QUANTUM COMPUTING (AND OTHER SHORTCUTS FOR SOLVING HARD PROBLEMS)

Lecture 28 – CS2110 – Spring 2013

The world isn't as simple as it seems!

- Starting as early as the Greek philosophers, people have wondered what the world is "made of"
  - Fire, earth, water and air?
  - Atoms?
  - Basic particles: electrons, neutrons, protons?
  - Quarks?
  - Or perhaps… m-branes?
- Each discovery has explained things a bit better and also revealed new puzzles
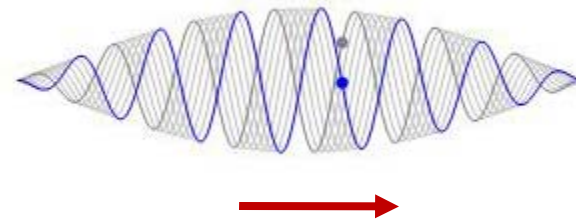
Examples of puzzles

- Accounting for the big bang

- Explaining the nature of dark matter

- Understanding what happens inside a black hole

- Understanding what it means to "observe" something
  - Quantum computing revolves around this problem

What is an elementary particle?

- This is an old question
  - Bohr visualized a nice hard nugget of matter with various properties
  - Heisenberg was convinced that when you look very closely, you see some form of waves, not particles
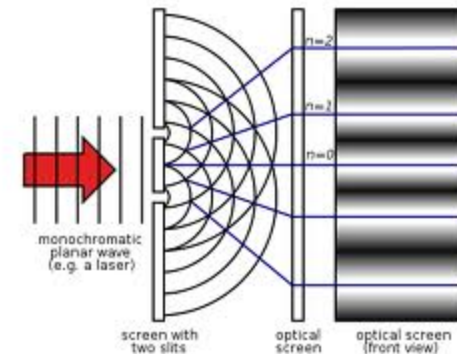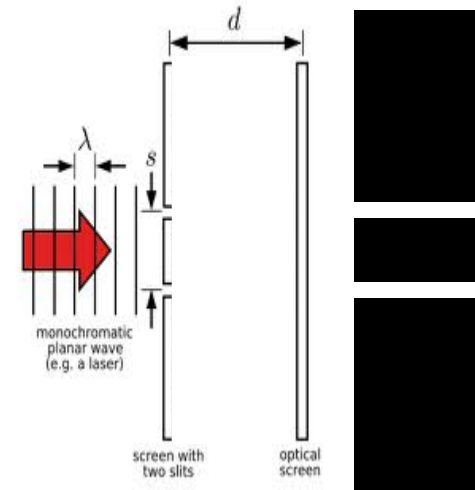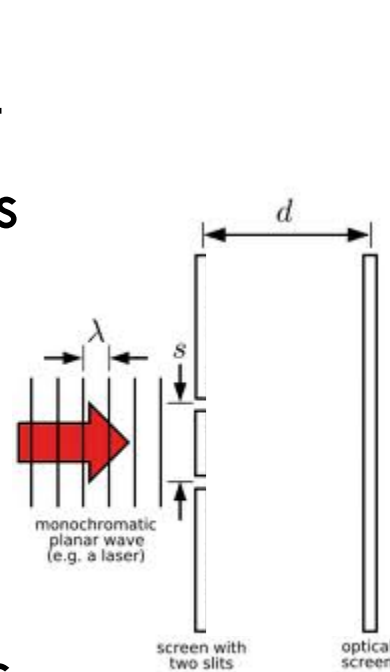
Are elementary particles like the bullet, or like the wave?

