega,\ f(\omega) \leq g(\omega)$.
- Unit: $\forall \omega \in \Omega,\ \tilde{1}(\omega) = 1$. Zero: $\forall v \in V,\ \tilde{0}(v) = 0$.
- Normalized effects: $[\tilde{0}, \tilde{1}] = \{f \in V(\Omega) | \tilde{0} \leq f \leq \tilde{1}\}$.

Measurement Outcomes → Effects

Definition

Let $A(\Omega)$ be the set of affine functionals $\Omega \to \mathbb{R}$ and $V(\Omega)$ be the set of positive affine functionals $\Omega \to \mathbb{R}^+$.

$$\forall p \in [0,1],\ f(p\omega + (1-p)\mu) = pf(\omega) + (1-p)f(\mu)$$

- $A(\Omega)$ is a vector space and $V(\Omega)$ is a convex cone.

$$(\alpha f + \beta g)(\omega) = \alpha f(\omega) + \beta g(\omega)$$

- $V(\Omega)$ spans $A(\Omega)$.
- Partial order on $A(\Omega)$: $f \leq g$ iff $\forall \omega \in \Omega,\ f(\omega) \leq g(\omega)$.
- Unit: $\forall \omega \in \Omega,\ \tilde{1}(\omega) = 1$. Zero: $\forall v \in V,\ \tilde{0}(v) = 0$.
- Normalized effects: $[\tilde{0}, \tilde{1}] = \{f \in V(\Omega) | \tilde{0} \leq f \leq \tilde{1}\}$.

Measurement Outcomes → Effects

Definition

Let $A(\Omega)$ be the set of affine functionals $\Omega \to \mathbb{R}$ and $V(\Omega)$ be the set of positive affine functionals $\Omega \to \mathbb{R}^+$.

$$\forall p \in [0,1],\ f(p\omega + (1-p)\mu) = pf(\omega) + (1-p)f(\mu)$$

- $A(\Omega)$ is a vector space and $V(\Omega)$ is a convex cone.

$$(\alpha f + \beta g)(\omega) = \alpha f(\omega) + \beta g(\omega)$$

- $V(\Omega)$ spans $A(\Omega)$.
- Partial order on $A(\Omega)$: $f \leq g$ iff $\forall \omega \in \Omega,\ f(\omega) \leq g(\omega)$.
- Unit: $\forall \omega \in \Omega,\ \tilde{1}(\omega) = 1$. Zero: $\forall v \in V,\ \tilde{0}(v) = 0$.
- Normalized effects: $[\tilde{0}, \tilde{1}] = \{f \in V(\Omega) | \tilde{0} \leq f \leq \tilde{1}\}$.

Measurement Outcomes → Effects

Definition

Let $A(\Omega)$ be the set of affine functionals $\Omega \to \mathbb{R}$ and $V(\Omega)$ be the set of positive affine functionals $\Omega \to \mathbb{R}^+$.

$$\forall p \in [0,1],\ f(p\omega + (1-p)\mu) = pf(\omega) + (1-p)f(\mu)$$

- $A(\Omega)$ is a vector space and $V(\Omega)$ is a convex cone.

$$(\alpha f + \beta g)(\omega) = \alpha f(\omega) + \beta g(\omega)$$

- $V(\Omega)$ spans $A(\Omega)$.
- Partial order on $A(\Omega)$: $f \leq g$ iff $\forall \omega \in \Omega,\ f(\omega) \leq g(\omega)$.
- Unit: $\forall \omega \in \Omega,\ \tilde{1}(\omega) = 1$. Zero: $\forall v \in V,\ \tilde{0}(v) = 0$.
- Normalized effects: $[\tilde{0}, \tilde{1}] = \{f \in V(\Omega) | \tilde{0} \leq f \leq \tilde{1}\}$.

States as vectors

- Consider the dual space $A(\Omega)^*$ of linear functionals $A(\Omega) \longrightarrow \mathbb{R}$ and the dual cone of $V(\Omega)^*$ of linear functionals $V(\Omega) \longrightarrow \mathbb{R}^+$.
- $V(\Omega)^*$ can be extended to $A(\Omega)$.
- An element of Ω can be mapped to an element of $V(\Omega)^*$ via $\omega^*(f) = f(\omega)$.
- $V(\Omega)^*$ can be thought of as the set of unnormalized states.

