Title: Separations of generalized probabilistic theories via their information processing capabilities

Date: Jun 04, 2007 11:30 AM

URL: http://pirsa.org/07060033

Abstract:

Separations of probabilistic theories via their information processing capabilities

H. Barnum[1] J. Barrett[2] M. Leifer[2,3] A. Wilce[4]

[1]Los Alamos National Laboratory

[2]Perimeter Institute

[3]Institute for Quantum Computing
University of Waterloo

[4]Susquehanna University

June 4th 2007 / OQPQCC Workshop

Separations of probabilistic theories via their information processing capabilities

H. Barnum[1] J. Barrett[2] M. Leifer[2,3] A. Wilce[4]

[1]Los Alamos National Laboratory

[2]Perimeter Institute

[3]Institute for Quantum Computing
University of Waterloo

[4]Susquehanna University

June 4th 2007 / OQPQCC Workshop

Outline

1. Introduction
2. Review of Convex Sets Framework
3. Cloning and Broadcasting
4. The de Finetti Theorem
5. Teleportation
6. Conclusions

Why Study Info. Processing in GPTs?

- Axiomatics for Quantum Theory.
- What is responsible for enhanced info processing power of Quantum Theory?
- Security paranoia.
- Understand logical structure of information processing tasks.

Why Study Info. Processing in GPTs?

- Axiomatics for Quantum Theory.
- What is responsible for enhanced info processing power of Quantum Theory?
- Security paranoia.
- Understand logical structure of information processing tasks.

Why Study Info. Processing in GPTs?

- Axiomatics for Quantum Theory.
- What is responsible for enhanced info processing power of Quantum Theory?
- Security paranoia.
- Understand logical structure of information processing tasks.

Why Study Info. Processing in GPTs?

- Axiomatics for Quantum Theory.
- What is responsible for enhanced info processing power of Quantum Theory?
- Security paranoia.
- Understand logical structure of information processing tasks.

Examples

- Security of QKD can be proved based on...
  - Monogamy of entanglement.
  - The "uncertainty principle".
  - Violation of Bell inequalities.
- Informal arguments in QI literature:
  - Cloneability ⇔ Distinguishability.
  - Monogamy of entanglement ⇔ No-broadcasting.

These ideas do not seems to require the full machinery of Hilbert space QM.

Examples

- Security of QKD can be proved based on...
  - Monogamy of entanglement.
  - The "uncertainty principle".
  - Violation of Bell inequalities.
- Informal arguments in QI literature:
  - Cloneability $\Leftrightarrow$ Distinguishability.
  - Monogamy of entanglement $\Leftrightarrow$ No-broadcasting.

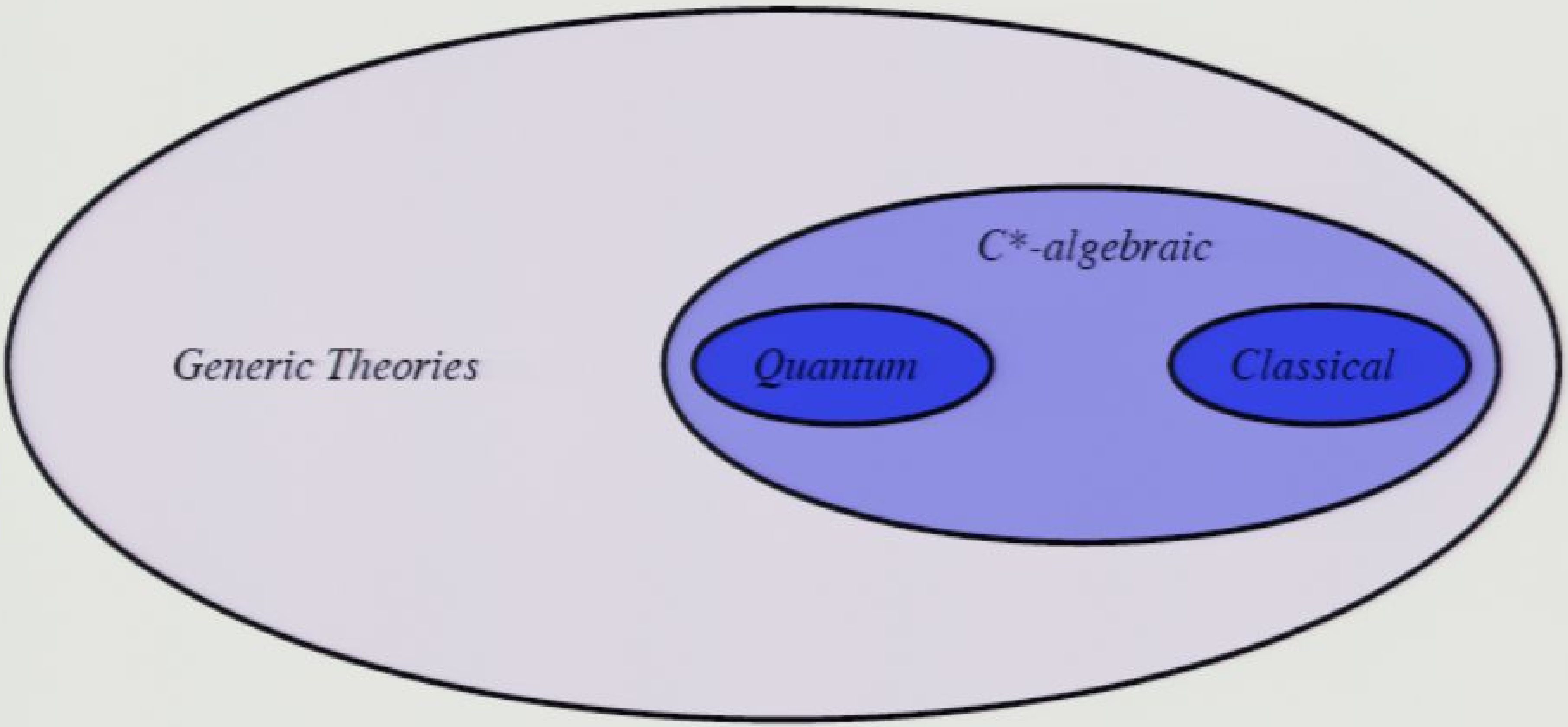
These ideas do not seems to require the full machinery of Hilbert space QM.

Examples

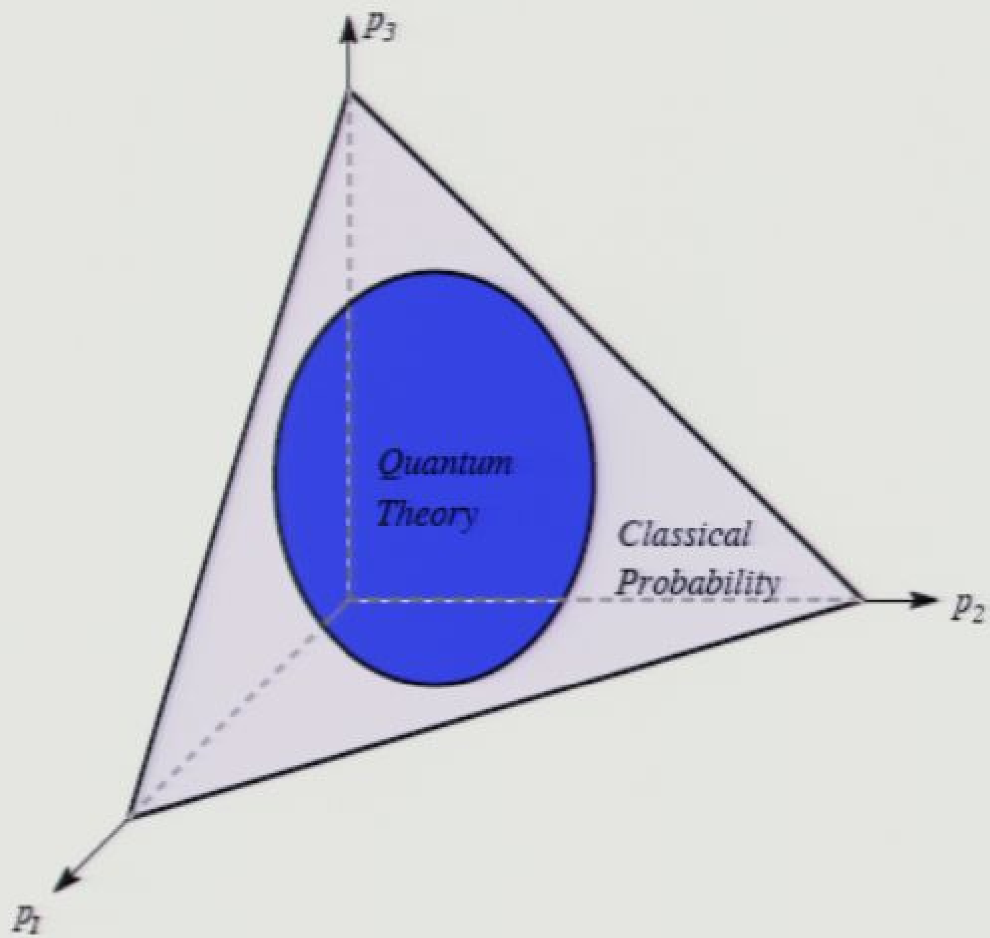
- Security of QKD can be proved based on...
  - Monogamy of entanglement.
  - The "uncertainty principle".
  - Violation of Bell inequalities.
- Informal arguments in QI literature:
  - Cloneability $\Leftrightarrow$ Distinguishability.
  - Monogamy of entanglement $\Leftrightarrow$ No-broadcasting.

These ideas do not seems to require the full machinery of Hilbert space QM.