Two slit experiment

- We point a laser at a mask with two slits scratched on it

- If the laser light is particles, we would expect to see two bright spots

- Instead, see an interference pattern
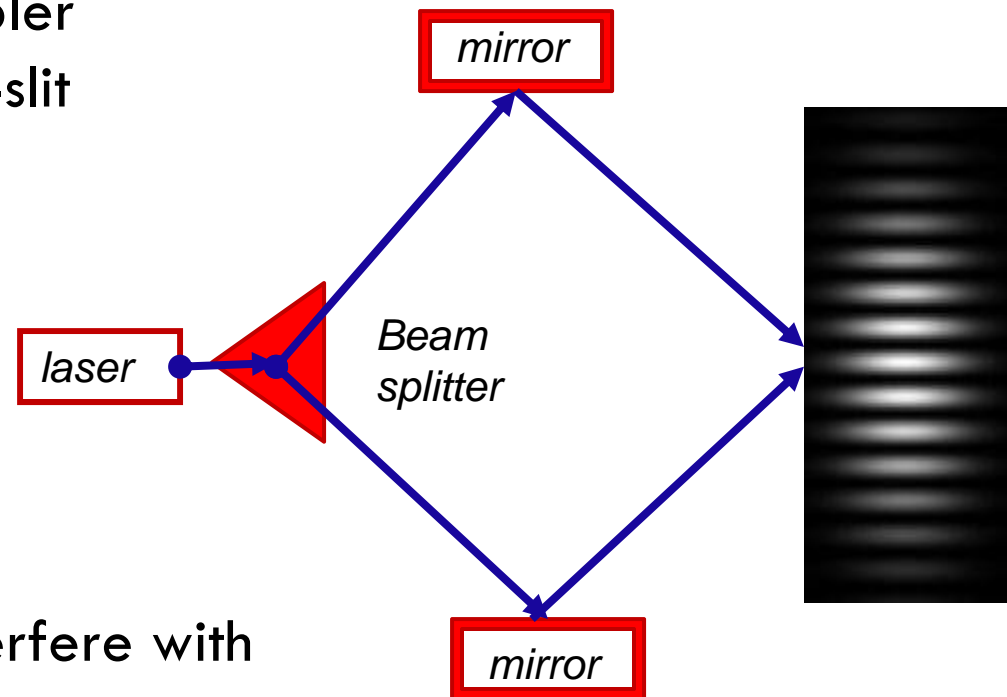
Variations on the experiment

- With just a _single_ slit, we do get a very crisp single bright spot, as expected

- In fact we get this if we cover either slit

- But (here's the tricky part) what if you reduce the power of the laser until just one particle is emitted at a time?
  - This was the surprise
  - Turns out _we still get an interference pattern_!

A *really* peculiar example

- Wheeler suggested this diamond setup as an even simpler illustration of the two-slit experiments

mirror

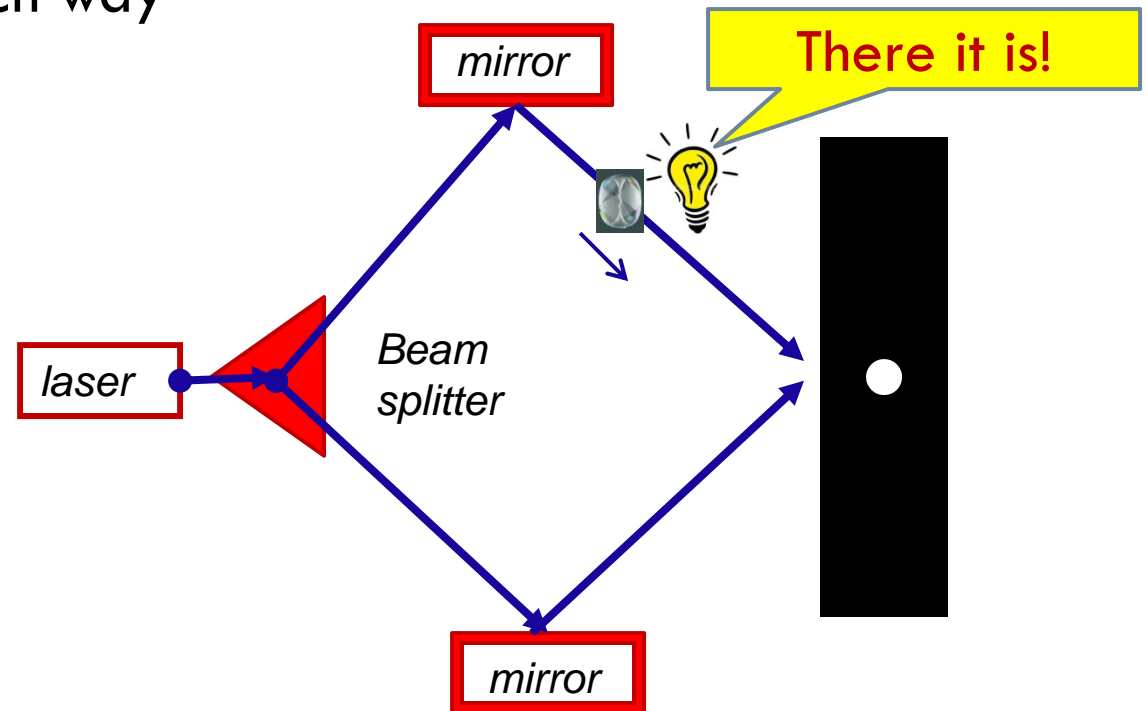Beam splitter

laser

mirror

- A laser beam will interfere with itself… even if the intensity is just one photon at a time