States as vectors

- Consider the dual space $A(\Omega)^*$ of linear functionals $A(\Omega) \longrightarrow \mathbb{R}$ and the dual cone of $V(\Omega)^*$ of linear functionals $V(\Omega) \longrightarrow \mathbb{R}^+$.
- $V(\Omega)^*$ can be extended to $A(\Omega)$.
- An element of Ω can be mapped to an element of $V(\Omega)^*$ via $\omega^*(f) = f(\omega)$.
- $V(\Omega)^*$ can be thought of as the set of unnormalized states.

States as vectors

- Consider the dual space $A(\Omega)^*$ of linear functionals $A(\Omega) \longrightarrow \mathbb{R}$ and the dual cone of $V(\Omega)^*$ of linear functionals $V(\Omega) \longrightarrow \mathbb{R}^+$.
- $V(\Omega)^*$ can be extended to $A(\Omega)$.
- An element of Ω can be mapped to an element of $V(\Omega)^*$ via $\omega^*(f) = f(\omega)$.
- $V(\Omega)^*$ can be thought of as the set of unnormalized states.

States as vectors

- Consider the dual space $A(\Omega)^*$ of linear functionals $A(\Omega) \to \mathbb{R}$ and the dual cone of $V(\Omega)^*$ of linear functionals $V(\Omega) \to \mathbb{R}^+$.
- $V(\Omega)^*$ can be extended to $A(\Omega)$.
- An element of Ω can be mapped to an element of $V(\Omega)^*$ via $\omega^*(f) = f(\omega)$.
- $V(\Omega)^*$ can be thought of as the set of unnormalized states.

Examples

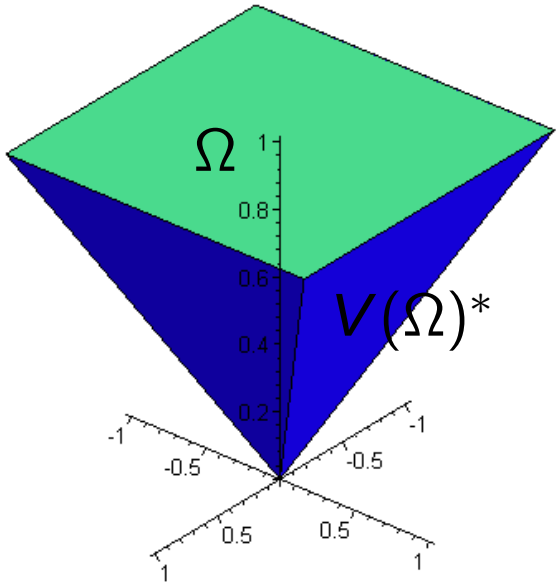
- Classical:
  - $A(\Omega) = \{\text{functions}\}$
  - $V(\Omega) = \{\text{positive functions}\}$
  - $[\tilde{0}, \tilde{1}] = \{\text{Fuzzy indicator functions}\}$
  - $V(\Omega)^* = \{\text{positive functions}\}$
- Quantum:
  - $A(\Omega) \cong \{\text{Hermitian operators}\}$ via $f(\rho) = \text{Tr}(A_f \rho)$
  - $V(\Omega) \cong \{\text{positive operators}\}$
  - $[\tilde{0}, \tilde{1}] \cong \{\text{POVM elements}\}$
  - $V(\Omega)^* \cong \{\text{positive operators}\}$