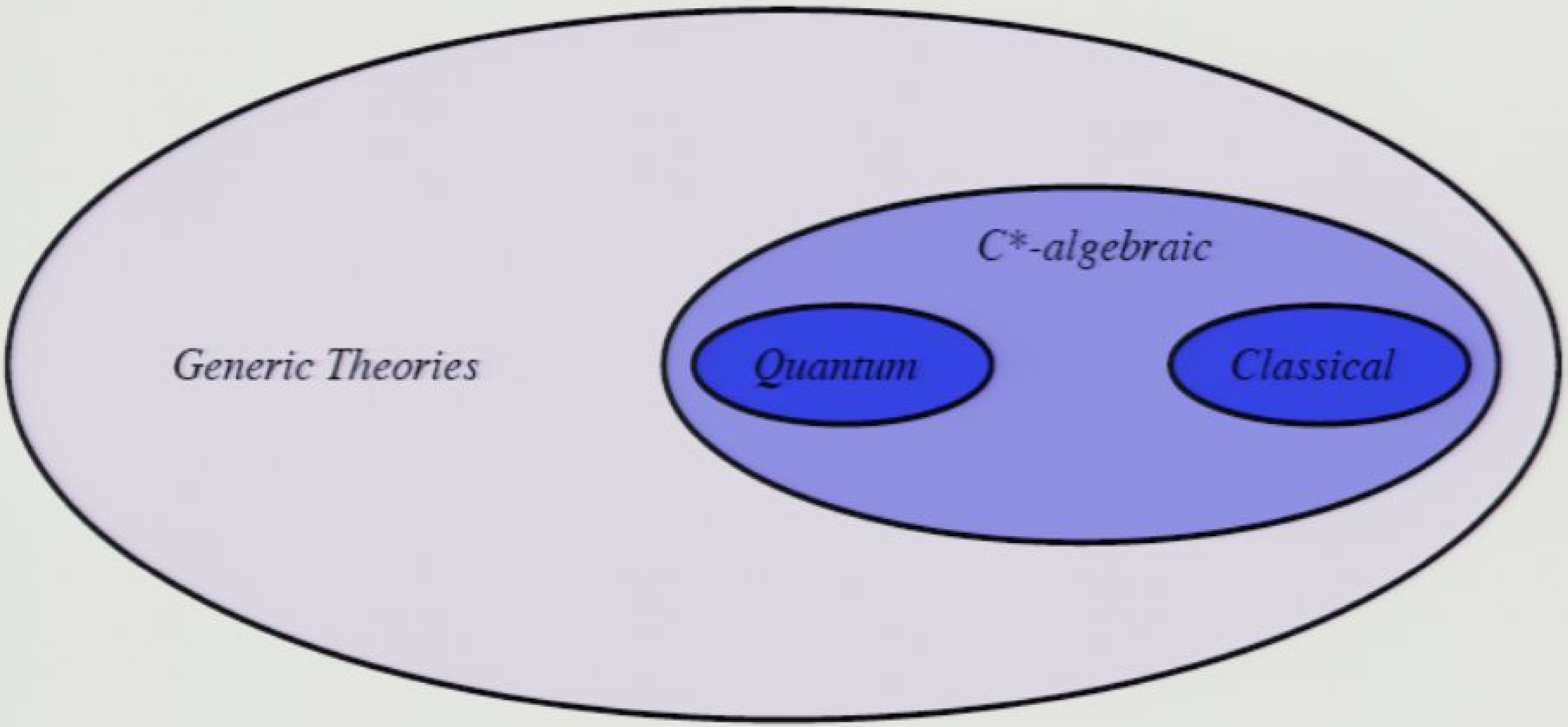
Generalized Probabilistic Frameworks



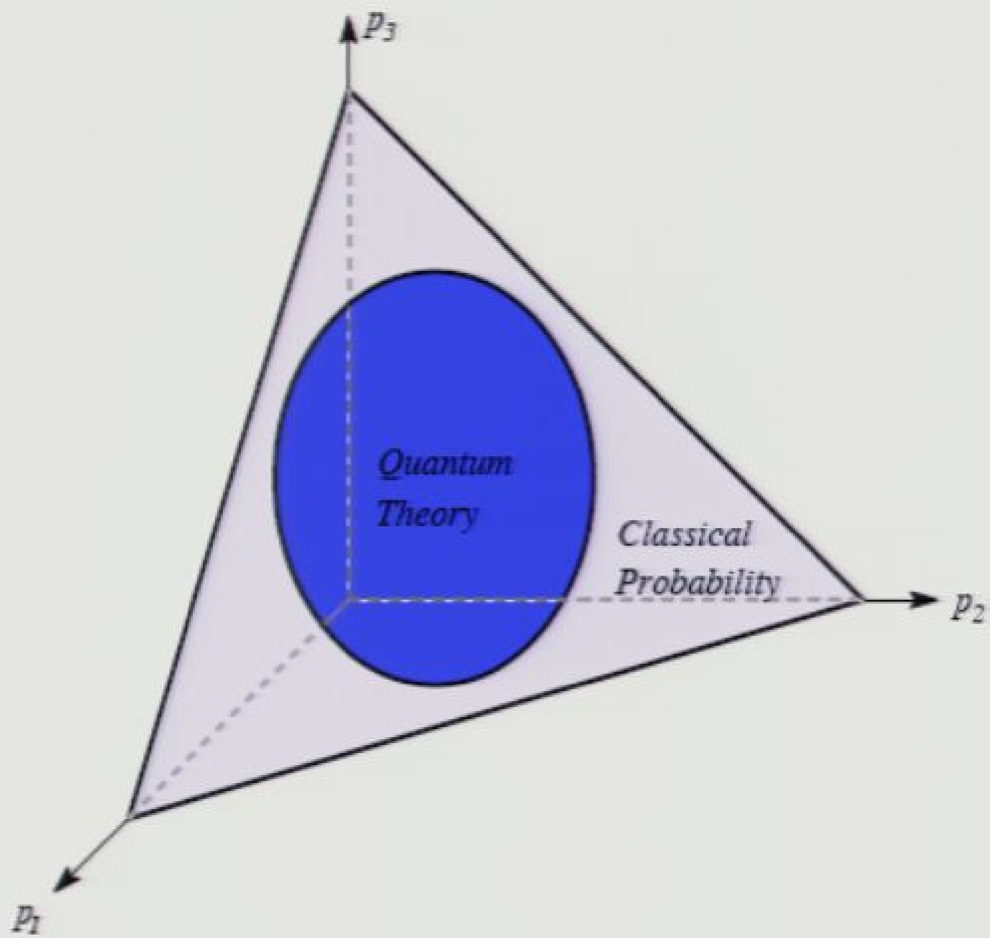
Specialized Probabilistic Frameworks



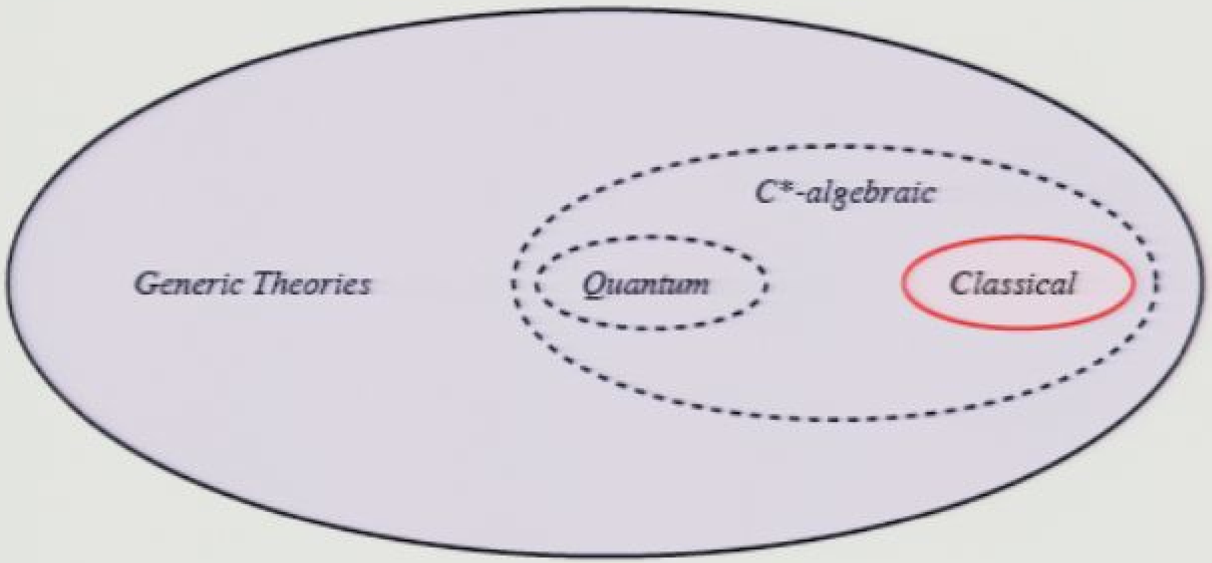
Generalized Probabilistic Frameworks



Specialized Probabilistic Frameworks

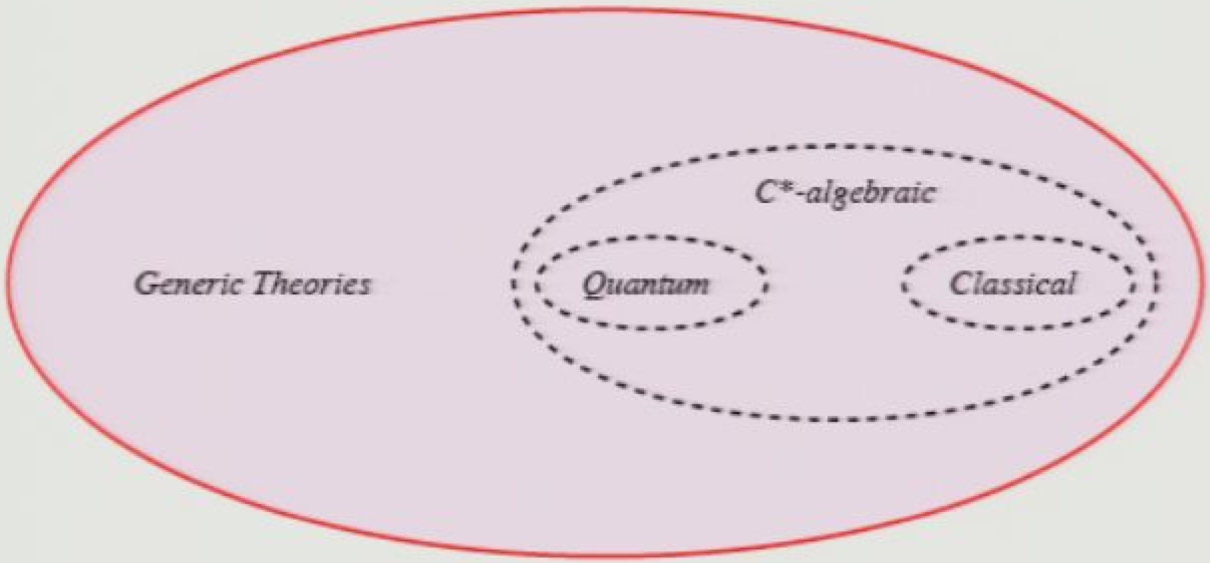


Types of Separation



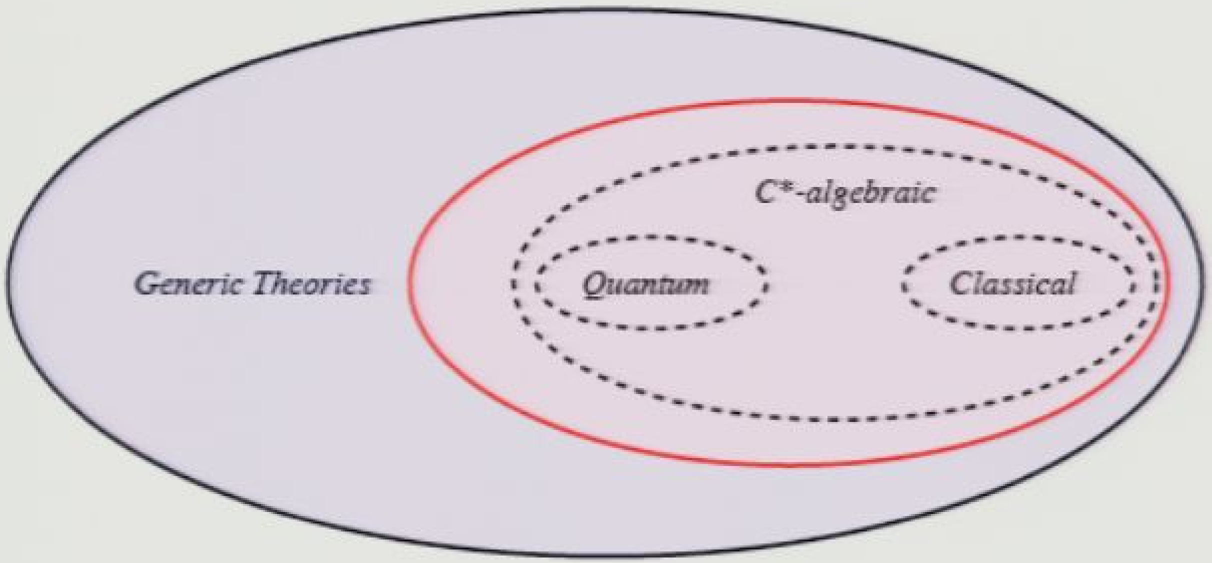
- Classical vs. Nonclassical, e.g. cloning and broadcasting.
- All Theories, e.g. de Finetti theorem.
- Nontrivial, e.g. teleportation.

Types of Separation



- Classical vs. Nonclassical, e.g. cloning and broadcasting.
- All Theories, e.g. de Finetti theorem.
- Nontrivial, e.g. teleportation.

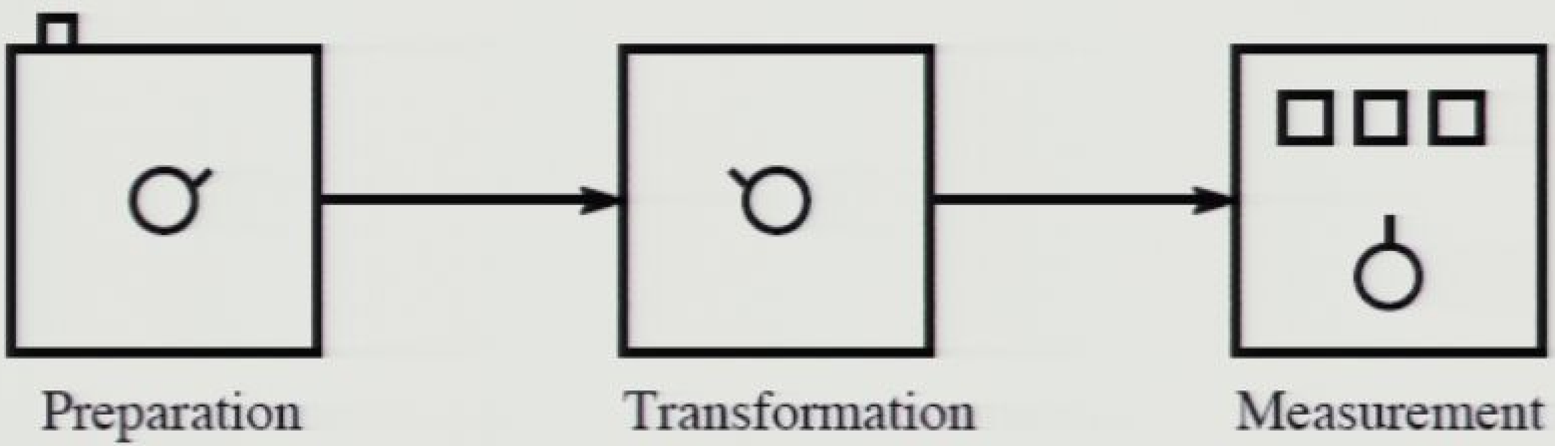
Types of Separation



- Classical vs. Nonclassical, e.g. cloning and broadcasting.
- All Theories, e.g. de Finetti theorem.
- Nontrivial, e.g. teleportation.

Review of the Convex Sets Framework

- A traditional operational framework.



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

State Space

Definition

The set V of unnormalized states is a compact, closed, convex cone.

