Today:

Finishing up quantum measurement

Quantum computers and cryptography

Perspectives on measurement

- The central problem of the folk approach is that it does not specify at what point the linear wave eq. ceases to apply, and thus is incomplete in the sense that it does not fully describe whether interference effects will be found in hypothetical experiments with large-scale quantum coherence.
- The formal Copenhagen approach avoids that problem by saying that the wave function is a non-existent entity to which the linear wave function applies exactly, in between experiences, which are real. The problem here is that "experience" is elevated to a central position in the physical working of the universe- it delimits the applicability of the wave equation. However, "experience' is an extremely fuzzy concept, and appears to play an ephemeral role in a universe whose physical behavior seems to be consistent over broad expanses of time and space.
- The Bohm approach invokes a dualist picture: a well-defined global position (of all particle coordinates) guided by a wave. It is unclear whether it would allow some experimental test of the existence of the well-defined position variable, i.e. the line between the microworld (with an equilibrated probability density) and the macro world (which is known with certainty) remains somewhat arbitrary. It is not fundamentally Lorentz-invariant. It is equally compatible with single-world or many-world interpretations.
- The "macro-realist" approaches predict that the wave function really does collapse (following a non-linear equation), under circumstances which depend on physical parameters. The theories are not yet full developed, and invoke non-QM random fields, and severe non-locality, including tachyons in current versions.

.

Perspectives on measurement

- The standard Many Worlds picture contains only the wave function obeying the linear wave equation. It doesn't yet explain why the universe is found in a condition in which "measurement" occurs, but it is consistent with that description. It gives the wrong probabilities for experimental outcomes in simple cases. Do the actual probabilities only emerge because of background noise?
- Notice that the Many-Worlds pictures approach the experience/reality question in a way opposite to the Copenhagen. For Copenhagen, experience is the central theme, even at the cost of making the theory anthropocentric. People sound central to the process. For Many Worlds, the math is taken to be central, with the requirement that experience be correctly predicted. People are so radically peripheral to the process that most aspects of reality remain completely hidden from any individual experience.

Perspectives on measurement

Conclusion

- The world has not been kind to local realism. The observed violations of local realism are just what QM predicts. However, special relativity has survived intact, no matter how beat-up our intuitions may be.
- It is evident that the current state of the interpretation of QM (centered around the measurement problem) is unsatisfactory. We have been driven to a variety ideas, some out of touch with the rest of science, some incomplete, some utterly fantastical.
- We do not know if a proper theory exists

Quantum Computation:

- So long as no decoherence events occur, QM proceeds as if even single particles were undergoing many parallel experiences. Is there a way to then use a small number of particles to generate in effect a large number of parallel processes, i.e. to get ultra-massive parallel computing with only a small computer?
- E.g. 4 classical two-state bits: A or a, B or b, C or c, D or d.
- These give 2^4=16 possible combinations:
- ABCD, ABCd, ABcD, ABcd, AbCD, AbCd, AbcD, Abcd,
  aBCD, aBCd, aBcD, aBcd, abCD, abCd, abcD, abcd.
- Now let's take 4 quantum particles, each of which has two accessible states, as above. As in EPR, distinct particles can be *entangled*. In other words, the overall quantum states are not restricted to ones with definite classical combinations. One can have a state such as:

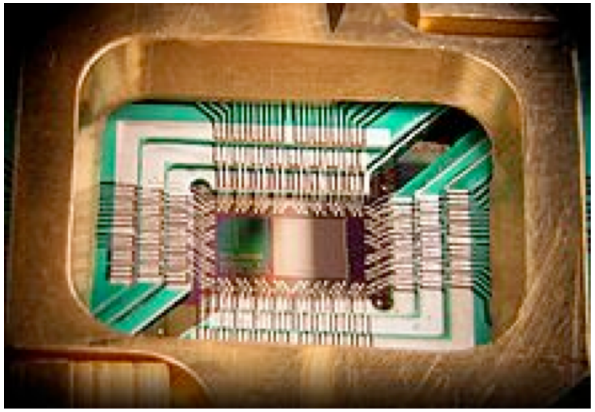
  (ABCD + ABCd- ABcD- ABcd+AbCD- AbCd- AbcD+ Abcd+ aBCD - aBCd - aBcD - aBcd+ abCD+ abCd- abcD+ abcd)/4

- The 16 phases of the 16 components can each evolve separately. In effect, that gives the equivalent of about 16 classical bits of information, *inside* the computer.

