Information processing protocols and primitives and the structure of physical theories

Howard Barnum

LANL; soon, Perimeter Institute

July 12, 2009 / 2nd FQXI Conference

Information Sciences Group/CCS-3 (LANL)
Aug. 2009 – Aug. 2010: Perimeter Institute for Theoretical Physics, Waterloo Ontario hnbarnum@aol.com

Collaborators: J. Barrett, DAMTP, University of Cambridge; O. Dahlsten, ETH Zürich;
M. Leifer, CQC, University of Waterloo; B. Toner, CWI, Amsterdam; A. Wilce, University of Susquehanna

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, Alfsén-Shultz, Araki 1980, Quantum logical

Generalized Probabilistic or “Operational” Approach

- Whatever else they are, quantum states are compendia of probabilities for the outcomes of all measurements we might make on them. And quantum effects (POVM elements) are compendia of their probabilities in all states they might occur on. Study more general theories in such a states/effects framework.
- Some think a fundamental theory should not be about probabilities of measurement outcomes. We may not know what QM is “really about” or how it “should” be formulated, but studying the structure of these probabilities may help us understand it. Maybe QM is a theory for how small subsystems of the universe look to other, somewhat larger, subsystems...

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, $\mathscr{D}_A$.
- Perhaps: way(s) of making "composite" systems, or of recognizing compositeness: $C = A \otimes B$

(Looks a bit categorical!)

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)
- Exponentially secure bit commitment is possible in any non-classical theory that does not have entanglement. (BDLT)
- Necessary conditions for conclusive teleportation (BBLW)
- Sufficient conditions for deterministic teleportation (BBLW)
- 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 $A = K - K = \{a - b | a, b \in K\}$.

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 compact convex set of *normalized states* $\Omega_A = u^{-1}(1)$.

(Every compact convex set can be given this form.)

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 maximal *simplex* in $\mathbf{R}^d$.

Definition

A **simplex** in $\mathbf{R}^d$ is the convex hull of $d+1$ or fewer linearly 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 the cone of unnormalized states.
Effects f also satisfy $\forall \omega \in \Omega, f(\omega) \leq 1$. I.e. $f \leq u$ (u is the *unit effect*.)

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 $u_{AB} = u_A \otimes u_B$.

This implies:

- No signalling (marginals are well defined)
- Local observability Expectations of products of local observables determine states.

NB: this definition doesn't determine $A \otimes B$, unless one of them is classical.

Composites II

Examples

(a) The *maximal tensor product*, $A \otimes_{\max} B$, consists of *all* states positive on product effects.

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

(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.

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)).

Nonclassicality + No Entanglement = Bit Commitment

Theorem (Barnum, Dahlsten, Leifer, Toner)

In any non-classical theory that does not allow entanglement, there is a family of perfectly hiding, perfectly sound, ε-binding protocols, where ε is exponentially small in the number of identical systems the protocol uses.

Proceedings of the 2008 IEEE Information Theory Workshop (ITW 2008), Porto, Portugal.

Nonclassicality + No Entanglement = Bit Commitment

The Protocol:

1. Alice encodes the committed bit b in which of two convex decompositions of a fixed mixed state

$$\mu = \sum_{i=1}^{N^0} p_i^0 \mu_i^0 = \sum_{j=1}^{N^1} p_j^1 \mu_j^1, \tag{1}$$

   into exposed pure states she draws from, i.e. she draws n independent values of i with probabilities p_i^b if she is committing to b, and sends the pure states μ_i^b to Bob.
2. To reveal, she tells Bob b and the string of i values she drew.
3. To test for cheating, he performs, on each system, a two-valued observable that has probability 1 for a positive outcome if the state is the one Alice claimed, and probability less than 1 for all other states. He rejects unless all outcomes are positive.

Nonclassicality + No Entanglement = Bit Commitment: Elements of the proof

- That the "distinguishing observables" described above exist for all the states used in the protocol is the definition of "exposed state".
- It's well known that in any nonclassical theory, there are mixed states with nonunique decompositions into *pure* states. The following fairly easy lemma adds the fact that these states can always be chosen to be exposed, and a bound on the number of states needed in the decompositions.

Lemma

Every nonsimplicial convex compact set Ω of dimension d contains a state μ with two convex decompositions into disjoint sets of exposed states, whose total cardinality is no greater than than $d+1$.

Conditionalization maps: "Generalized Choi-Jamiolkowski isomorphism"

Conditional state:

$$\omega_a^B(b) = \omega^{AB}(a \otimes b) \left(= \omega_b^A(a) \right) . \tag{2}$$

Conditionalization map $\hat{\omega} : A^* \to B$ takes effect $a \in A^*$ to conditional state ω_a^B. (It's linear, positive.) Similarly, $f \in A^* \otimes B^*$ is associated with a linear positive $\hat{f} : A \to B^*$.

In quantum case, self-duality of A means $A \simeq A^*$ canonically, so $\omega^{AB} \leftrightarrow \hat{\omega}' : A \to B$ canonically: e.g. bipartite states on $A \otimes A$ correspond to completely positive maps on A.

Ensembles

Definition (Ensemble)

Normalized ensemble for state ω: p_i, ω_i: $\sum_i p_i \omega_i = \omega$. **Ensemble** for ω: unnormalized states $\omega_i : \sum_i \omega_i = \omega$.

Fact

For any state ω^{AB} and any measurement $\{f_i\}$, $\omega^B_{f_i}$ are an ensemble for the marginal state ω^B.

Definition (State steering for marginal)

A state ω^{AB} is *steering* for its marginal ω^B, if for *every* ensemble $\{\omega_i\}$ for ω^B, there exists an observable $\{f_i\}$ such that $\omega_i = \omega^{AB}_{f_i}$.

Steering

Proposition (Isomorphism states are steering)

If ω^{AB} is a state such that $\hat{\omega} : A^* \to B$ is an isomorphism, it is steering for ω^B.

In a theory in which such a state ω^{AB} can be prepared, *no* bit commitment protocol based (like the one presented earlier) on the nonuniqueness of ω^B's decomposition into pure states can be secure. Alice can obtain *any* ensemble for ω^B by preparing ω^{AB}, sending the B part to Bob to commit, and inducing either the 0 ensemble or the 1 ensemble by choice of measurement *after* the commit stage.

Steering II

Proposition (Slight generalization of above)

If ω^{AB} is a state such that $\hat{\omega} : A^* \to B$ is an isomorphism from A^* to $\mathrm{Face}(\omega^B)$, then it is steering for ω^B.

Proof.

Let $\omega^B = \sum_i \eta_i$, with $\eta_i \neq 0$ pure states (i.e. in extremal rays of B, though typically subnormalized). For all i, $\eta_i \in \mathrm{Face}(\omega^B)$. Now, view $\hat{\omega}$ as a map from A^* onto ω^B; by assumption it is an isomorphism. So there is a unique $f_i := \hat{\omega}^{-1}(\eta_i) \in A^*$ such that $\hat{\omega}(f_i) = \eta_i$. Now, $\sum_i f_i \equiv \sum_i \hat{\omega}^{-1}(\eta_i) \equiv \hat{\omega}^{-1}(\sum_i \eta_i) \equiv \hat{\omega}^{-1}(\omega^B) \equiv u$. Therefore, f_i are a measurement that steers to the ensemble $\{\eta_i\}$ for ω^B. *Any* ensemble, not necessarily of pure states, has the form $\{\sum_j \eta_{ij}\}_i$ for some pure states η_{ij}. So it can be steered to by the measurement $\{\sum_j f_{ij}\}_i$. □