- Convex: If $\mathrm{u}, \mathrm{v} \in \mathrm{V}$ and $\alpha, \beta \geq 0$ then $\alpha\mathrm{u} + \beta\mathrm{v} \in \mathrm{V}$.
- Finite dim $\Rightarrow$ Can be embedded in $\mathbb{R}^n$.
- Define a (closed, convex) section of normalized states Ω.
- Every $\mathrm{v} \in \mathrm{V}$ can be written uniquely as $\mathrm{v} = \alpha\omega$ for some $\omega \in \Omega, \alpha \geq 0$.
- Extreme points of Ω/Extremal rays of V are pure states.

State Space

Definition

The set V of unnormalized states is a compact, closed, convex cone.

- Convex: If $\mathrm{u}, \mathrm{v} \in \mathrm{V}$ and $\alpha, \beta \geq 0$ then $\alpha \mathrm{u} + \beta \mathrm{v} \in \mathrm{V}$.
- Finite dim $\Rightarrow$ Can be embedded in $\mathbb{R}^{\mathrm{n}}$.
- Define a (closed, convex) section of normalized states Ω.
- Every $\mathrm{v} \in \mathrm{V}$ can be written uniquely as $\mathrm{v} = \alpha\omega$ for some $\omega \in \Omega, \alpha \geq 0$.
- Extreme points of Ω/Extremal rays of V are pure states.

State Space

Definition

The set V of unnormalized states is a compact, closed, convex cone.

- Convex: If $u, v \in V$ and $\alpha, \beta \geq 0$ then $\alpha u + \beta v \in V$.
- Finite dim $\Rightarrow$ Can be embedded in $\mathbb{R}^n$.
- Define a (closed, convex) section of normalized states Ω.
- Every $v \in V$ can be written uniquely as $v = \alpha\omega$ for some $\omega \in \Omega, \alpha \geq 0$.
- Extreme points of Ω/Extremal rays of V are pure states.

State Space

Definition

The set V of unnormalized states is a compact, closed, convex cone.

- Convex: If $\mathrm{u}, \mathrm{v} \in \mathrm{V}$ and $\alpha, \beta \geq 0$ then $\alpha \mathrm{u} + \beta \mathrm{v} \in \mathrm{V}$.
- Finite dim $\Rightarrow$ Can be embedded in $\mathbb{R}^{\mathrm{n}}$.
- Define a (closed, convex) section of normalized states Ω.
- Every $\mathrm{v} \in \mathrm{V}$ can be written uniquely as $\mathrm{v} = \alpha\omega$ for some $\omega \in \Omega, \alpha \geq 0$.
- Extreme points of Ω/Extremal rays of V are pure states.

State Space

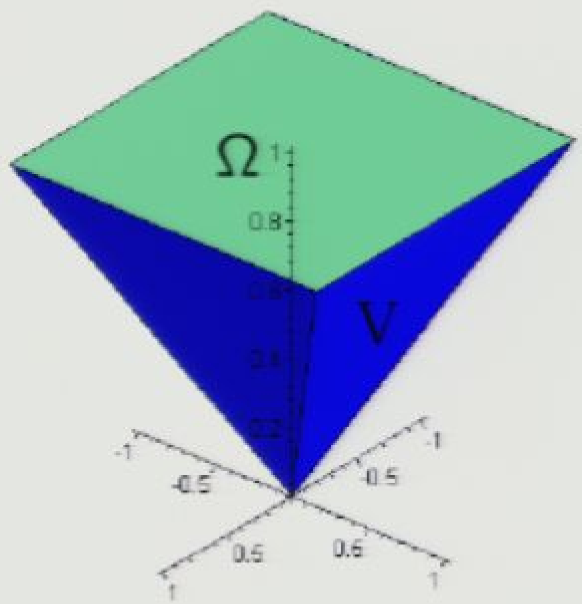
Definition

The set V of unnormalized states is a compact, closed, convex cone.

- Convex: If $\mathrm{u}, \mathrm{v} \in \mathrm{V}$ and $\alpha, \beta \geq 0$ then $\alpha \mathrm{u} + \beta \mathrm{v} \in \mathrm{V}$.
- Finite dim $\Rightarrow$ Can be embedded in $\mathbb{R}^{\mathrm{n}}$.
- Define a (closed, convex) section of normalized states Ω.
- Every $\mathrm{v} \in \mathrm{V}$ can be written uniquely as $\mathrm{v} = \alpha\omega$ for some $\omega \in \Omega, \alpha \geq 0$.
- Extreme points of Ω/Extremal rays of V are pure states.

Examples

- Classical: $\Omega =$ Probability simplex, $V = \text{conv}\{\Omega, 0\}$.
- Quantum:
  $V = \{\text{Semi-} + \text{ve matrices}\}$, $\Omega = \{\text{Denisty matrices }\}$.
- Polyhedral:



Effects

Definition

The dual cone V^* is the set of positive affine functionals on V.

$$V^* = \{f : V \to \mathbb{R} | \forall v \in V, \; f(v) \geq 0\}$$

$$\forall \alpha, \beta \geq 0, \; f(\alpha u + \beta v) = \alpha f(u) + \beta f(v)$$

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

Effects

Definition

The dual cone V^* is the set of positive affine functionals on V.

$$V^* = \{f : V \to \mathbb{R} | \forall v \in V,\ f(v) \geq 0\}$$

$$\forall \alpha, \beta \geq 0,\ f(\alpha u + \beta v) = \alpha f(u) + \beta f(v)$$

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

Effects

Definition

The dual cone V^* is the set of positive affine functionals on V.

$$V^* = \{f : V \to \mathbb{R} | \forall v \in V,\ f(v) \geq 0\}$$

$$\forall \alpha, \beta \geq 0,\ f(\alpha u + \beta v) = \alpha f(u) + \beta f(v)$$

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

Effects

Definition

The dual cone V^* is the set of positive affine functionals on V.

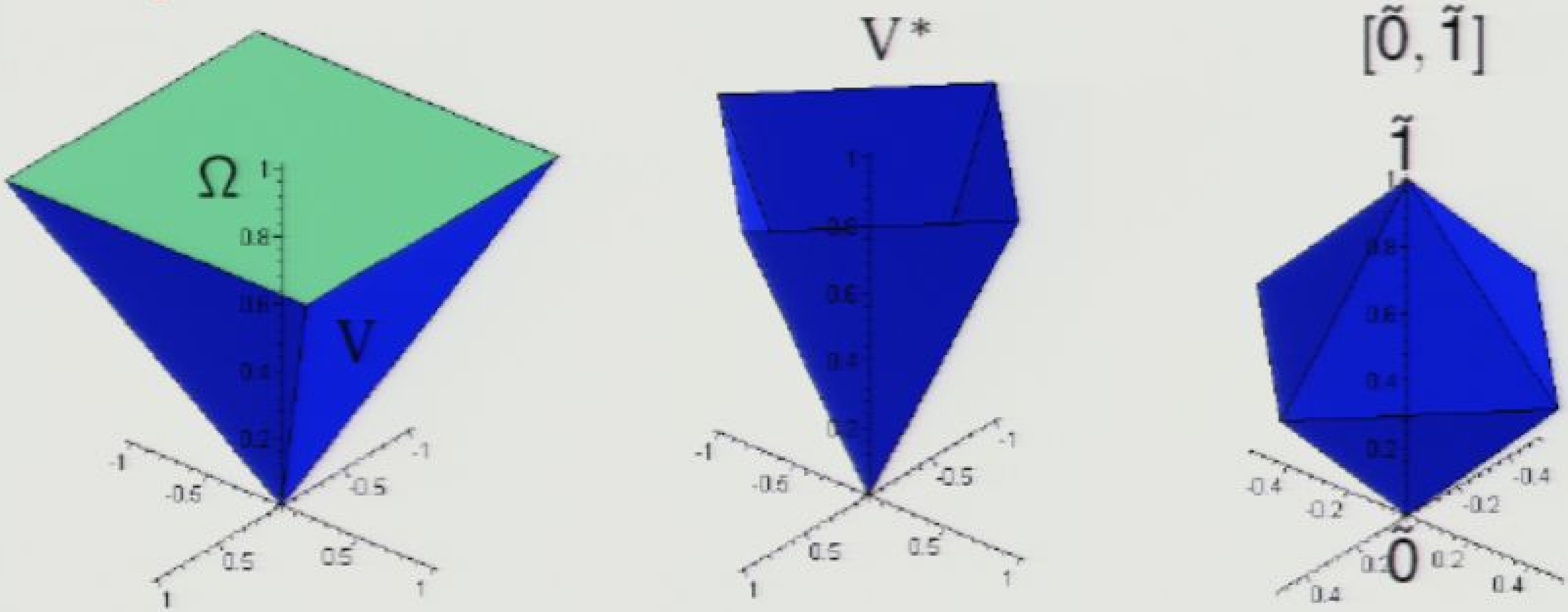
$$V^* = \{f : V \to \mathbb{R} | \forall v \in V,\ f(v) \geq 0\}$$

$$\forall \alpha, \beta \geq 0,\ f(\alpha u + \beta v) = \alpha f(u) + \beta f(v)$$

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

Examples

- Classical: $[\tilde{0}, \tilde{1}] = \{$Fuzzy indicator functions$\}$.
- Quantum: $[\tilde{0}, \tilde{1}] \cong \{$POVM elements$\}$ via $f(\rho) = \mathrm{Tr}(E_f \rho)$.
- 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 $\sum_{j=1}^{N} f_j = u$.

- 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 $\sum_{j=1}^{N} f_j = u$.

- 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 $\sum_{j=1}^{N} f_j = u$.

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

Informationally Complete Observables

- An observable $(f_1, f_2, \ldots, f_N)$ induces an affine map:

$$\psi_f : \Omega \to \Delta_N \qquad \psi_f(\omega)_j = f_j(\omega).$$

Definition

An observable $(f_1, f_2, \ldots, f_N)$ is informationally complete if

$$\forall \omega, \mu \in \Omega, \ \psi_f(\omega) \neq \psi_f(\mu).$$

Lemma

Every state space has an informationally complete observable.

Informationally Complete Observables

- An observable $(f_1, f_2, \ldots, f_N)$ induces an affine map:

$$\psi_f : \Omega \to \Delta_N \qquad \psi_f(\omega)_j = f_j(\omega).$$

Definition

An observable $(f_1, f_2, \ldots, f_N)$ is informationally complete if

$$\forall \omega, \mu \in \Omega,\ \psi_f(\omega) \neq \psi_f(\mu).$$

Lemma

Every state space has an informationally complete observable.

Informationally Complete Observables

- An observable $(f_1, f_2, \ldots, f_N)$ induces an affine map:

$$\psi_f : \Omega \to \Delta_N \qquad \psi_f(\omega)_j = f_j(\omega).$$

Definition

An observable $(f_1, f_2, \ldots, f_N)$ is informationally complete if

$$\forall \omega, \mu \in \Omega,\ \psi_f(\omega) \neq \psi_f(\mu).$$

Lemma

Every state space has an informationally complete observable.

Tensor Products

Definition

Separable TP: $V_A \otimes_{\mathrm{sep}} V_B = \mathrm{conv}\left\{ v_A \otimes v_B | v_A \in V_A,\ v_B \in V_B \right\}$

Definition

Maximal TP: $V_A \otimes_{\max} V_B = \left(V_A^* \otimes_{\mathrm{sep}} V_B^* \right)^*$

Definition

A tensor product $V_A \otimes V_B$ is a convex cone that satisfies

$$V_A \otimes_{\mathrm{sep}} V_B \subseteq V_A \otimes V_B \subseteq V_A \otimes_{\max} V_B.$$

Tensor Products

Definition

Separable TP: $V_A \otimes_{sep} V_B = \text{conv}\{v_A \otimes v_B | v_A \in V_A,\ v_B \in V_B\}$

Definition

Maximal TP: $V_A \otimes_{max} V_B = (V_A^* \otimes_{sep} V_B^*)^*$

Definition

A tensor product $V_A \otimes V_B$ is a convex cone that satisfies

$$V_A \otimes_{sep} V_B \subseteq V_A \otimes V_B \subseteq V_A \otimes_{max} V_B.$$

Tensor Products

Definition

Separable TP: $V_A \otimes_{sep} V_B = \text{conv}\{v_A \otimes v_B | v_A \in V_A,\ v_B \in V_B\}$

Definition

Maximal TP: $V_A \otimes_{max} V_B = \left(V_A^* \otimes_{sep} V_B^*\right)^*$

Definition

A **tensor product** $V_A \otimes V_B$ is a convex cone that satisfies

$$V_A \otimes_{sep} V_B \subseteq V_A \otimes V_B \subseteq V_A \otimes_{max} V_B.$$

Dynamics

Definition

The dynamical maps $\mathfrak{D}_{B|A}$ are a convex subset of the affine maps $\phi : V_A \to V_B$.

$$\forall \alpha, \beta \geq 0, \ \phi(\alpha u_A + \beta v_A) = \alpha\phi(u_A) + \beta\phi(v_A)$$

- Dual map: $\phi^* : V_B^* \to V_A^*$ $\quad [\phi^*(f_B)](v_A) = f_B(\phi(v_A))$
- Normalization preserving affine (NPA) maps: $\phi^*(\tilde{1}_B) = \tilde{1}_A$.
- Require: $\forall f \in V_A^*, v_B \in V_B$, $\phi(v_A) = f(v_A)v_B$ is in $\mathfrak{D}_{B|A}$.