A *really* peculiar example

☐ Suppose we add a "photon detector"?
Now we can tell "which way"
the particle went…

mirror
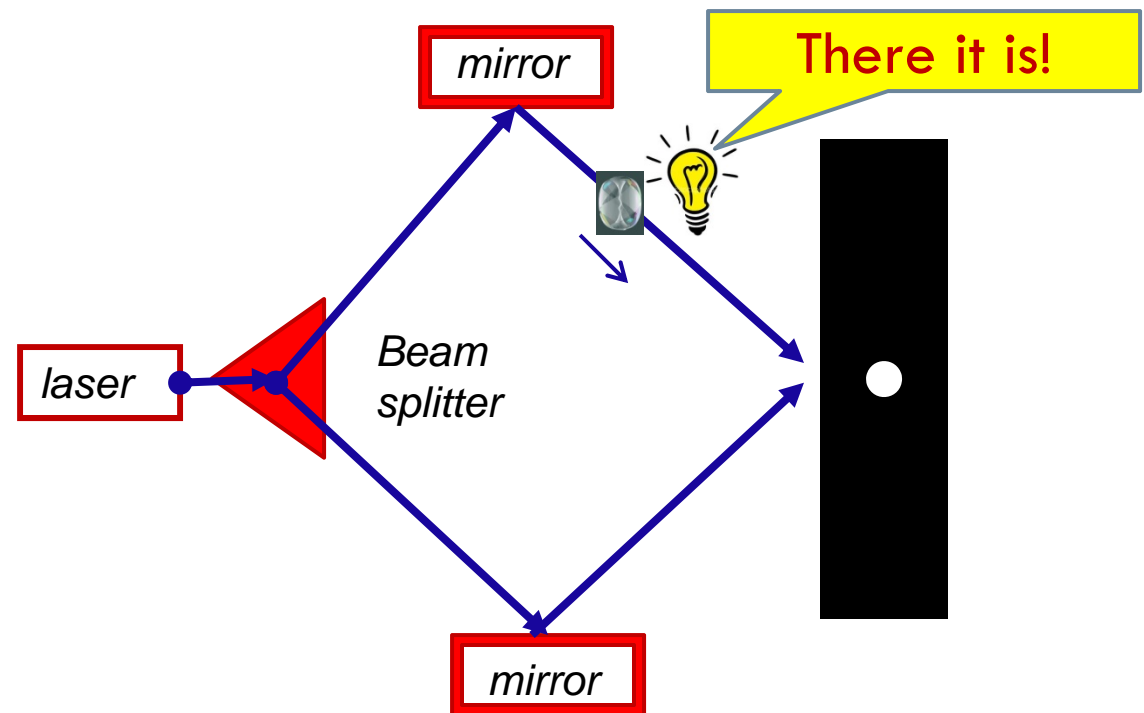
There it is!

laser

Beam
splitter

mirror

☐ …. And it switches to classical behavior!

A *really* peculiar example

- And this is true even if the detector isn't turned on until *after* the photon hits the beam splitter

mirror

There it is!

laser

Beam splitter

mirror

- …. detector "active" $\rightarrow$ classical behavior.
  Switched off and inactive $\rightarrow$ interference!

Weird science

- How about… turn on detector but hide it in a box?
  - This destroys the information about which way the photon went…
    - *and we see an interference pattern*
    - *… open the box and the system becomes classical again*

- What if we use electronics to <u>destroy</u> the reading *after* the photon has already passed the detector?
  - …. Guess what? *Interference pattern reappears*
  - *Isn't this "editing the past"?*

Weird science

- In some sense when we *observe* a system we force it to behave classically.
  - Even if our observation occurs *after* the event that seems to determine classical/quantum behavior!
  - But only observations that actually reach the observer matter.

- So we need to think about the meaning of "information reaching an observer"

Must the observer be a person?

observer

observed

- Actual act of observation occurs when a particle interacts with some other particle

- But apparently, if we don't have a way to know this happened, we didn't observe it!

