The Strange Quantum

Robert Spekkens (ISSYP lecturer), as filtered through Alex Dehnert

Thursday, August 24, 2007

1 Measuring and Commutativity

- Consider boxes that measure $\pm X$, $\pm Y$, $\pm Z$ spin.
- Outcome of a second $\pm Z$ measurement is exactly same as first
- Outcome of a $\pm Z \pm X$ sequence is random (all four possibilities equal)
- Outcome of a $\pm Z \pm X \pm Z$ sequence is random (all *eight* possibilities equal)
- An intervening X randomizes the Z (equivalently, $[\widehat{X}, \widehat{Z}] \neq \widehat{0}]$)
- If Alice has a $\pm Z$ box behind a wall, Bob (maybe) measures with a $\pm X$ or $\pm Z$ box, Alice can detect Bob with another $\pm Z$ — Bob has a low chance of measuring Alice's polarization without detection

2 Cryptographic Applications

2.1 Quantum Counterfeit-Proof Money

- Take a bill, put small storage chambers inside
- Put randomly selected atoms with polarization
- Save polarization data $(+Z - Z - X + X + X)$
- To check a bill, merchant teleports atoms to the mint, which checks the polarization
- To counterfeit, measure the atoms. However, counterfeiter needs to guess, and his guessing destroys the information.
- Probability of copied money passing the test: 2^{-B}, where B = number of atoms
- Probability of original passing the test: $\left(\frac{3}{4}\right)^B$, where B = number of atoms

2.2 Quantum Detection of Eavesdroppers

- Alice and Bob have a channel to communicate on
- Eve wants to add a wiretap
- Conventional Ciphers

  Caesar Easy to brute-force, or just use frequency analysis

  Vernam (One time pad) Impossible to break, but need a really long, random key (Information theoretic security)
- Quantum Key distribution

- Alice picks some bases at random ($\pm X$, $\pm Z$)
- Bob also picks some bases at random
- Alice sends those photons, and keeps track of what she saw
- Alice, Bob compare which pairs should have been measured equally
- Take a small subset of the successfully transmitted photons, and compare what they should have been
- If some differ, we know that the photon interacted with the environment (including possibly Eve)
- Need a source of randomness (but needn't share anything, I think)

3 Idea of Hidden Variable Models of QM

- Toy world with restrictions on knowledge
- Four states, can't know which — can know that it is equally likely to be in either of two states (and know not in the other two states)
- Can only check whether in one pair, or the other (eg, in (1 or 2) or (3 or 4))
- Updating the probability distribution
  - $\pm Z \rightarrow$ (1 or 2)
  - $\pm X \rightarrow$ (1 or 3)
  - $\pm Z \pm X$ must just force the measurement to (1 or 2) (and let states jump around), b/c otherwise we could get maximal knowledge
  - Half the time swap states (1 and 2), half the time don't do anything

4 Bell's Theorem

Why any realistic account of quantum mechanics must be nonlocal

- Take a laser, nonlinear crystal, polarization to get entangled states
- Send one photon to Alice, one to Bob
- Measurements: S, T
- Alice, Bob give an answer to S or T measurement, with required method of correlation
- Some of these "games" can never be won (classically)
- You can cheat in one of these guessing games by sending what the measurement was
- However, photons can "cheat" this way even when they are too far for even light to get there in time
- How does this work with both no faster-than-light information transfer, and the necessity of faster-than-light info transfer for entanglement to work