Dynamics

Definition

The dynamical maps $\mathfrak{D}_{B|A}$ are a convex subset of the affine maps $\phi : V_A \rightarrow V_B$.

$$\forall \alpha, \beta \geq 0,\ \phi(\alpha u_A + \beta v_A) = \alpha\phi(u_A) + \beta\phi(v_A)$$

- Dual map: $\phi^* : V_B^* \rightarrow V_A^*$ $\quad [\phi^*(f_B)](v_A) = f_B(\phi(v_A))$
- Normalization preserving affine (NPA) maps: $\phi^*(\tilde{1}_B) = \tilde{1}_A$.
- Require: $\forall f \in V_A^*, v_B \in V_B$, $\phi(v_A) = f(v_A)v_B$ is in $\mathfrak{D}_{B|A}$.

Dynamics

Definition

The dynamical maps $\mathfrak{D}_{B|A}$ are a convex subset of the affine maps $\phi : V_A \to V_B$.

$$\forall \alpha, \beta \geq 0, \ \phi(\alpha u_A + \beta v_A) = \alpha\phi(u_A) + \beta\phi(v_A)$$

- Dual map: $\phi^* : V_B^* \to V_A^*$ $\quad [\phi^*(f_B)](v_A) = f_B(\phi(v_A))$
- Normalization preserving affine (NPA) maps: $\phi^*(\tilde{1}_B) = \tilde{1}_A$.
- Require: $\forall f \in V_A^*, v_B \in V_B, \ \phi(v_A) = f(v_A)v_B$ is in $\mathfrak{D}_{B|A}$.

Dynamics

Definition

The dynamical maps $\mathfrak{D}_{\mathrm{B|A}}$ are a convex subset of the affine maps $\phi : \mathrm{V}_{\mathrm{A}} \rightarrow \mathrm{V}_{\mathrm{B}}$.

$$\forall \alpha, \beta \geq 0, \ \phi(\alpha \mathrm{u}_{\mathrm{A}} + \beta \mathrm{v}_{\mathrm{A}}) = \alpha\phi(\mathrm{u}_{\mathrm{A}}) + \beta\phi(\mathrm{v}_{\mathrm{A}})$$

- Dual map: $\phi^* : \mathrm{V}_{\mathrm{B}}^* \rightarrow \mathrm{V}_{\mathrm{A}}^*$ $\quad [\phi^*(\mathrm{f}_{\mathrm{B}})]\,(\mathrm{v}_{\mathrm{A}}) = \mathrm{f}_{\mathrm{B}}\,(\phi(\mathrm{v}_{\mathrm{A}}))$
- Normalization preserving affine (NPA) maps: $\phi^*(\tilde{1}_{\mathrm{B}}) = \tilde{1}_{\mathrm{A}}$.
- Require: $\forall \mathrm{f} \in \mathrm{V}_{\mathrm{A}}^*, \mathrm{v}_{\mathrm{B}} \in \mathrm{V}_{\mathrm{B}}, \ \phi(\mathrm{v}_{\mathrm{A}}) = \mathrm{f}(\mathrm{v}_{\mathrm{A}})\mathrm{v}_{\mathrm{B}}$ is in $\mathfrak{D}_{\mathrm{B|A}}$.

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.

Cloning

Definition

An NPA map $\phi : \mathrm{V} \to \mathrm{V} \otimes \mathrm{V}$ clones a state $\omega \in \Omega$ if $\phi(\omega) = \omega \otimes \omega$.

- Every state has a cloning map: $\phi(\mu) = \tilde{1}(\mu)\omega \otimes \omega = \omega \otimes \omega$.

Definition

A set of states $\{\omega_1, \omega_2, \ldots, \omega_N\}$ is co-cloneable if $\exists$ an affine map in $\mathfrak{D}$ that clones all of them.

Cloning

Definition

An NPA map $\phi : \mathrm{V} \to \mathrm{V} \otimes \mathrm{V}$ clones a state $\omega \in \Omega$ if $\phi(\omega) = \omega \otimes \omega$.

- Every state has a cloning map: $\phi(\mu) = \tilde{1}(\mu)\omega \otimes \omega = \omega \otimes \omega$.

Definition

A set of states $\{\omega_1, \omega_2, \ldots, \omega_N\}$ is co-cloneable if $\exists$ an affine map in $\mathfrak{D}$ that clones all of them.

Cloning

Definition

An NPA map $\phi : \mathrm{V} \to \mathrm{V} \otimes \mathrm{V}$ clones a state $\omega \in \Omega$ if $\phi(\omega) = \omega \otimes \omega$.

- Every state has a cloning map: $\phi(\mu) = \tilde{1}(\mu)\omega \otimes \omega = \omega \otimes \omega$.

Definition

A set of states $\{\omega_1, \omega_2, \ldots, \omega_\mathrm{N}\}$ is co-cloneable if $\exists$ an affine map in $\mathfrak{D}$ that clones all of them.

The No-Cloning Theorem

Theorem

A set of states is co-cloneable iff they are jointly distinguishable.

Proof.

- If J.D. then $\phi(\omega) = \sum_{j=1}^{N} f_j(\omega)\omega_j \otimes \omega_j$ is cloning.
- If co-cloneable then iterate cloning map and use IC observable to distinguish the states.

□

The No-Cloning Theorem

Theorem

A set of states is co-cloneable iff they are jointly distinguishable.

Proof.

- If J.D. then $\phi(\omega) = \sum_{j=1}^{N} f_j(\omega)\omega_j \otimes \omega_j$ is cloning.
- If co-cloneable then iterate cloning map and use IC observable to distinguish the states.

The No-Cloning Theorem

Theorem

A set of states is co-cloneable iff they are jointly distinguishable.

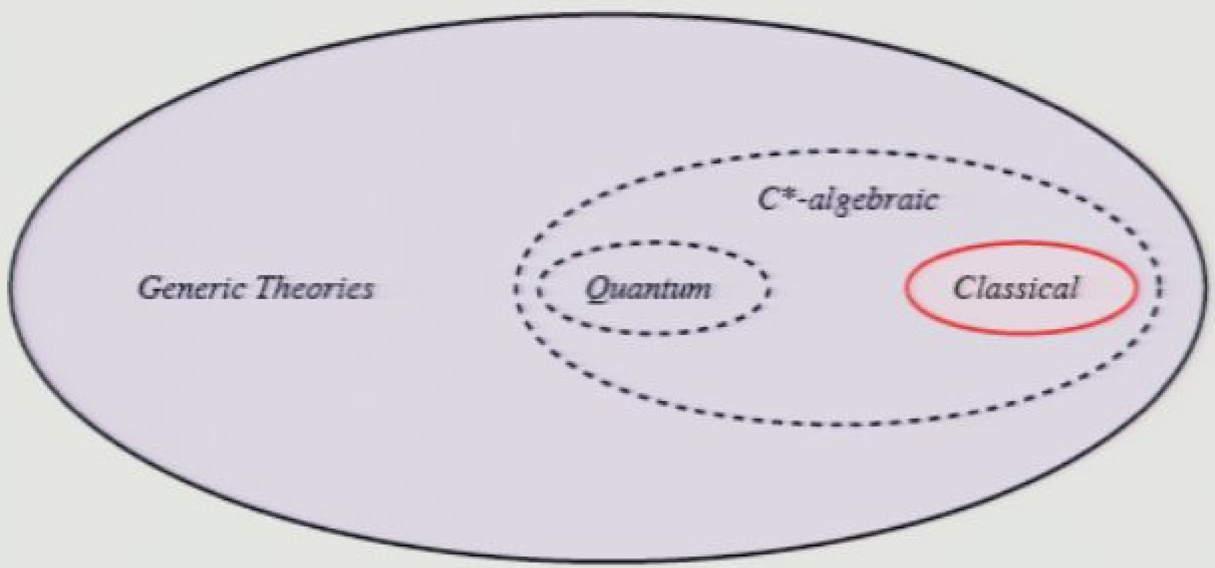
Proof.

- If J.D. then $\phi(\omega) = \sum_{j=1}^{N} f_j(\omega)\omega_j \otimes \omega_j$ is cloning.
- If co-cloneable then iterate cloning map and use IC observable to distinguish the states.

□

The No-Cloning Theorem

- Universal cloning of pure states is only possible in classical theory.



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 $\phi_{\mathrm{A'A''|A}} : \mathrm{V_A} \rightarrow \mathrm{V_{A'}} \otimes \mathrm{V_{A''}}$ if $\phi_{\mathrm{A'|A}}(\omega) = \phi_{\mathrm{A''|A}}(\omega) = \omega$.

- 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 $\phi_{A'A''|A} : V_A \rightarrow V_{A'} \otimes V_{A''}$ 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 $\phi_{\mathrm{A}'\mathrm{A}''|\mathrm{A}} : \mathrm{V}_\mathrm{A} \to \mathrm{V}_{\mathrm{A}'} \otimes \mathrm{V}_{\mathrm{A}''}$ if $\phi_{\mathrm{A}'|\mathrm{A}}(\omega) = \phi_{\mathrm{A}''|\mathrm{A}}(\omega) = \omega$.

- 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 $\phi_{A'A''|A} : V_A \rightarrow V_{A'} \otimes V_{A''}$ 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

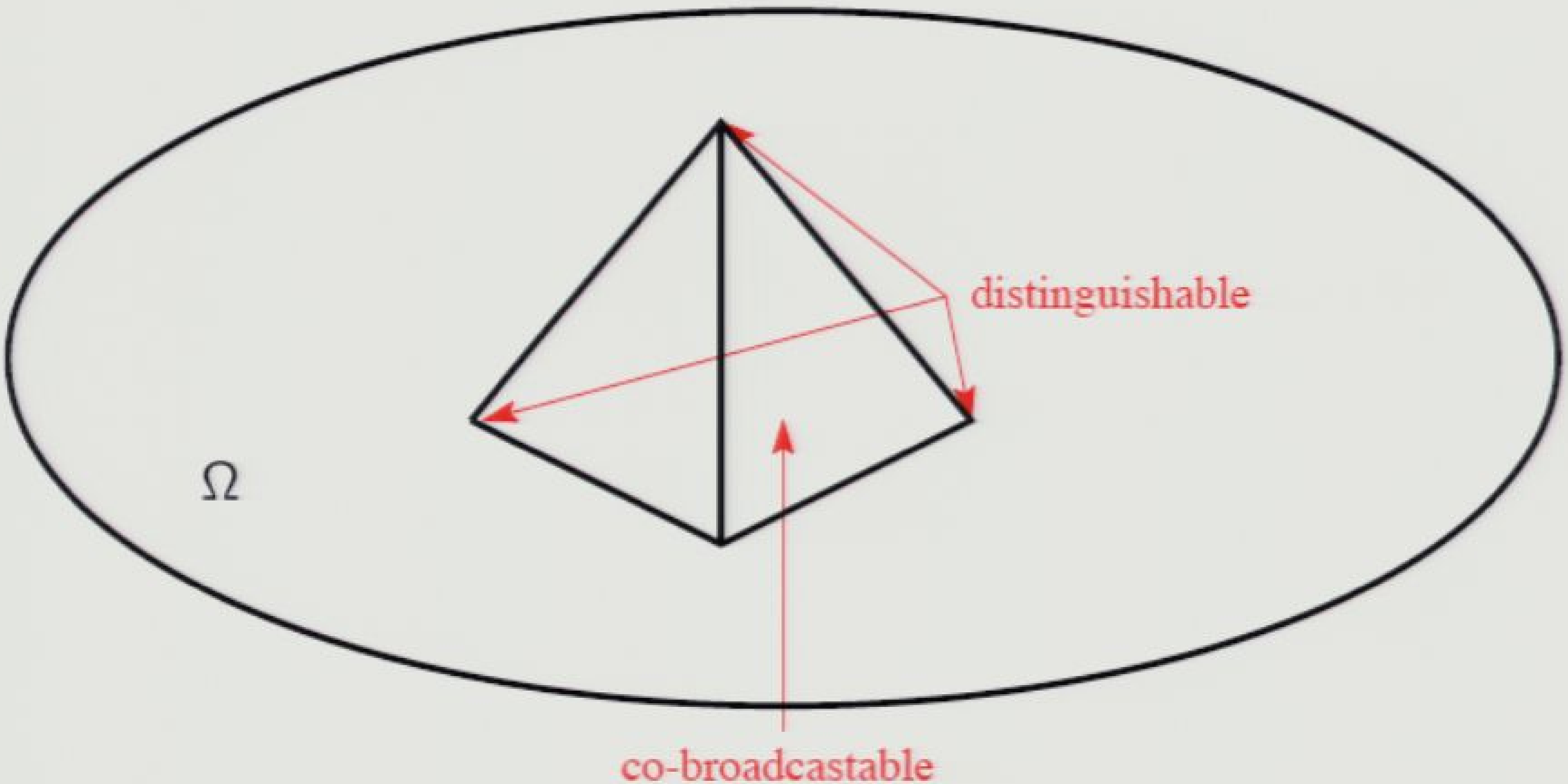
A set of states is co-broadcastable iff it is contained in a simplex that has jointly distinguishable vertices.