- Leads to a view in which a system learns something through unbroken chains of events

Decoherence

- When a quantum state collapses into a classical one because of an interaction with the outside world we say it has *decohered*
  - And it won't take long: outside of very careful experiments, most quantum superpositions collapse within 10^{-13} seconds
- But macro-scale quantum effects *do* arise
  - In superconductors and superfluids
  - In analogues of the "Schrödinger's Cat" scenario
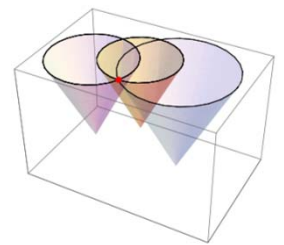
What does it mean to say "X saw Y"?

- This is a statement about something that happened: a measurement

- And it was made at some point in "time"

- Pre-Einstein it seemed obvious that we could do experiments that measure time. For example, could talk about simultaneous events occurring at different places

  - We would say "X happened, and O was watching. When the light from X reached O, O could see that (and when) X happened."

  - We could even claim that "events X and Y happened simultaneously, because O saw them both at the same time."

  - These statements seemed to make sense
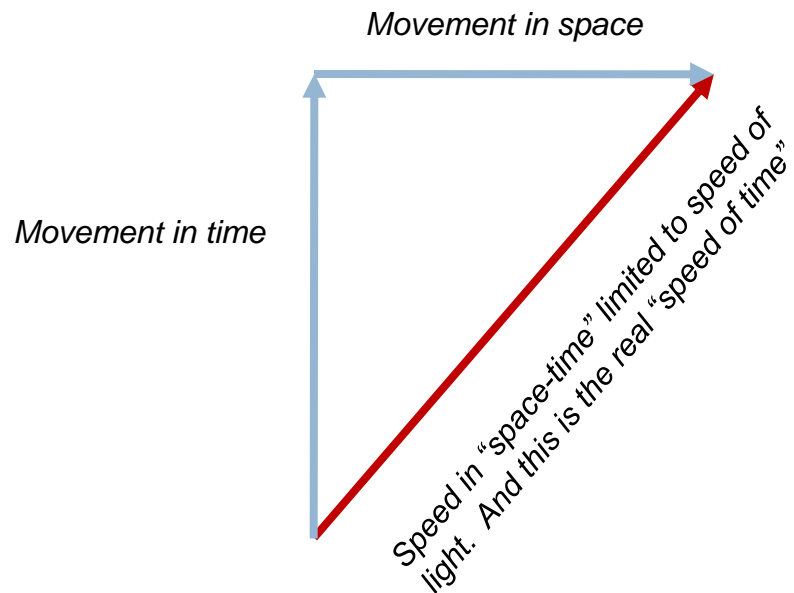
What does it mean to say "X saw Y"?

- Einstein's theory of "relativity" changed that

- He showed that the frame of reference of an observer determines her notion of "time" or of "simultaneous events"
  - A fast observer experiences "slower" time, relative to a slower observer
  - For a photon, all instants are simultaneous

- Time doesn't really exist in the sense that we perceive… reality is actually a series of interacting states
  - Information communicated within "light cones"

Speed of light limit

- Time is best measured in terms of the "real" speed of light, and this speed is the hypotenuse of a triangle

Movement in space

Movement in time

Speed in "space-time" limited to speed of light. And this is the real "speed of time"

- This sheds light (groan) on our experiments
  - A photon (moves at the speed of light) sees no "time" stand still!

Things we can say

- *Time per se may not have any absolute meaning at all.*

- When we talked about deciding whether to turn the detector on "before" or "after" the photon hit the splitter, that comfortable notion isn't a very good way to understand the system

- Better is to think of information moving from place A to place B and not worrying about "when" at all
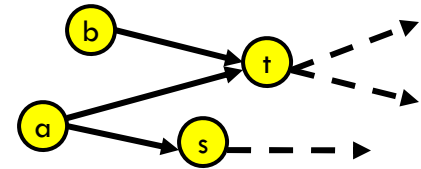
So…

- Part of our confusion is based on accidentally thinking that time was really meaningful

- But "x had an effect on y" *is* meaningful

- Think of an event "x" and an edge from "x" to "y"

How can a photon "interfere" with itself?