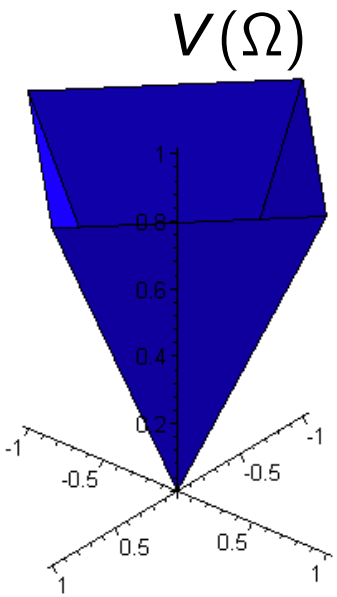
Examples

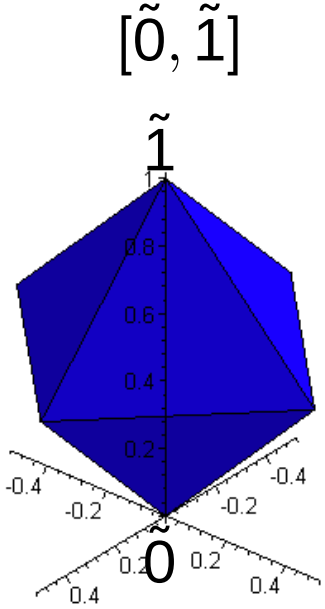
- Classical:
  - $A(\Omega) = \{\text{functions}\}$
  - $V(\Omega) = \{\text{positive functions}\}$
  - $[\tilde{0}, \tilde{1}] = \{\text{Fuzzy indicator functions}\}$
  - $V(\Omega)^* = \{\text{positive functions}\}$
- Quantum:
  - $A(\Omega) \cong \{\text{Hermitian operators}\}$ via $f(\rho) = \text{Tr}(A_f \rho)$
  - $V(\Omega) \cong \{\text{positive operators}\}$
  - $[\tilde{0}, \tilde{1}] \cong \{\text{POVM elements}\}$
  - $V(\Omega)^* \cong \{\text{positive operators}\}$

Examples

- Polyhedral:







Observables

Definition

An observable is a finite collection $(f_1, f_2, \ldots, f_N)$ of elements of $[\tilde{0}, \tilde{1}]$ that satisfies $\sum_{j=1}^{N} f_j = \tilde{1}$.

- Note: Analogous to a POVM in Quantum Theory.
- Can give more sophisticated measure-theoretic definition.

Observables

Definition

An observable is a finite collection $(f_1, f_2, \ldots, f_N)$ of elements of $[\tilde{0}, \tilde{1}]$ that satisfies $\sum_{j=1}^{N} f_j = \tilde{1}$.

- Note: Analogous to a POVM in Quantum Theory.
- Can give more sophisticated measure-theoretic definition.

Observables

Definition

An observable is a finite collection $(f_1, f_2, \ldots, f_N)$ of elements of $[\tilde{0}, \tilde{1}]$ that satisfies $\sum_{j=1}^{N} f_j = \tilde{1}$.

- Note: Analogous to a POVM in Quantum Theory.
- Can give more sophisticated measure-theoretic definition.

Dynamics

Definition

The dynamical maps $\mathfrak{D}_{B|A}$ are a convex subset of the affine maps $\phi : V(\Omega_A)^* \to V(\Omega_B)^*$.

$$\forall \alpha, \beta \geq 0,\ \phi(\alpha\omega_A + \mu_B) = \alpha\phi(\omega_A) + \beta\phi(\mu_B)$$

You might want to require other things, e.g.

- The identity is in $\mathfrak{D}_{A|A}$.
- Maps can be composed.
- $\forall f \in V(\Omega_A), \mu_B \in V(\Omega_B)^*,\ \phi(\omega_A) = f(\omega_A)\mu_B$ is in $\mathfrak{D}_{B|A}$.

Dynamics

Definition

The dynamical maps $\mathfrak{D}_{B|A}$ are a convex subset of the affine maps $\phi : V(\Omega_A)^* \to V(\Omega_B)^*$.

$$\forall \alpha, \beta \geq 0,\ \phi(\alpha\omega_A + \mu_B) = \alpha\phi(\omega_A) + \beta\phi(\mu_B)$$

You might want to require other things, e.g.

- The identity is in $\mathfrak{D}_{A|A}$.
- Maps can be composed.
- $\forall f \in V(\Omega_A), \mu_B \in V(\Omega_B)^*,\ \phi(\omega_A) = f(\omega_A)\mu_B$ is in $\mathfrak{D}_{B|A}$.

Dynamics

Definition

The dynamical maps $\mathfrak{D}_{B|A}$ are a convex subset of the affine maps $\phi : V(\Omega_A)^* \to V(\Omega_B)^*$.

$$\forall \alpha, \beta \geq 0,\ \phi(\alpha\omega_A + \mu_B) = \alpha\phi(\omega_A) + \beta\phi(\mu_B)$$

You might want to require other things, e.g.