- 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



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

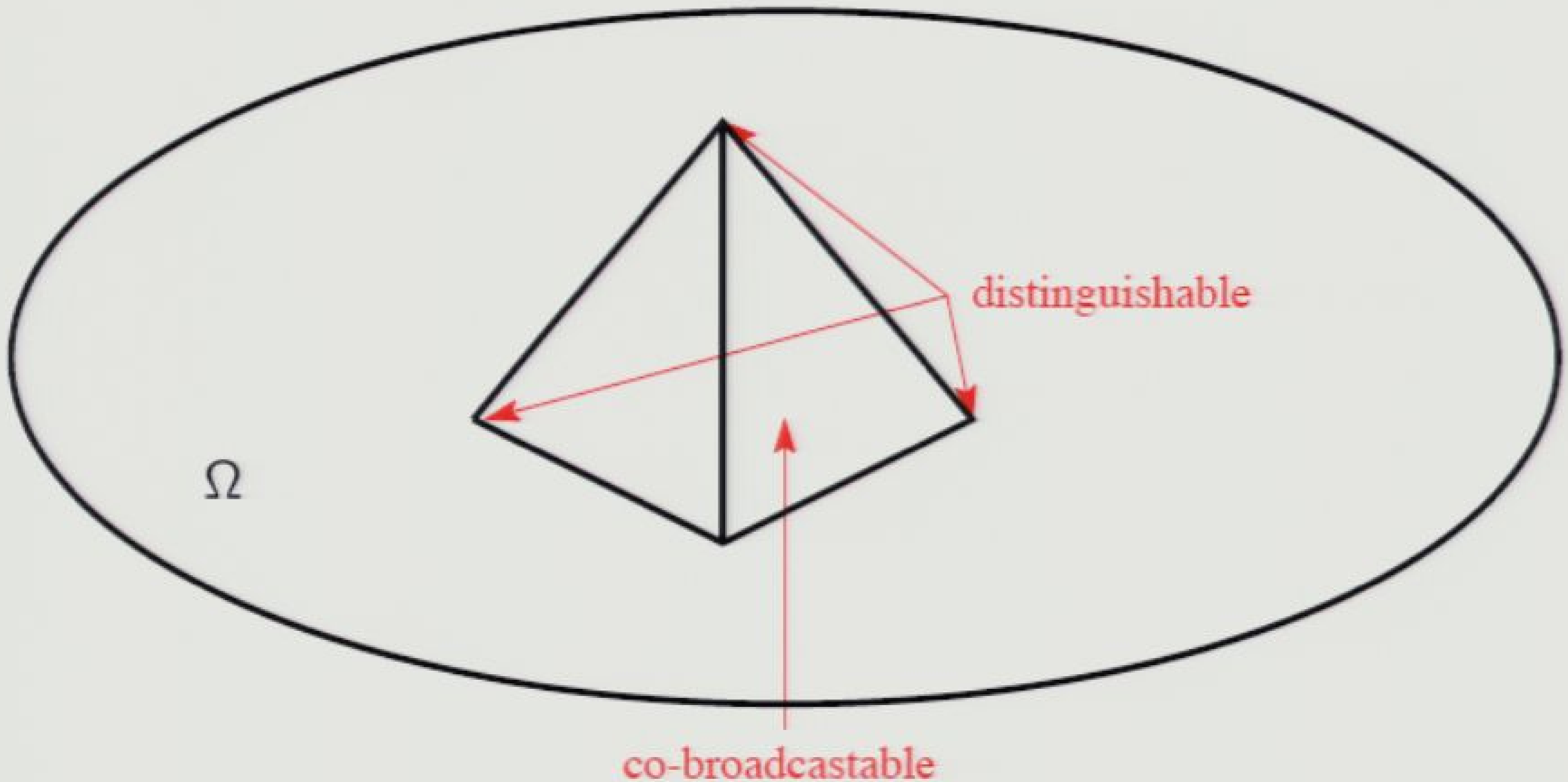
A set of states is co-broadcastable iff it is contained in a simplex that has jointly distinguishable vertices.

- 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



The No-Broadcasting Theorem

Theorem

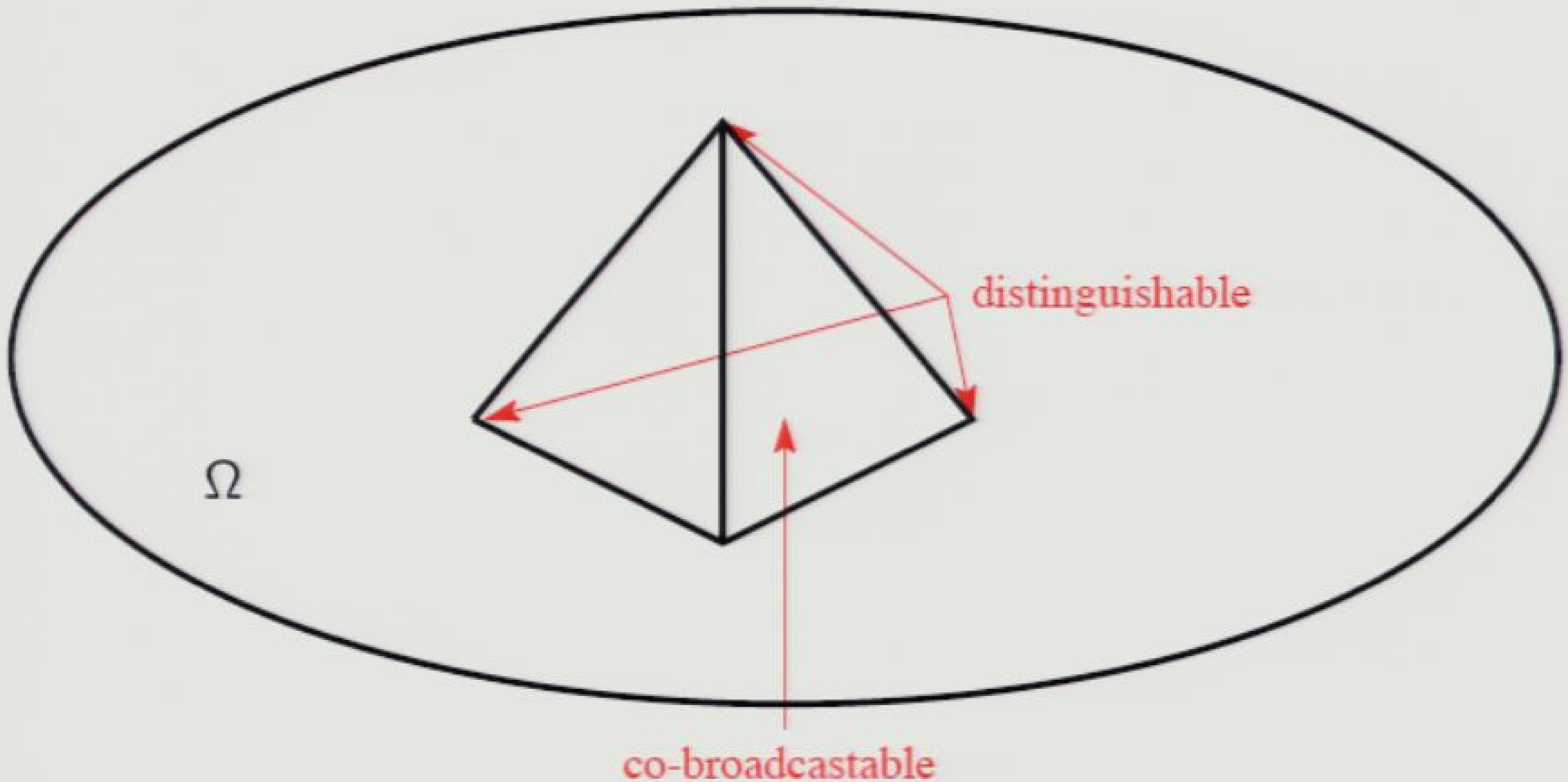
A set of states is co-broadcastable iff it is contained in a simplex that has jointly distinguishable vertices.

- 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



The de Finetti Theorem

- A structure theorem for symmetric classical probability distributions.
- In Bayesian Theory:
  - Enables an interpretation of "unknown probability".
  - Justifies use of relative frequencies in updating prob. assignments.
- Other applications, e.g. cryptography.

The de Finetti Theorem

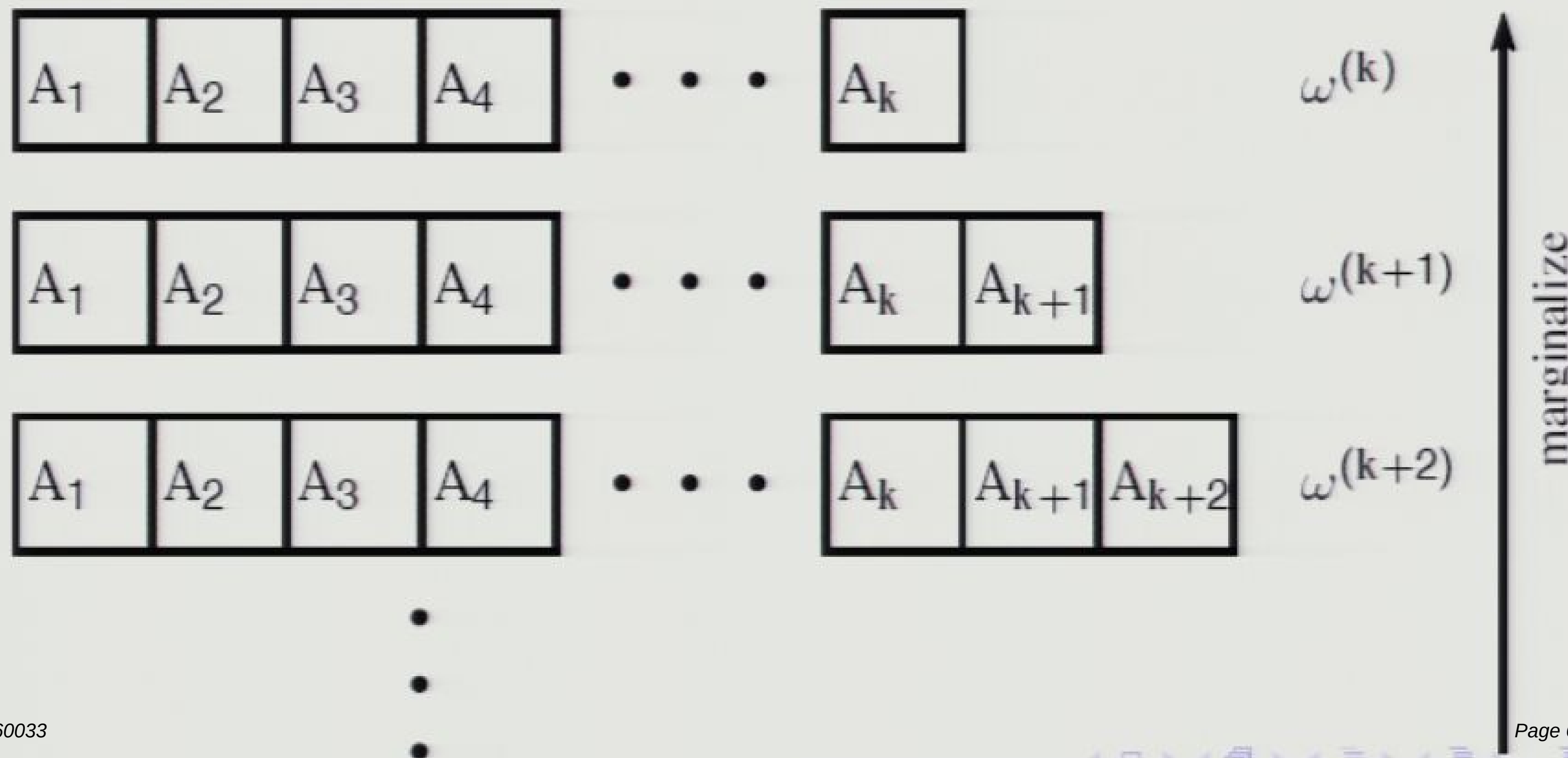
- A structure theorem for symmetric classical probability distributions.
- In Bayesian Theory:
  - Enables an interpretation of “unknown probability”.
  - Justifies use of relative frequencies in updating prob. assignments.
- Other applications, e.g. cryptography.

The de Finetti Theorem

- A structure theorem for symmetric classical probability distributions.
- In Bayesian Theory:
  - Enables an interpretation of "unknown probability".
  - Justifies use of relative frequencies in updating prob. assignments.
- Other applications, e.g. cryptography.