- You might have several ideas for explaining this
  - Maybe you doubt the experimental setup. But we can really build experiments this sensitive
  - Perhaps photons are "pure waves"?
    - But this contradicts the single-slit variation. And a famous experiment by Bell rules out some other versions of this idea
- Our single experiment reveals that a photon behaves like *both* a solid little object *and* a probability wave, depending on circumstances
  - Modern thinking: the experiments aren't measuring the identical thing…
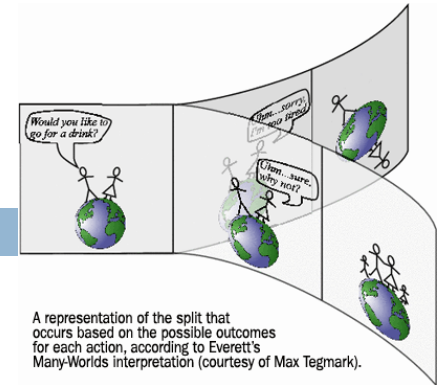
What is the universe?

- Since we can't talk about time except in a relative sense, how can we talk about the universe?

- Think about graphs. We can model the quantum universe as a graph of "states" connected by "state transition" edges.

- From each state there are other reachable states, and probabilities of reaching them
  - Who throws the dice? Maybe the graph is "all there is". Or maybe God does.

Theories of the universe

□ Many-worlds hypothesis:

▪ In this model, the universe is full described by the state space graph we just drew.

▪ The ensemble of universes is what we observe and *we see them all at once*.

   ▪ In any particular path through the state space, events are completely classical, except for the event of "observation"

   ▪ But *one state may be reachable from more than one prior state*, explaining probability interference

▪ No "state" is any more real than any other state. The graph of reachable states is "reality"

What's <u>really</u> going on here?

- Nobody knows. Maybe there is a deeper truth that will explain things better someday.

- But we can still model a quantum "state space"
  - Each state is a (long) vector of complex numbers called "amplitudes." One amplitude for every classical configuration the system can be in
  - To find the absolute probability the system is really in classical state s just compute $(amplitude_s)^2$
  - Insight: "QM is just probability theory with minus signs:"
    - Probabilities are non-negative real numbers
    - Amplitudes are complex numbers: mysterious in a philosophical sense but perfectly reasonable in a formal sense
- States transition to one-another in a graph-like manner.

Schrödinger's equation

Second derivative with respect to X — Shrodinger Wave Function

$$\frac{\partial^2 \psi}{\partial x^2} + \frac{8\pi^2 m}{h^2}(E - V)\psi = 0$$

Position — Energy — Potential Energy

23

- A model predicting evolution of amplitudes
- The mathematics of state evolution in quantum systems

- Curiously, Schrödinger himself wasn't a believer in the many worlds model, yet his equations work just as well in that model as in the model he was more fond of!
  - The math seems to be valid
  - All the rest is just philosophical speculation!

All of these ideas come together…

- … in *quantum computing.*

- Basic idea: manipulate a particle to create a superimposed quantum state

- Now allow that particle to evolve in a way that computes some function on its state

  - Our understanding of the quantum mechanisms (the state space) lets us design this function

  - If we measure the output of the function, it will be a superimposition of all the different results for all the different initial states
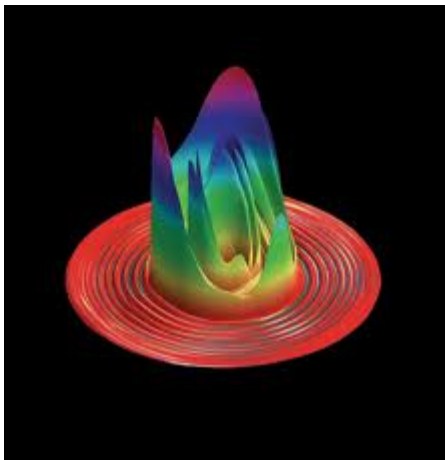
For example

- Suppose that our function computes F(x) = 1/x

- Now suppose that the value of "x" represented with a vector of qbits, and we can set those to 0, 1, or to a superposition of 0 and 1

- Then we can write "multiple values" into x, via superposition… and compute multiple versions of 1/x

  - But better not set x=0.0!

    - 1/x would be undefined.