- Now what if we had 10 classical bits, rather than 4?
- If we convert each to a qbit, we have $2^{10} = 1024$ distinct (orthogonal) entangled states, i.e. about 1024 bits worth of information.
- The number of bits of information being simultaneously processed by the N sites is about 2^N, rather than N.
- Nevertheless, there are severe limits on getting classical-like information in and out of this system, greatly restricting the types of algorithms for which quantum computation is effective.

Quantum Computers

- Factoring large numbers: Shor's algorithm can be used to read encrypted messages.
- Searching data bases.
- Finding global minima
- Simulating quantum systems
- There are claims, by D-Wave, that they have such a device, but it has not yet been shown to be better than a regular laptop.



Quantum cryptography

(semi-relevant, but interesting)

- One can use QM correlations and the collapse of the wave function to devise perfectly encrypted communication. A perfect code is one in which the encryption scheme changes randomly from one character to the next. Then, a spy can learn nothing at all about future messages, no matter what she knows about past ones.
- If the sender and recipient share a table of random numbers, they can use it to ensure privacy. This "one time pad" is the method used by governments to send secure communications overseas. However, it requires advance (insecure) transmission of the table. The EPR apparatus can avoid this insecurity.
- Consider a sequence of correlated photon pairs. Let each observer (sender and receiver) set his polarizer along the x-axis.
- Each observer measures a random sequence of passes and fails. This sequence must be kept secret. This is easy, because it is not sent anywhere.
- The two sequences are perfectly correlated, so they can be used to encode/decode messages.
- Requires long distance QM correlations. About 250 km of optical fiber length or 23 km of satellite spacing has been achieved, 143 km between telescopes.

Eavesdroppers?

- The presence of an eavesdropper is immediately detected, because making a measurement collapses the 2-photon wave function. This means:
  - The observers can compare a subset of their sequences, looking for a loss of correlation.
    - And they can use perfectly open communication to make this comparison, then throw out that subset
  - The received message will be gibberish, due to the loss of correlation.
    - UNLESS: the eavesdropper sends his own duplicate photon , with the same polarization as the one detected.

- How can that problem be avoided?

- Have each of the two communicators *randomly change* the setting on their polarization analyzers (0-90 or 45-135 degrees)
- In the subsequent open communication, they tell each other what their settings were, and throw out all measurements where their settings weren't the same.
- Now they are left with a set of perfectly correlated pairs.

Quantum Cryptography

What happens if you eavesdrop?

- You don't know which axis to set your polarizer on. Sometimes, e.g., you will use 0-90 when the communicators use 45-135. For those, even if you send something with the polarization you measure, it will be RANDOMLY polarized along their axes. They will notice that a significant number of their photons are uncorrelated.
- When you later overhear what their analyzer settings were, the damage has already been done; they know someone is listening.

Is this really an unbreakable code?

- It uses the breakdown of local realism. What about our other assumption in deriving the Bell Inequalities: no conspiracies?
- Say that you bought the source of the particle pairs and the detectors with their random number generators from the TrustMe Corp. Maybe it has no particle pairs, random number generators, etc. There's just a pre-programmed output that looks exactly like the quantum case. Maybe it's a classical record of the output of a real quantum device they've run previously. They know your whole code. Nothing is secure.
- The "no conspiracy" assumption is crucial for the use of Bell violations in cryptography!