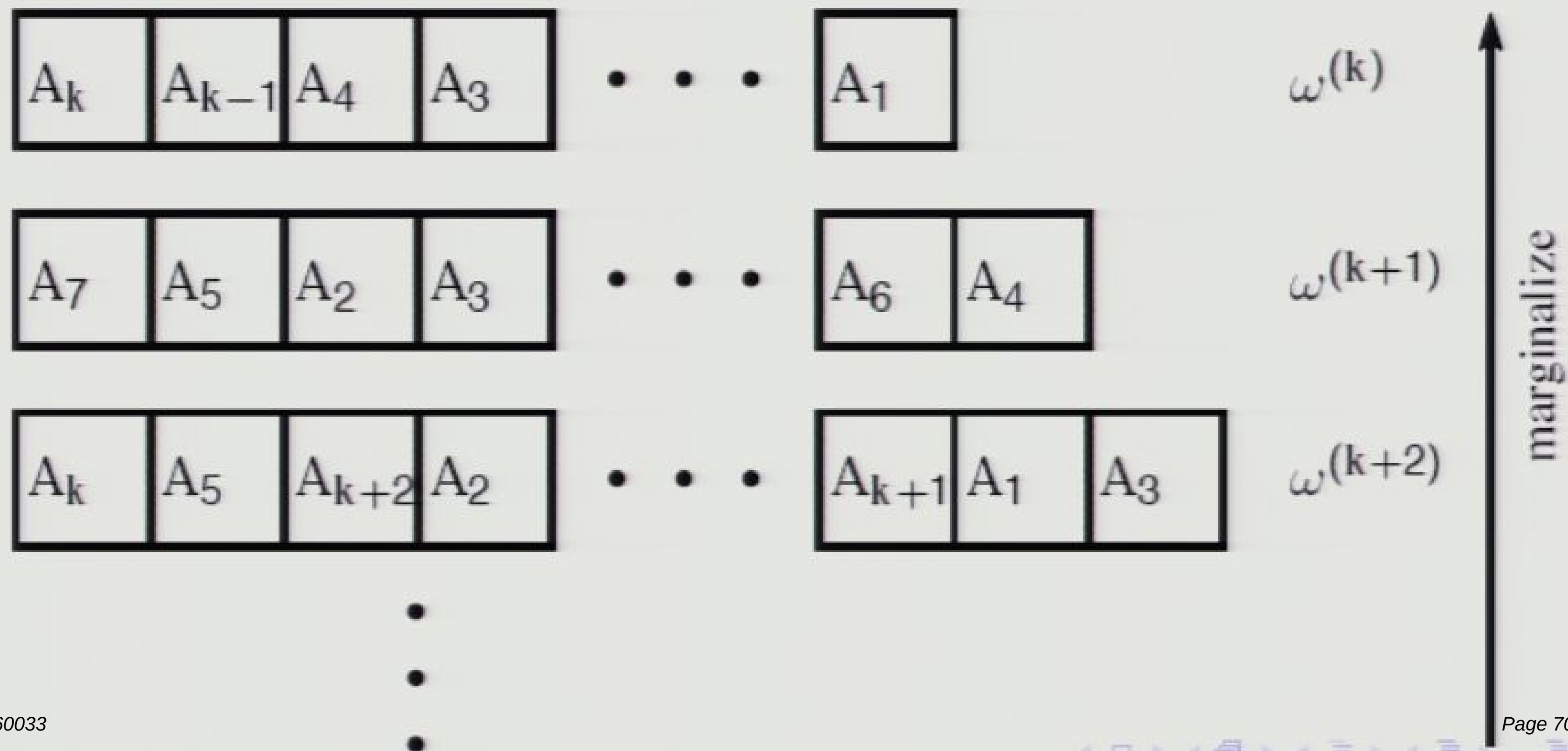
Exchangeability

- Let $\omega^{(k)} \in \Omega_{A_1} \otimes \Omega_{A_2} \otimes \ldots \otimes \Omega_{A_k}$.



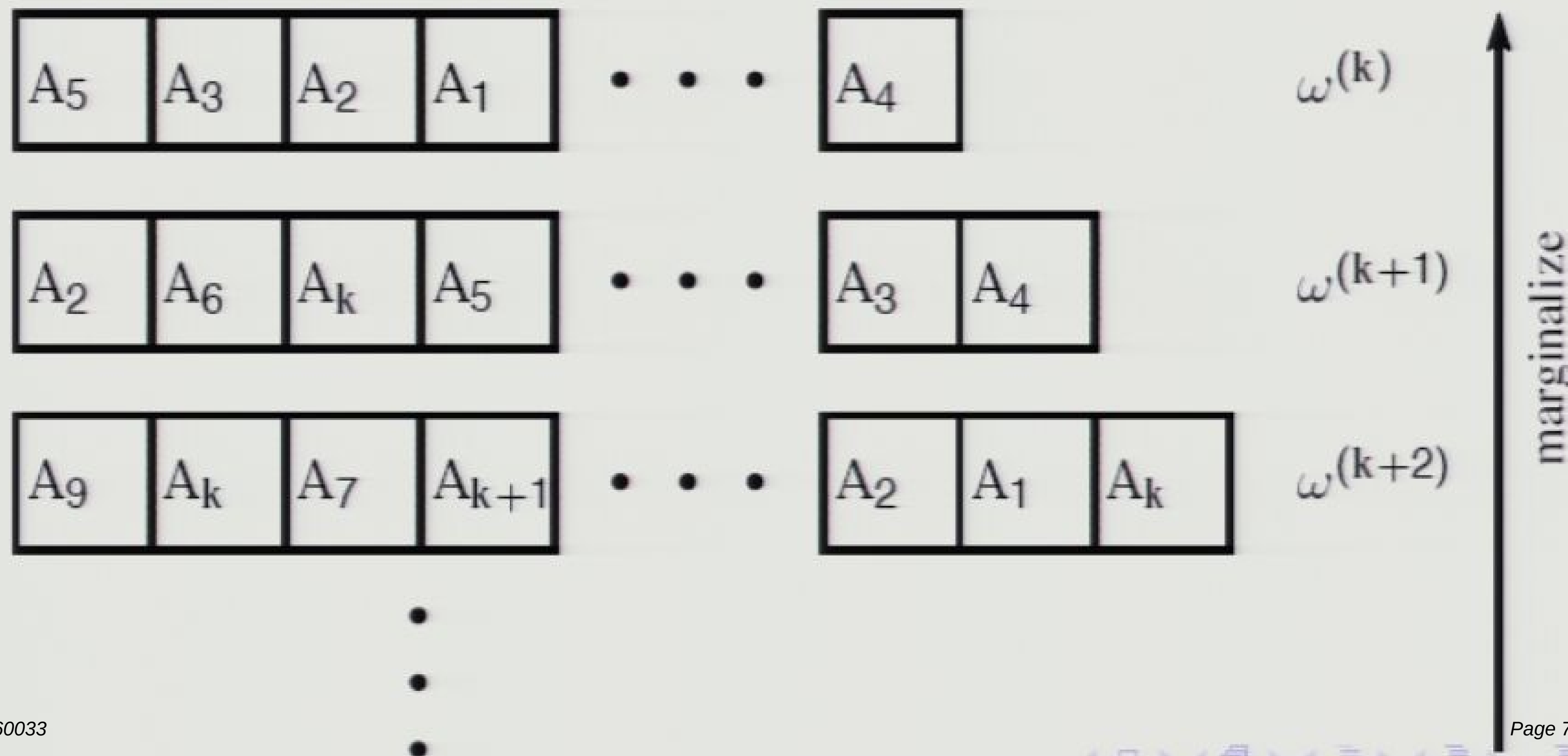
Exchangeability

- Let $\omega^{(k)} \in \Omega_{A_1} \otimes \Omega_{A_2} \otimes \ldots \otimes \Omega_{A_k}$.



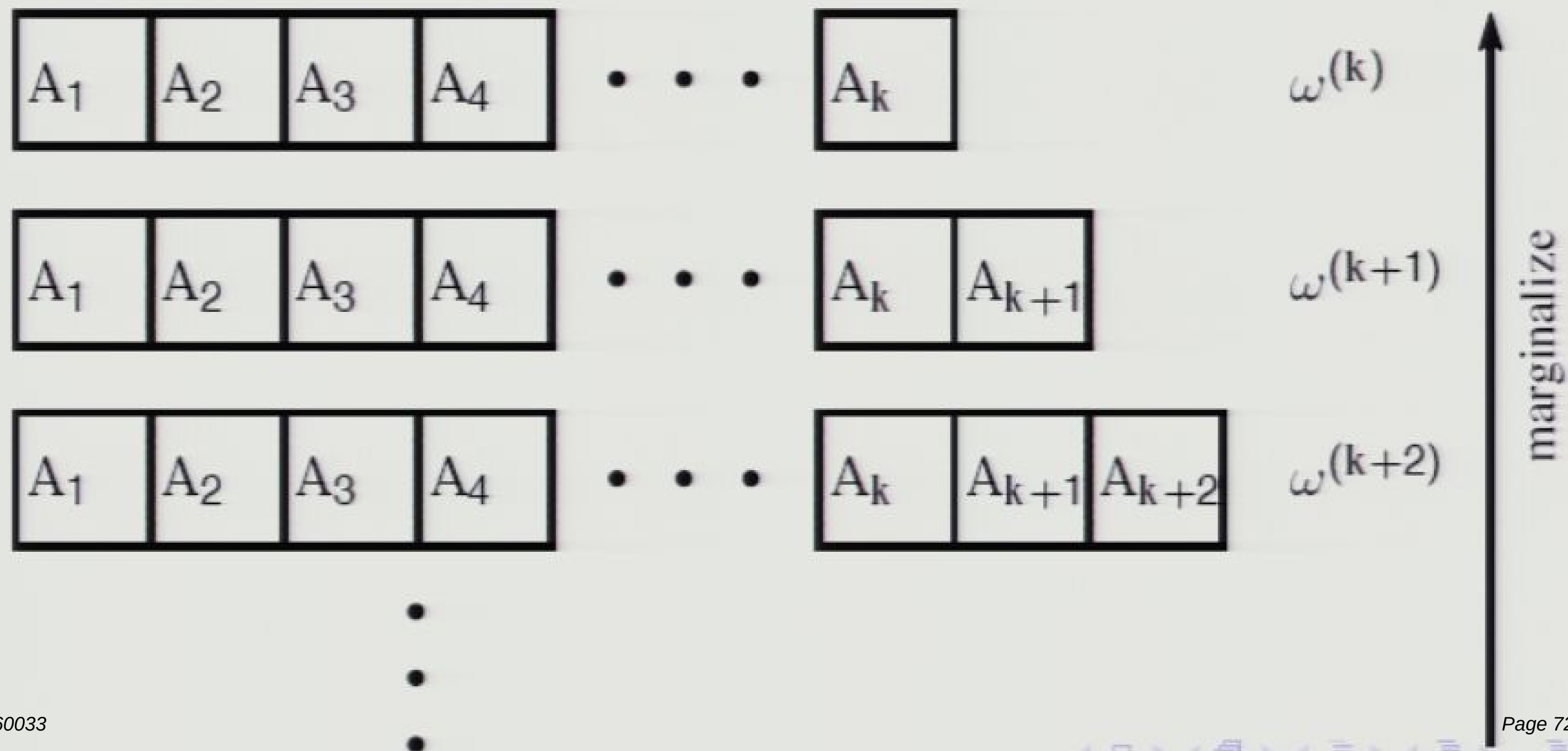
Exchangeability

- Let $\omega^{(k)} \in \Omega_{A_1} \otimes \Omega_{A_2} \otimes \ldots \otimes \Omega_{A_k}$.



Exchangeability

- Let $\omega^{(k)} \in \Omega_{A_1} \otimes \Omega_{A_2} \otimes \ldots \otimes \Omega_{A_k}$.



The de Finetti Theorem

Theorem

All exchangeable states can be written as

$$\omega^{(k)} = \int_{\Omega_A} p(\mu)\mu^{\otimes k} d\mu \tag{1}$$

where $p(\mu)$ is a prob. density and the measure $d\mu$ can be any induced by an embedding in $\mathbb{R}^n$.

The de Finetti Theorem

Proof.

- Consider an IC observable $(f_1, f_2, \ldots, f_n)$ for Ω_A.
- $\{f_{j_1} \otimes f_{j_2} \otimes \ldots \otimes f_{j_k}\}$ is IC for $\Omega_A^{\otimes k}$.
- The prob. distn. it generates is exchangeable - use classical de Finetti theorem.

$$\mathrm{Prob}(j_1, j_2, \ldots, j_k) = \int_{\Delta_N} P(q) q_{j_1} q_{j_2} \ldots q_{j_k} dq$$

- Verify that all q's are of the form $q = \psi_f(\mu)$ for some $\mu \in \Omega_A$.

The de Finetti Theorem

Proof.

- Consider an IC observable $(f_1, f_2, \ldots, f_n)$ for Ω_A.
- $\{f_{j_1} \otimes f_{j_2} \otimes \ldots \otimes f_{j_k}\}$ is IC for $\Omega_A^{\otimes k}$.
- The prob. distn. it generates is exchangeable - use classical de Finetti theorem.

$$\mathrm{Prob}(j_1, j_2, \ldots, j_k) = \int_{\Delta_N} P(q) q_{j_1} q_{j_2} \ldots q_{j_k} dq$$

- Verify that all q's are of the form $q = \psi_f(\mu)$ for some $\mu \in \Omega_A$.