    - A quantum circuit can't throw exceptions! The "execution" of the function needs to be identical for all the inputs
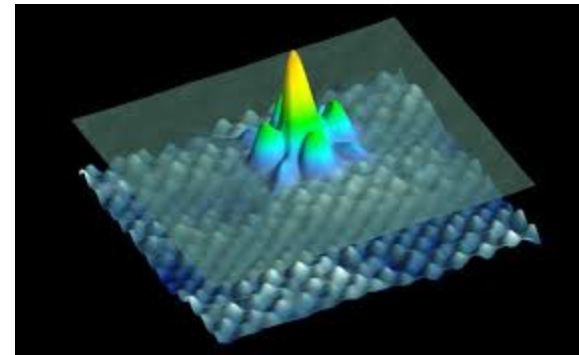
Quantum computing

- A quantum circuit represents the same data but in two equivalent representations

Zero-energy function f

Quantum state of x

Quantum state of f(x)
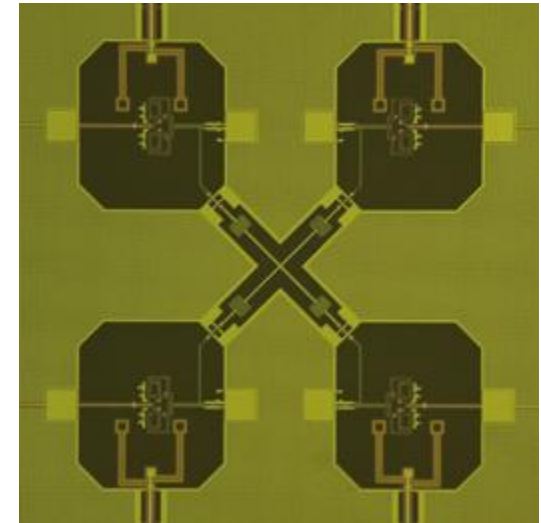
Why a "zero energy" function?

- ☐ If the function somehow dissipates energy, we lose the quantum superposition state (a form of observation that communicates information)

- ☐ Think of a quantum circuit as a single entangled particle in a superimposed (quantum) state

- ☐ We think of x and f(x) as two representations of the same state (like entangled particles)

Quantum noise is an issue

- Decoherence limits time that a qBit can hold it's quantum state

- Remedy seems to be to create circuits with multiple qBits that have entangled states and employ a form of quantum error-correction: even if some circuits decohere, others should still be stable

Reading the answer out?

- This is a difficult issue
  - When you "observe" a quantum state, it collapses: you see just one of its possible configurations
  - So you need to observe it again and again and build up a probability distribution from which you can estimate the output function value
  - Quantum computing isn't like normal computing where you put in the question once and get an answer once. Instead you need to put in a question again and again, and read the answers again and again
  - Like building an interference pattern one dot at a time

Complexity of quantum computing

- Very much like normal complexity
  - Time complexity is defined as usual, although it applies to "paths" through the quantum state space
  - "Error" complexity is often measured in terms of how many times we need to sample the system to get an answer of a given quality
  - "Space" complexity (storage) measures the number of qbits needed, as a function of the problem size.
- They all matter... but of course we want low time complexity (else, why bother?) and small numbers of qBits (they cost a fortune!)

So, are they amazingly powerful?

- Probably, but we're not totally sure
  - For example, the secret to cryptography today is that *factoring very long numbers seems to be hard*
  - With QC factoring becomes very fast
    - Shor's algorithm: factors in time O(1) if you have a fully functional quantum computing system
      - At the core it transforms the problem into an FFT problem, and uses QC to compute the FFT
      - This is *not* the popular science way that QC works but this is the way it actually works! (In science fiction, the QC system "guesses" all possible factors... nope...)

Complexity of quantum computing

- Theoretical work leads to a paradox

  - A quantum computing system could solve problems that are *apparently* very hard with classical computing

    - *But….   Extracting the answer takes so many tries that in fact, the process often ends up being way slower than classical!*

    - Example: today with cutting edge QC we can use Shor's algorithm to factor 15 = 5*3. Just barely.

- But in future may succeed in building QC systems that scale to very large problems.

  - Something to worry about: someday, all our cyptographic keys might suddenly break. Will QC doom security?

Bottom line?

- Nobody has found a provably hard classical problem that is provably easy in QC (yet).
  - For example, Travelling Salesman is NP complete: a "hard" problem, very likely needs exponential time to solve.
  - Nobody knows how to solve the problem faster using QC. "Try all possible paths" is just not the way QC works.