- The identity is in $\mathfrak{D}_{A|A}$.
- Maps can be composed.
- $\forall f \in V(\Omega_A), \mu_B \in V(\Omega_B)^*,\ \phi(\omega_A) = f(\omega_A)\mu_B$ is in $\mathfrak{D}_{B|A}$.

Dynamics

Definition

The dynamical maps $\mathfrak{D}_{B|A}$ are a convex subset of the affine maps $\phi : V(\Omega_A)^* \to V(\Omega_B)^*$.

$$\forall \alpha, \beta \geq 0,\ \phi(\alpha\omega_A + \mu_B) = \alpha\phi(\omega_A) + \beta\phi(\mu_B)$$

You might want to require other things, e.g.

- The identity is in $\mathfrak{D}_{A|A}$.
- Maps can be composed.
- $\forall f \in V(\Omega_A), \mu_B \in V(\Omega_B)^*,\ \phi(\omega_A) = f(\omega_A)\mu_B$ is in $\mathfrak{D}_{B|A}$.

Combining Systems: Tensor Products

- Given Ω_A and Ω_B, what is the joint space Ω_{AB}?
- We assume:
  - A joint state must assign joint probabilities to $f_A \in [\tilde{0}_A, \tilde{1}_B], f_B \in [\tilde{0}_A, \tilde{1}_B]$.
  - No-signaling.
  - States are uniquely determined by probability assignments to pairs f_A, f_B.
- This does not give a unique tensor product, but a range of possibilities.
- Direct products: $\omega_A \otimes \omega_B(f_A, f_B) = \omega_A(f_A)\omega_B(f_B)$

Combining Systems: Tensor Products

- Given Ω_A and Ω_B, what is the joint space Ω_{AB}?
- We assume:
  - A joint state must assign joint probabilities to $f_A \in [\tilde{0}_A, \tilde{1}_B], f_B \in [\tilde{0}_A, \tilde{1}_B]$.
  - No-signaling.
  - States are uniquely determined by probability assignments to pairs f_A, f_B.
- This does not give a unique tensor product, but a range of possibilities.
- Direct products: $\omega_A \otimes \omega_B(f_A, f_B) = \omega_A(f_A)\omega_B(f_B)$

Combining Systems: Tensor Products

- Given Ω_A and Ω_B, what is the joint space Ω_{AB}?
- We assume:
  - A joint state must assign joint probabilities to $f_A \in [\tilde{0}_A, \tilde{1}_B], f_B \in [\tilde{0}_A, \tilde{1}_B]$.
  - No-signaling.
  - States are uniquely determined by probability assignments to pairs f_A, f_B.
- This does not give a unique tensor product, but a range of possibilities.
- Direct products: $\omega_A \otimes \omega_B(f_A, f_B) = \omega_A(f_A)\omega_B(f_B)$

Combining Systems: Tensor Products

- Given Ω_A and Ω_B, what is the joint space Ω_{AB}?
- We assume:
  - A joint state must assign joint probabilities to $f_A \in [\tilde{0}_A, \tilde{1}_B], f_B \in [\tilde{0}_A, \tilde{1}_B]$.
  - No-signaling.
  - States are uniquely determined by probability assignments to pairs f_A, f_B.
- This does not give a unique tensor product, but a range of possibilities.
- Direct products: $\omega_A \otimes \omega_B(f_A, f_B) = \omega_A(f_A)\omega_B(f_B)$

Combining Systems: Tensor Products

- Given Ω_A and Ω_B, what is the joint space Ω_{AB}?
- We assume:
  - A joint state must assign joint probabilities to $f_A \in [\tilde{0}_A, \tilde{1}_B], f_B \in [\tilde{0}_A, \tilde{1}_B]$.
  - No-signaling.
  - States are uniquely determined by probability assignments to pairs f_A, f_B.
- This does not give a unique tensor product, but a range of possibilities.
- Direct products: $\omega_A \otimes \omega_B(f_A, f_B) = \omega_A(f_A)\omega_B(f_B)$

Combining Systems: Tensor Products

- Given Ω_A and Ω_B, what is the joint space Ω_{AB}?
- We assume:
  - A joint state must assign joint probabilities to $f_A \in [\tilde{0}_A, \tilde{1}_B], f_B \in [\tilde{0}_A, \tilde{1}_B]$.
  - No-signaling.
  - States are uniquely determined by probability assignments to pairs f_A, f_B.
- This does not give a unique tensor product, but a range of possibilities.
- Direct products: $\omega_A \otimes \omega_B(f_A, f_B) = \omega_A(f_A)\omega_B(f_B)$

