Report on Conceptual Foundations and Foils for QIP at the Perimeter Institute, May 9 – May 13 2011

Vlad Gheorghiu

Department of Physics
Carnegie Mellon University
Pittsburgh, PA 15213, U.S.A.

May 19, 2011

1. Gilles Brassard – Is Information the Key?
2. Paolo Perinotti – Quantum Theory as a Theory of Information Processing
3. Scott Aaronson – The Territory Around BQP

- All talks from this conference are video-recorded at http://pirsa.org/C11006
- A summary of this talk is available online at http://quantum.phys.cmu.edu/QIP

Gilles Brassard – Is Information the Key?

Abstract: Consider the two great physical theories of the twentieth century: relativity and quantum mechanics. Einstein derived relativity from very simple principles. By contrast, the foundation of quantum mechanics is built on a set of rather strange, disjointed and ad hoc axioms, reflecting at best the history that led to discovering this new world order. The purpose of this talk is to argue that a better foundation for quantum mechanics lies within the teachings of quantum information science. The basic postulate is that the truly fundamental laws of Nature concern information, not waves or particles. For example, it is known that quantum key distribution is possible but quantum bit commitment is not and that nature is nonlocal but not as nonlocal as is imposed by causality. But should these statements be considered as theorems or axioms? It's time to pause and reflect on what is really fundamental and what are merely consequences. Could information be the key?

- Throw away quantum axioms (Hilbert spaces, measurements etc)
- From what deep informational principles might we derive this exquisite mathematical structure?
- John Wheeler, Chris Fuchs
- Theory about the representation and manipulation of information, not about the mechanics of nonclassical waves or particles. The notion of quantum information is to be understood as a new physical primitive.
- Einstein, 1948: We all of us have some idea of what the basic axioms in physics will turn out to be. The quantum of the particle will surely not be amongst them.
- Strong contrast between special relativity (2 postulates) and quantum mechanics.

Brassard's dream

1. Confidentiality (QM Cryptography)
2. Impossibility of Commitment (Q Bit Commitment)

- John Smolin proved that only these 2 principles are not enough (toy world).

1. Faster-than-light Information Transfer Impossible
2. Impossibility of Commitment (Q Bit Commitment)
3. Perfect Broadcasting Impossible

Almost quantum mechanics, still need Underlying Formalism is a C^*-algebra. Doesn't look fundamental.

Non-local boxex

- $a \oplus b = x$ AND y
- Cannot be used to communicate. Are causal and atemporal.
- Can be simulated classically with $p = 75\%$.
- Can be simulated *quantumly* with $p = \cos^2(\frac{\pi}{8}) \approx 85\%$.
- Is this a fundamental principle?
- Why can't quantum mechanics yield the strongest nonlocal correlations possible among all causal theories? Why did QM picked 85%?

Communication complexity

- Communication complexity: Alice and Bob have inputs x, y, want to compute a Boolean function $f(x, y)$. Goal: minimize the number of bits of communication.
- Shared entanglement can sometimes reduce exponentially the amount of communication.
- Still, even with shared entanglement, there are non-trivial Boolean functions (that require more than one bit of communication).
- If non-local boxes were possible, all Boolean functions would become trivial (Wim van Dam, arXiv:quant-ph/0501159v1).
- New axiom: Some Boolean functions have nontrivial communication complexity. Explains why QM is not 100% non-local, but not the 85%.

Information causality as a physical principle

- Brassard et al, PRL **96**, 250401 (2006): Limit on Nonlocality in Any World in Which Communication Complexity Is Not Trivial.
- Why are the correlations achievable by QM non-maximal among those that preserve causality?
- Partial answer: Slightly stronger ($\frac{3+\sqrt{6}}{6} \approx 90.8\%$) correlations would result in a world in which communication complexity becomes trivial.
- Information causality as a physical principle, Nature **461**, 1101 (2009): Alice has some unknown set, and sends to Bob m bits of information. Bob cannot learn more than m bits of information about Alice's set!
- This brings it down to 85%! All other causal theories with stronger correlations violates the information causality principle!

Paolo Perinotti – Quantum Theory as a Theory of Information Processing

- Conceptual physics and not purely mathematical QM axioms.
- Looking for physical axioms that are operationally defined!
- Then the axioms can be translate into a suitable mathematical language.
- Axioms should be about information processing capabilities. Example: "The state of a single system cannot be cloned."
- Operational language: boxes, inputs, outputs, tests (preparation, observation), composition rules, coarse-graining, refinements etc. This is a generalized probabilistic theory.
- States are functionals on effects and viceversa.

The Axioms

1. Causality: The probability of preparations is independent of the choice of observations. No backwards signalling. Implies no signalling!
2. Local discriminability: If two bipartite states are different, they give different probabilities for at least one product experiment. Implies tensor product structure.
3. Atomicity of the composition: The sequential composition of two atomic operations (don't allow refinement) is atomic.
4. Perfect distinguishability: Every state that is not completely mixed can be perfectly distinguished from some other state.
5. Efficient lossless compression: For every state there exists an ideal compression scheme. Implies subsystems.
6. Purification: Every state has a purification. For fixed purifying system, every two purifications of the same state are connected by a reversible transformation on the purifying system. Singles out QM from the other general causal probabilistic theories. Implies the Stinespring dilation theorem.

Scott Aaronson – The Territory Around BQP

- Use computational complexity to look for "foils" of Quantum Mechanics.
- Subclasses of BQP, but not yet P.
- Example: Log-depth QC (BQNC). Don't know to be equivalent to full BQP, but *contains factoring*!
- Open problem by Jozsa: Is BQP = BQNC + poly-time classical computation?
- Another example: Separable Mixed State Model. At every time step, the quantum computer is in a separable mixed state.
- No entanglement, but still no efficient classical simulation of this model! Find an interesting problem that can be done with this model (and that is classically hard).

- Problem: Is there a set of (unitary qubit) gates that gives you an intermediate model between P and BQP?
- Superclasses of BQP.
- Non-linear QM: can solve NP-complete problems in poly-time (can distinguish exponentially-closed non-orthogonal states, non-isometries!). But all non-linear models allow signalling!
- Post-selected BQP Proved that = PP (decision problem which asks if a majority (more than half) of the computational paths accept)).
- QC with Time Travel (BQP_{CTC}) Proved that BQP_{CTC} = PSPACE.
- QC With Non-Collapsing Measurements: Can solve graph-isomorphism problem in poly-time! Can also solve Grover's in $N^{1/3}$ (vs $N^{1/2}$) steps. Still cannot (probably) solve NP-complete problems, but generalizes BQP by a little bit!