The de Finetti Theorem

Proof.

- Consider an IC observable $(f_1, f_2, \ldots, f_n)$ for Ω_A.
- $\{f_{j_1} \otimes f_{j_2} \otimes \ldots \otimes f_{j_k}\}$ is IC for $\Omega_A^{\otimes k}$.
- The prob. distn. it generates is exchangeable - use classical de Finetti theorem.

$$\mathrm{Prob}(j_1, j_2, \ldots, j_k) = \int_{\Delta_N} P(q) q_{j_1} q_{j_2} \ldots q_{j_k} dq$$

- Verify that all q's are of the form $q = \psi_\Gamma(\mu)$ for some $\mu \in \Omega_A$.

The de Finetti Theorem

Proof.

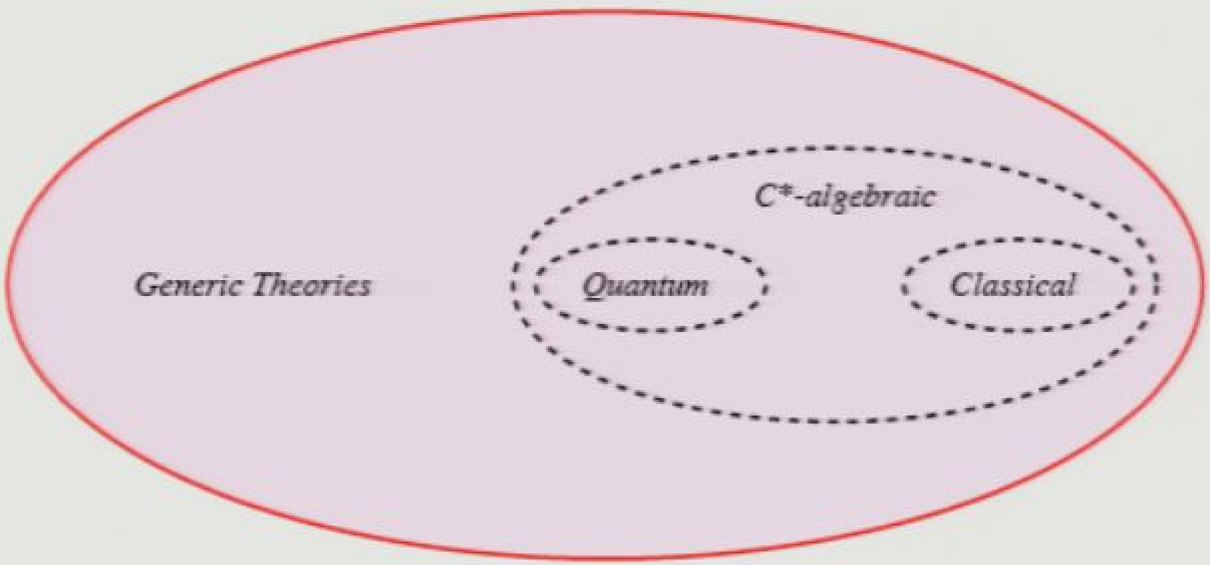
- Consider an IC observable $(f_1, f_2, \ldots, f_n)$ for Ω_A.
- $\{f_{j_1} \otimes f_{j_2} \otimes \ldots \otimes f_{j_k}\}$ is IC for $\Omega_A^{\otimes k}$.
- The prob. distn. it generates is exchangeable - use classical de Finetti theorem.

$$\text{Prob}(j_1, j_2, \ldots, j_k) = \int_{\Delta_N} P(q) q_{j_1} q_{j_2} \ldots q_{j_k} dq$$

- Verify that all q's are of the form $q = \psi_f(\mu)$ for some $\mu \in \Omega_A$.

The de Finetti Theorem

- Have to go outside framework to break de Finetti, e.g. Real Hilbert space QM.



The de Finetti Theorem

Proof.

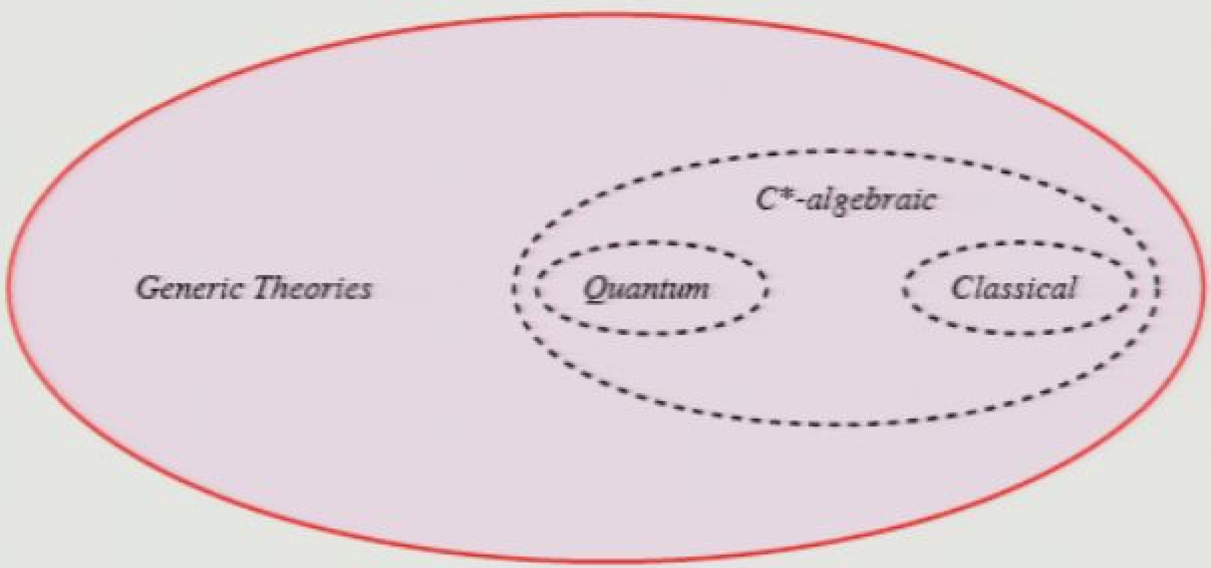
- Consider an IC observable $(f_1, f_2, \ldots, f_n)$ for Ω_A.
- $\{f_{j_1} \otimes f_{j_2} \otimes \ldots \otimes f_{j_k}\}$ is IC for $\Omega_A^{\otimes k}$.
- The prob. distn. it generates is exchangeable - use classical de Finetti theorem.

$$\text{Prob}(j_1, j_2, \ldots, j_k) = \int_{\Delta_N} P(q) q_{j_1} q_{j_2} \ldots q_{j_k} dq$$

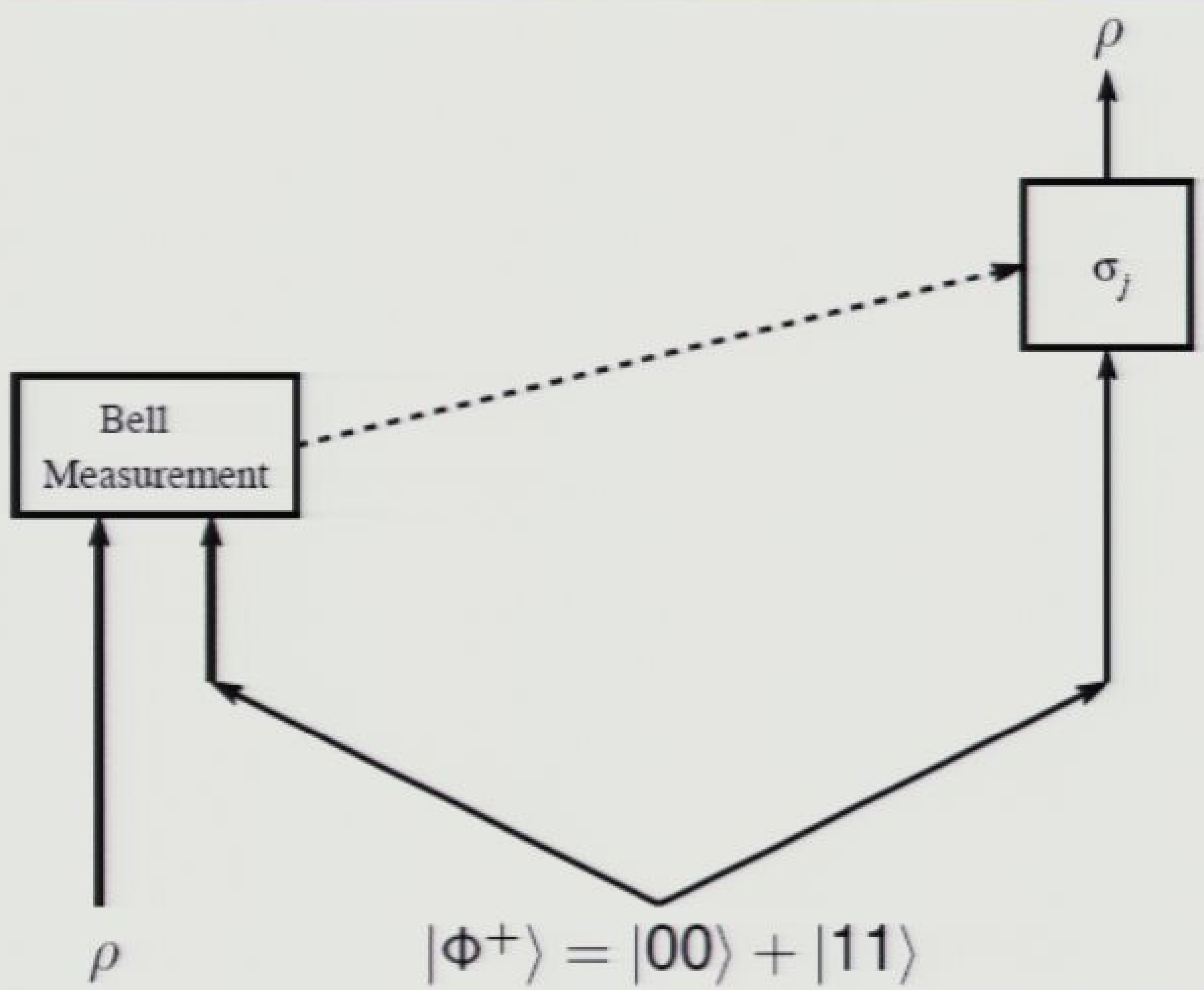
- Verify that all q's are of the form $q = \psi_f(\mu)$ for some $\mu \in \Omega_A$.

The de Finetti Theorem

- Have to go outside framework to break de Finetti, e.g. Real Hilbert space QM.