Combining Systems: Tensor Products

Definition

Separable TP: $V(\Omega_A)^* \otimes_{\text{sep}} V(\Omega_B)^* =$
conv $\{\omega_A \otimes \omega_B | \omega_A \in V(\Omega_A)^*,\ \omega_B \in V(\Omega_B)^*\}$

Definition

Maximal TP: $V(\Omega_A)^* \otimes_{\max} V(\Omega_B)^* = (V(\Omega_A) \otimes_{\text{sep}} V(\Omega_B))^*$

Definition

A tensor product $V(\Omega_A)^* \otimes V(\Omega_B)^*$ is a convex cone that satisfies

$$V(\Omega_A)^* \otimes_{\text{sep}} V(\Omega_B)^* \subseteq V(\Omega_A)^* \otimes V(\Omega_B)^* \subseteq V(\Omega_A)^* \otimes_{\max} V(\Omega_B)^*.$$

Combining Systems: Tensor Products

Definition

Separable TP: $V(\Omega_A)^* \otimes_{\text{sep}} V(\Omega_B)^* =$
$\text{conv}\{\omega_A \otimes \omega_B | \omega_A \in V(\Omega_A)^*,\ \omega_B \in V(\Omega_B)^*\}$

Definition

Maximal TP: $V(\Omega_A)^* \otimes_{\max} V(\Omega_B)^* = (V(\Omega_A) \otimes_{\text{sep}} V(\Omega_B))^*$

Definition

A tensor product $V(\Omega_A)^* \otimes V(\Omega_B)^*$ is a convex cone that satisfies

$$V(\Omega_A)^* \otimes_{\text{sep}} V(\Omega_B)^* \subseteq V(\Omega_A)^* \otimes V(\Omega_B)^* \subseteq V(\Omega_A)^* \otimes_{\max} V(\Omega_B)^*.$$

Combining Systems: Tensor Products

Definition

Separable TP: $V(\Omega_A)^* \otimes_{\text{sep}} V(\Omega_B)^* =$
$\text{conv}\{\omega_A \otimes \omega_B | \omega_A \in V(\Omega_A)^*,\ \omega_B \in V(\Omega_B)^*\}$

Definition

Maximal TP: $V(\Omega_A)^* \otimes_{\max} V(\Omega_B)^* = (V(\Omega_A) \otimes_{\text{sep}} V(\Omega_B))^*$

Definition

A tensor product $V(\Omega_A)^* \otimes V(\Omega_B)^*$ is a convex cone that satisfies

$$V(\Omega_A)^* \otimes_{\text{sep}} V(\Omega_B)^* \subseteq V(\Omega_A)^* \otimes V(\Omega_B)^* \subseteq V(\Omega_A)^* \otimes_{\max} V(\Omega_B)^*.$$

Distinguishability

Definition

A set of states $\{\omega_1, \omega_2, \ldots, \omega_N\}$, $\omega_j \in \Omega$, is jointly distinguishable if $\exists$ an observable $(f_1, f_2, \ldots, f_N)$ s.t.

$$f_j(\omega_k) = \delta_{jk}.$$

Fact

The set of pure states of Ω is jointly distinguishable iff Ω is a simplex.

Distinguishability

Definition

A set of states $\{\omega_1, \omega_2, \ldots, \omega_N\}$, $\omega_j \in \Omega$, is jointly distinguishable if $\exists$ an observable $(f_1, f_2, \ldots, f_N)$ s.t.

$$f_j(\omega_k) = \delta_{jk}.$$

Fact

The set of pure states of Ω is jointly distinguishable iff Ω is a simplex.

Reduced States and Maps

Definition

Given a state $v_{AB} \in V_A \otimes V_B$, the marginal state on V_A is defined by

$$\forall f_A \in V_A^*, \quad f_A(v_A) = f_A \otimes \tilde{1}_B(\omega_{AB}).$$

Definition

Given an affine map $\phi_{BC|A} : V_A \to V_B \otimes V_C$, the reduced map $\phi : V_A \to V_B$ is defined by

$$\forall f_B \in V_B^*, v_A \in V_A, \quad f_B(\phi_{B|A}(v_A)) = f_B \otimes \tilde{1}_C \left(\phi_{BC|A}(v_A)\right).$$

Reduced States and Maps

Definition

Given a state $v_{AB} \in V_A \otimes V_B$, the marginal state on V_A is defined by

$$\forall f_A \in V_A^*, \quad f_A(v_A) = f_A \otimes \tilde{1}_B(\omega_{AB}).$$

Definition

Given an affine map $\phi_{BC|A} : V_A \to V_B \otimes V_C$, the reduced map $\phi : V_A \to V_B$ is defined by

$$\forall f_B \in V_B^*, v_A \in V_A, \quad f_B(\phi_{B|A}(v_A)) = f_B \otimes \tilde{1}_C \left(\phi_{BC|A}(v_A)\right).$$

Broadcasting

Definition

A state $\omega \in \Omega$ is broadcast by a NPA map $\phi_{A'A''|A} : V_A \to V_{A'} \otimes V_{A''}$ if $\phi_{A'|A}(\omega) = \phi_{A''|A}(\omega) = \omega$.

- Cloning is a special case where outputs must be uncorrelated.

Definition

A set of states is co-broadcastable if there exists an NPA map that broadcasts all of them.

Broadcasting

Definition

A state $\omega \in \Omega$ is broadcast by a NPA map $\phi_{A'A''|A} : V_A \to V_{A'} \otimes V_{A''}$ if $\phi_{A'|A}(\omega) = \phi_{A''|A}(\omega) = \omega$.

- Cloning is a special case where outputs must be uncorrelated.

Definition

A set of states is co-broadcastable if there exists an NPA map that broadcasts all of them.

Broadcasting

Definition

A state $\omega \in \Omega$ is broadcast by a NPA map $\phi_{A'A''|A} : V_A \to V_{A'} \otimes V_{A''}$ if $\phi_{A'|A}(\omega) = \phi_{A''|A}(\omega) = \omega$.

- Cloning is a special case where outputs must be uncorrelated.

Definition

A set of states is co-broadcastable if there exists an NPA map that broadcasts all of them.

The No-Broadcasting Theorem

Theorem

A set of states is co-broadcastable iff it is contained in a simplex that has jointly distinguishable vertices.

- Quantum theory: states must commute.
- Universal broadcasting only possible in classical theories.

Theorem

The set of states broadcast by any affine map is a simplex that has jointly distinguishable vertices.

The No-Broadcasting Theorem

Theorem

A set of states is co-broadcastable iff it is contained in a simplex that has jointly distinguishable vertices.

- Quantum theory: states must commute.
- Universal broadcasting only possible in classical theories.

Theorem

The set of states broadcast by any affine map is a simplex that has jointly distinguishable vertices.