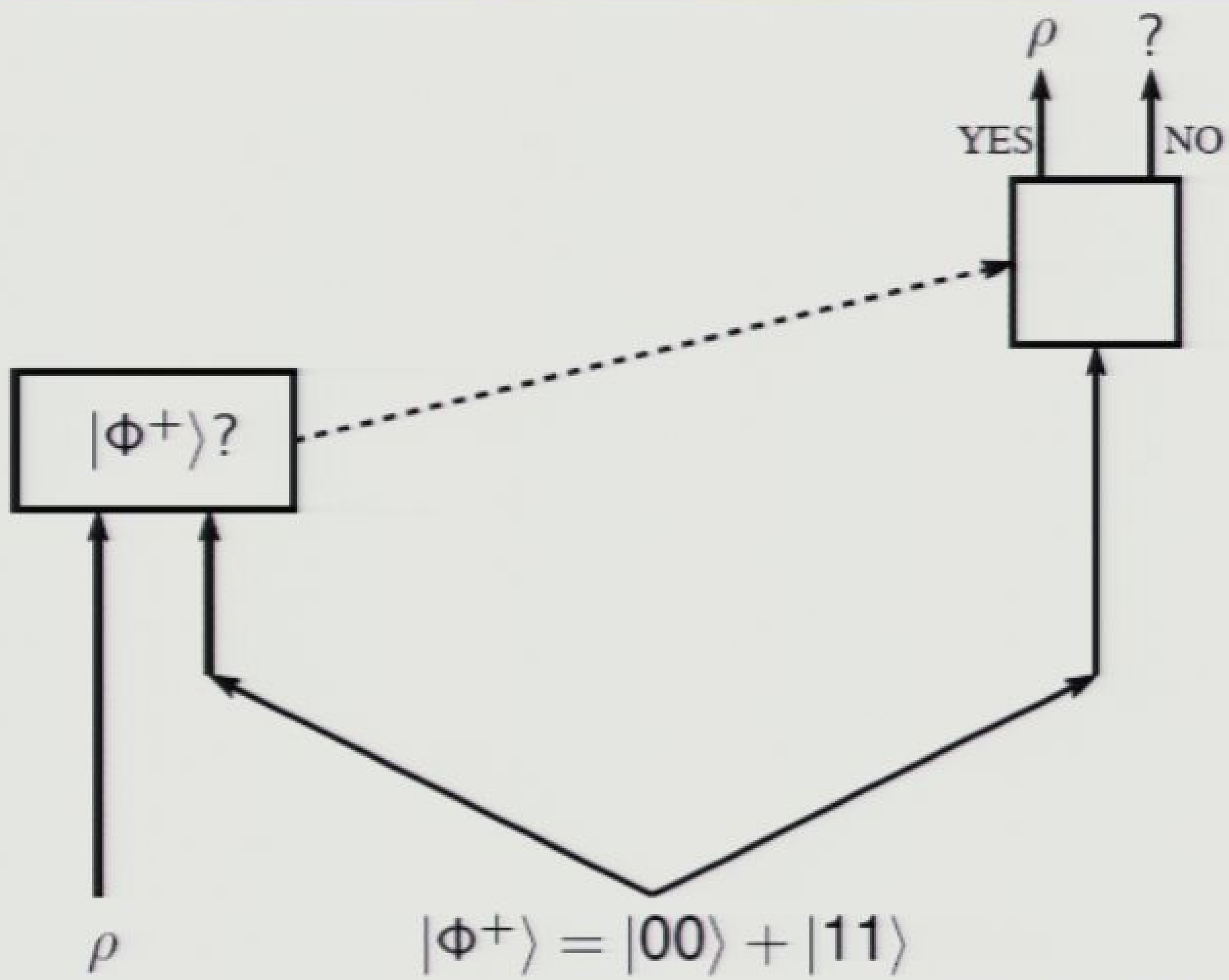


Teleportation



$$|\Phi^+\rangle = |00\rangle + |11\rangle$$

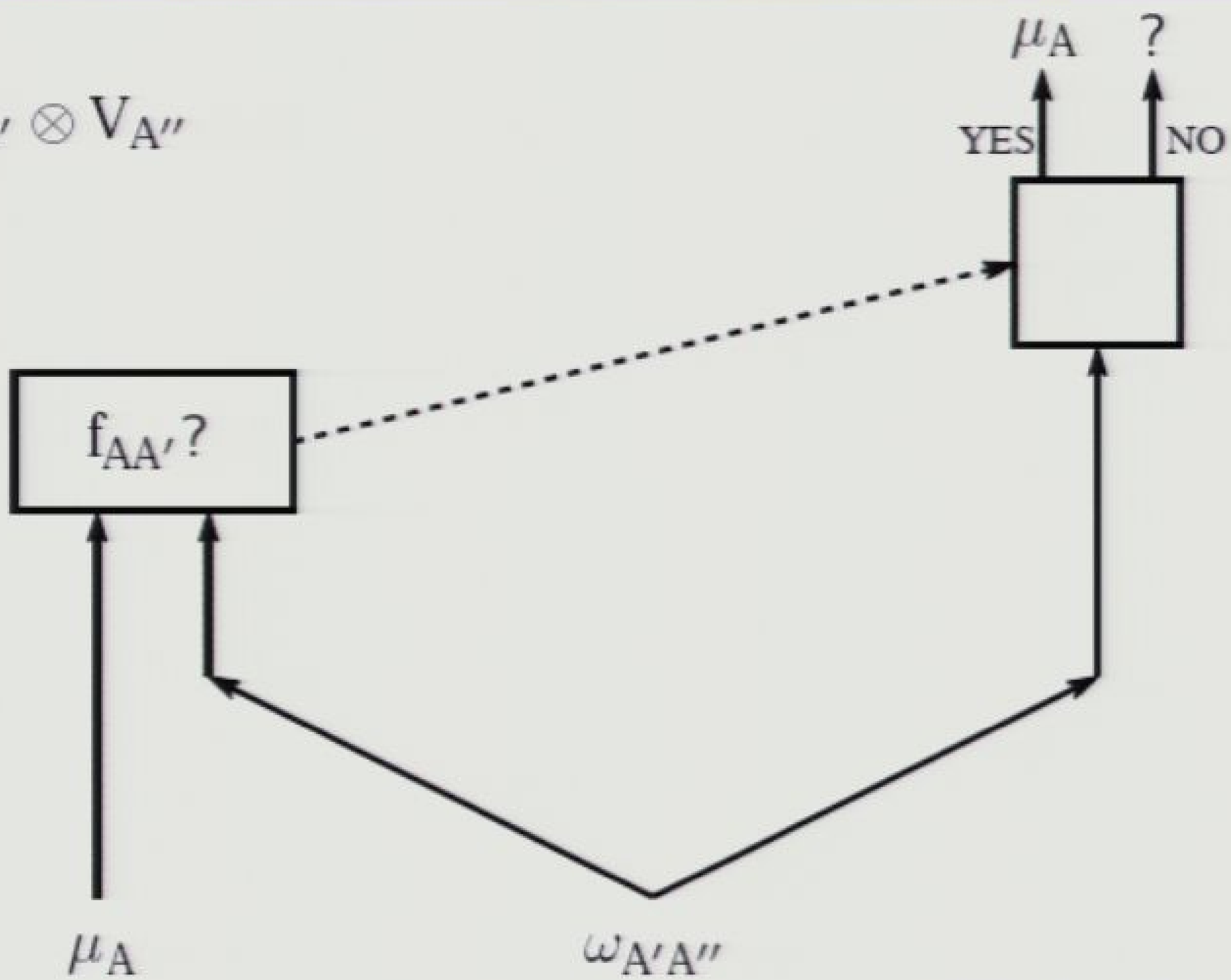
Conclusive Teleportation



$$|\Phi^+\rangle = |00\rangle + |11\rangle$$

Generalized Conclusive Teleportation

$V_A \otimes V_{A'} \otimes V_{A''}$



Generalized Conclusive Teleportation

Theorem

If generalized conclusive teleportation is possible then V_A is affinely isomorphic to V_A^*.

- Not known to be sufficient.
- Weaker than self-dual.
- Implies $\otimes \cong \mathfrak{D}$.

Generalized Conclusive Teleportation

Theorem

If generalized conclusive teleportation is possible then V_A is affinely isomorphic to V_A^*.

- Not known to be sufficient.
- Weaker than self-dual.
- Implies $\otimes \cong \mathfrak{D}$.

Generalized Conclusive Teleportation

Theorem

If generalized conclusive teleportation is possible then V_A is affinely isomorphic to V_A^*.

- Not known to be sufficient.
- Weaker than self-dual.
- Implies $\otimes \cong \mathfrak{D}$.

Generalized Conclusive Teleportation

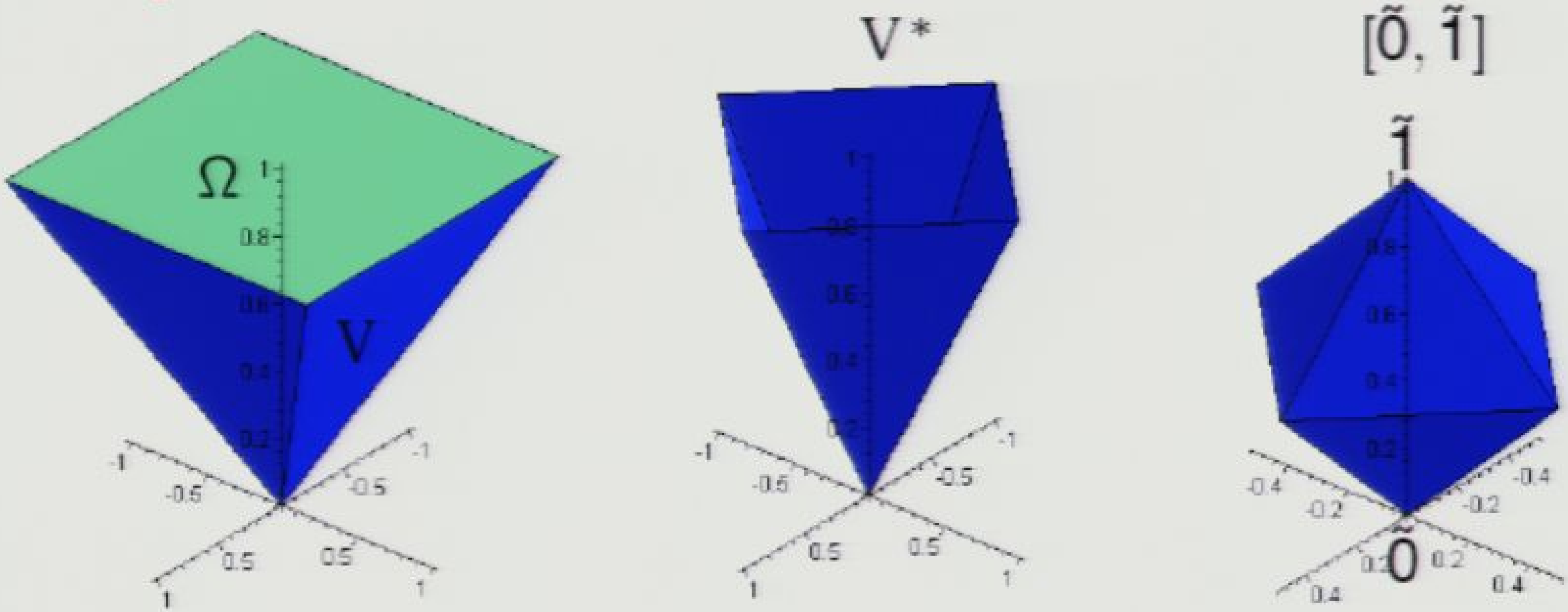
Theorem

If generalized conclusive teleportation is possible then V_A is affinely isomorphic to V_A^*.

- Not known to be sufficient.
- Weaker than self-dual.
- Implies $\otimes \cong \mathfrak{D}$.

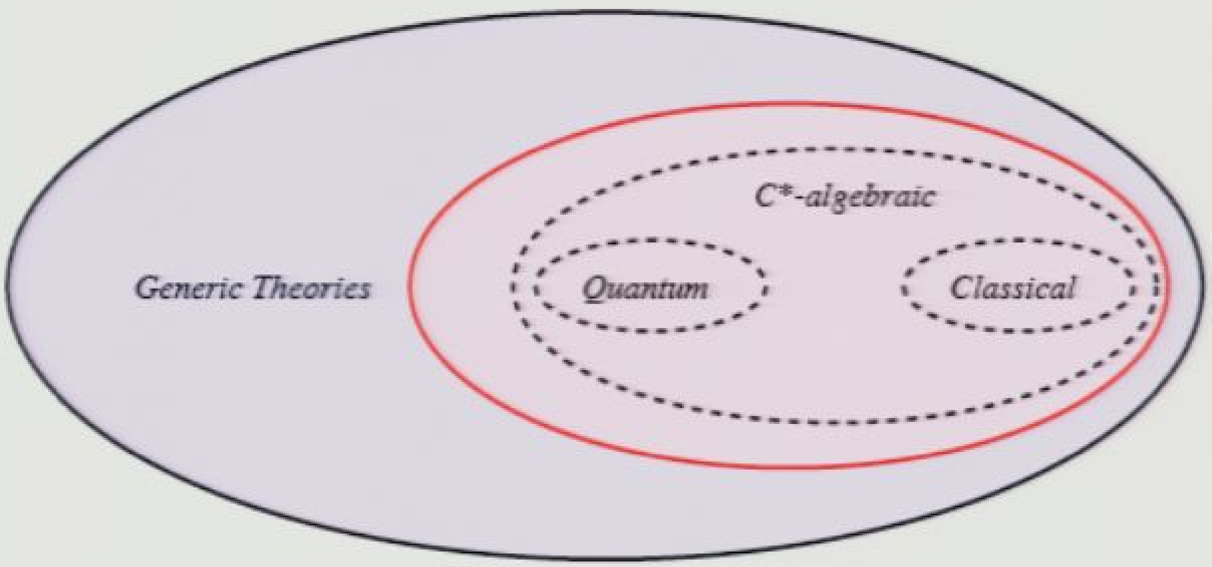
Examples

- Classical: $[\tilde{0}, \tilde{1}] = \{\text{Fuzzy indicator functions}\}$.
- Quantum: $[\tilde{0}, \tilde{1}] \cong \{\text{POVM elements}\}$ via $f(\rho) = \mathrm{Tr}(E_f \rho)$.
- Polyhedral:



Generalized Conclusive Teleportation

- Teleportation exists in all C^*-algebraic theories.



Summary

- Many features of QI thought to be "genuinely quantum mechanical" are generically nonclassical.
- Can generalize much of QI/QP beyond the C^* framework.
- Nontrivial separations exist, but have yet to be fully characterized.

Open Questions

- Finite de Finetti theorem?
- Necessary and sufficient conditions for teleportation.
- Other Protocols
  - Full security proof for Key Distribution?
  - Bit Commitment?
- Which primitives uniquely characterize quantum information?

References

- H. Barnum, J. Barrett, M. Leifer and A. Wilce, “Cloning and Broadcasting in Generic Probabilistic Theories”, quant-ph/0611295.
- J. Barrett and M. Leifer, “Bruno In Boxworld”, coming to an arXiv near you soon!