The No-Broadcasting Theorem

Theorem

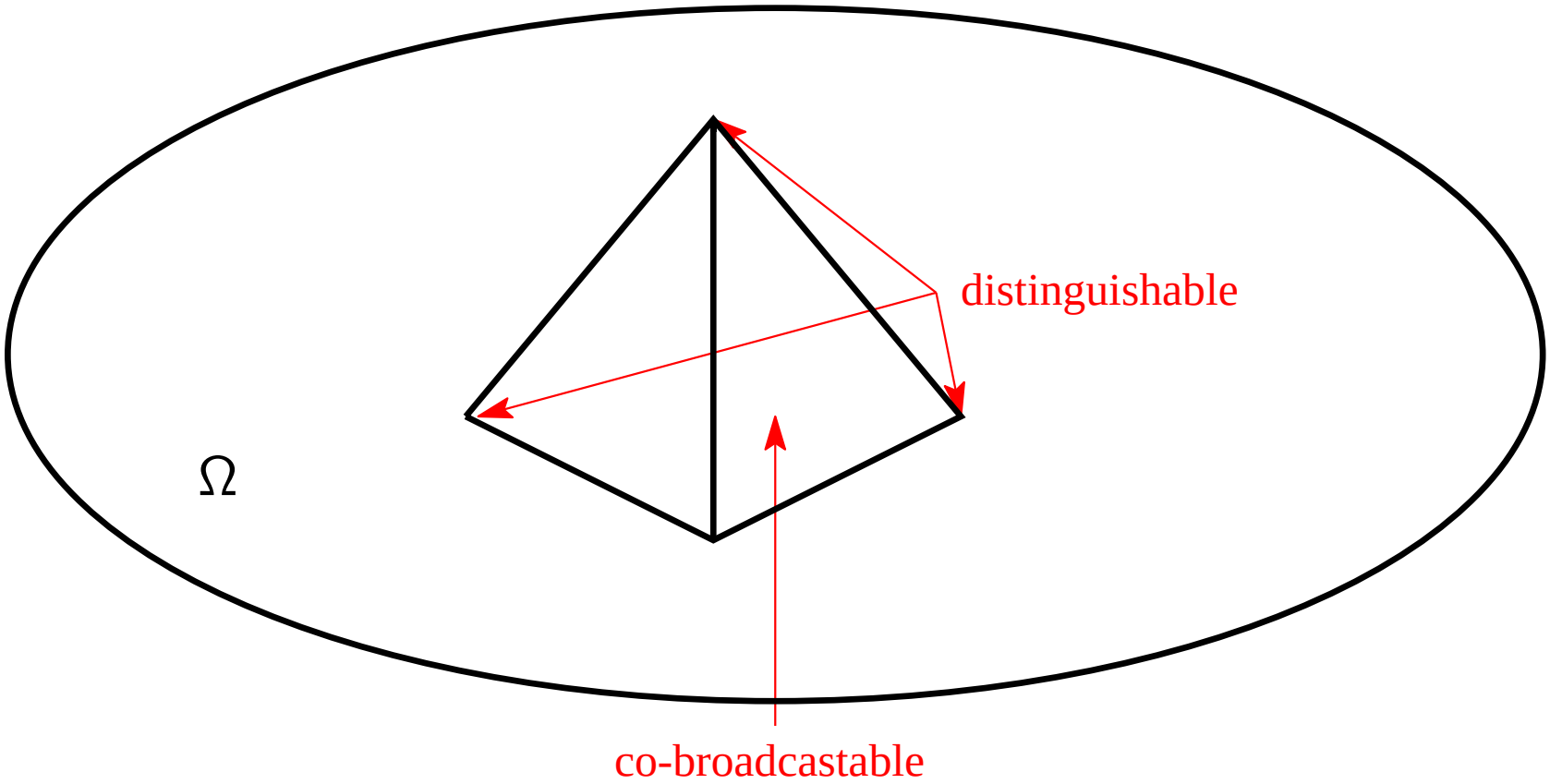
A set of states is co-broadcastable iff it is contained in a simplex that has jointly distinguishable vertices.

- Quantum theory: states must commute.
- Universal broadcasting only possible in classical theories.

Theorem

The set of states broadcast by any affine map is a simplex that has jointly distinguishable vertices.

The No-Broadcasting Theorem



Comparison to CBH Theorem

Like CBH we have:

- No broadcasting $\Rightarrow$ State spaces of individual systems are nonclassical.
- No bit commitment $\Rightarrow$ Entangled states must exist.

Unlike CBH:

- No signaling has become a framework assumption.
- Postulates are genuinely independent.
- We are not particularly close to quantum theory.

Comparison to CBH Theorem

Like CBH we have:

- No broadcasting $\Rightarrow$ State spaces of individual systems are nonclassical.
- No bit commitment $\Rightarrow$ Entangled states must exist.

Unlike CBH:

- No signaling has become a framework assumption.
- Postulates are genuinely independent.
- We are not particularly close to quantum theory.

Comparison to CBH Theorem

Like CBH we have:

- No broadcasting $\Rightarrow$ State spaces of individual systems are nonclassical.
- No bit commitment $\Rightarrow$ Entangled states must exist.

Unlike CBH:

- No signaling has become a framework assumption.
- Postulates are genuinely independent.
- We are not particularly close to quantum theory.

Comparison to CBH Theorem

Like CBH we have:

- No broadcasting $\Rightarrow$ State spaces of individual systems are nonclassical.
- No bit commitment $\Rightarrow$ Entangled states must exist.

Unlike CBH:

- No signaling has become a framework assumption.
- Postulates are genuinely independent.
- We are not particularly close to quantum theory.

Comparison to CBH Theorem

Like CBH we have:

- No broadcasting $\Rightarrow$ State spaces of individual systems are nonclassical.
- No bit commitment $\Rightarrow$ Entangled states must exist.

Unlike CBH:

- No signaling has become a framework assumption.
- Postulates are genuinely independent.
- We are not particularly close to quantum theory.

Open Questions

- Are all qualitative QCrypto results, e.g. key distribution, generic?
- Can other qinfo constraints, e.g. teleportation, get us closer to quantum theory?
- Is bit commitment possible in any theories with entanglement?

Open Questions

- Are all qualitative QCrypto results, e.g. key distribution, generic?
- Can other qinfo constraints, e.g. teleportation, get us closer to quantum theory?
- Is bit commitment possible in any theories with entanglement?

Open Questions

- Are all qualitative QCrypto results, e.g. key distribution, generic?
- Can other qinfo constraints, e.g. teleportation, get us closer to quantum theory?
- Is bit commitment possible in any theories with entanglement?

Conjecture

- Weak version: If the set of joint probabilities that Alice and Bob can obtain in a "prepare and measure" setup is the same as when those they can obtain from making measurements on joint states then bit commitment is impossible
- Strong version: In all other theories there is a secure bit commitment protocol.

Note:

- Applies to C^*-theories, i.e. classical and quantum, due to Choi-Jamiołkowski isomorphism, but it's weaker than this.
- But not unentangled nonclassical theories.
- Implies some sort of isomorphism between $\otimes$ and $\mathcal{D}_{B|A}$.

Conjecture

- Weak version: If the set of joint probabilities that Alice and Bob can obtain in a "prepare and measure" setup is the same as when those they can obtain from making measurements on joint states then bit commitment is impossible
- Strong version: In all other theories there is a secure bit commitment protocol.

Note:

- Applies to C^*-theories, i.e. classical and quantum, due to Choi-Jamiołkowski isomorphism, but it's weaker than this.
- But not unentangled nonclassical theories.
- Implies some sort of isomorphism between $\otimes$ and $\mathcal{D}_{B|A}$.

Conjecture

- Weak version: If the set of joint probabilities that Alice and Bob can obtain in a "prepare and measure" setup is the same as when those they can obtain from making measurements on joint states then bit commitment is impossible
- Strong version: In all other theories there is a secure bit commitment protocol.

Note:

- Applies to C^*-theories, i.e. classical and quantum, due to Choi-Jamiołkowski isomorphism, but it's weaker than this.
- But not unentangled nonclassical theories.
- Implies some sort of isomorphism between $\otimes$ and $\mathcal{D}_{B|A}$.

Conjecture

- Weak version: If the set of joint probabilities that Alice and Bob can obtain in a "prepare and measure" setup is the same as when those they can obtain from making measurements on joint states then bit commitment is impossible
- Strong version: In all other theories there is a secure bit commitment protocol.

Note:

- Applies to C^*-theories, i.e. classical and quantum, due to Choi-Jamiołkowski isomorphism, but it's weaker than this.
- But not unentangled nonclassical theories.
- Implies some sort of isomorphism between $\otimes$ and $\mathcal{D}_{B|A}$.

Conjecture

- Weak version: If the set of joint probabilities that Alice and Bob can obtain in a "prepare and measure" setup is the same as when those they can obtain from making measurements on joint states then bit commitment is impossible
- Strong version: In all other theories there is a secure bit commitment protocol.

Note:

- Applies to C^*-theories, i.e. classical and quantum, due to Choi-Jamiołkowski isomorphism, but it's weaker than this.
- But not unentangled nonclassical theories.
- Implies some sort of isomorphism between $\otimes$ and $\mathfrak{D}_{B|A}$.

Acknowledgments

- This work is supported by:
  - The Foundational Questions Institute (http://www.fqxi.org)
  - MITACS (http://www.mitacs.math.ca)
  - NSERC (http://nserc.ca/)
  - The Province of Ontario: ORDCF/MRI

References

- H. Barnum, O. Dahlsten, M. Leifer and B. Toner, “Nonclassicality without entanglement enables bit commitment”, arXiv soon.
- H. Barnum, J. Barrett, M. Leifer and A. Wilce, “Generalized No Broadcasting Theorem”, arXiv:0707.0620.
- H. Barnum, J. Barrett, M. Leifer and A. Wilce, “Cloning and Broadcasting in Generic Probabilistic Theories”, quant-ph/0611295.