- But QC will probably be a big win once we create real machines and learn more about how to use it
  - Simulating quantum mechanics (obvious choice)
  - Protein folding (many of the same issues arise)

Recap, catch our breath…

- Quantum computing is a new and powerful tool

- But we don't really understand that power yet
  - Like… what in the world is a "quantum state" anyhow?
  - Does anyone throw the dice?

- In fact QM is perhaps less weird than it sounds at first
  - Can't allow faster-than-light communication, or back-in-time
  - Doesn't change the "laws of logic"
  - Waveform collapse doesn't require a *human* observer: any particle or recording device can "observe" a state.
  - What matters to you are past states: observations that sent information to the states you are in
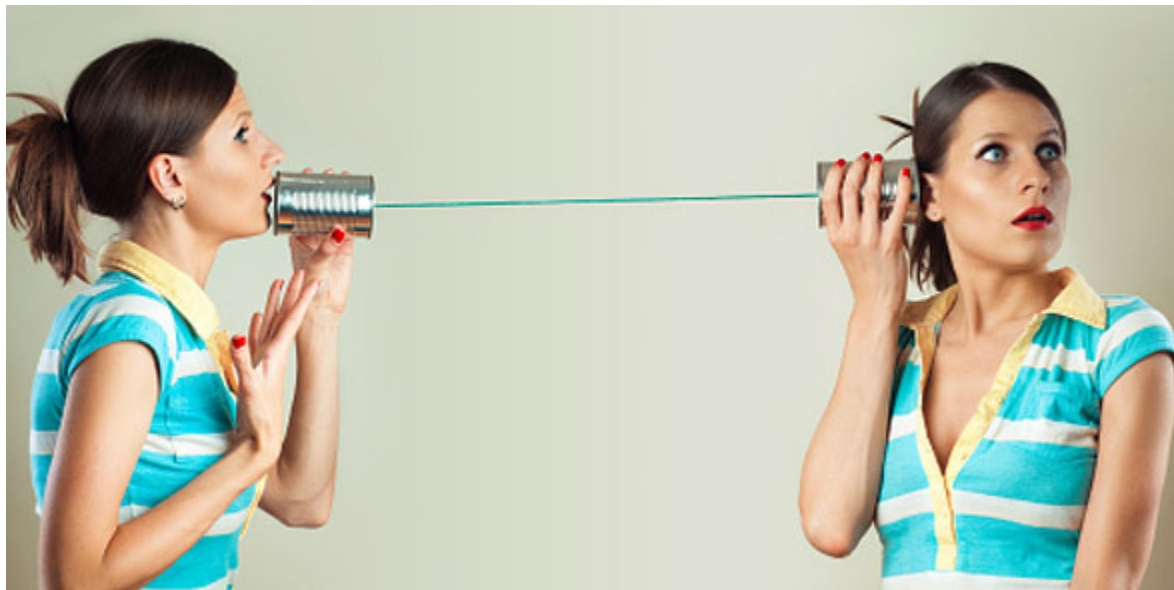
Wave particle duality

- A puzzle… but in retrospect, a digression!
- We stumbled onto the idea of quantum computing from the observation of wave particle duality
    - A historical fact.
- But we don't really need to "answer the question" this duality poses to do QC
    - Quantum computing simply leverages a real property of the universe to compute more than one thing at a time (via transformations on superpositions)
    - All we need is the math

Can quantum computers do other stuff?

- One idea relates to sharing secrets

- Suppose that Sally wants to share a secret with her best friend, Kate. Sam, a nosy guy, wants to snoop.

Sam is trying to eavesdrop

□ Sally's idea: let's "encrypt" our conversation

A great way to encrypt

- Share a secret key that has random 0's and 1's
  - 0101000010111010101010001110101010101010

- Write your message down as 0's and 1's
  - 0101000101010101010100111101010101010101

- Use "xor" to combine message and key
  - $0 \otimes 1 = 1$; $1 \otimes 0 = 1$; $0 \otimes 0 = 0$; $1 \otimes 1 = 0$;
    - Your message looks like random gibberish

- When Kate gets the message she repeats this encryption process with the same key. Out pops the message! Sam learns nothing unless he has the key

But where should the key come from?

- They could agree in advance…
  - … but Sally and Kate talk a lot and would run out of secret keys pretty quickly!
  - Plus, what if Sam somehow gets his hands on the key?

- So pre-agreed keys are a mistake
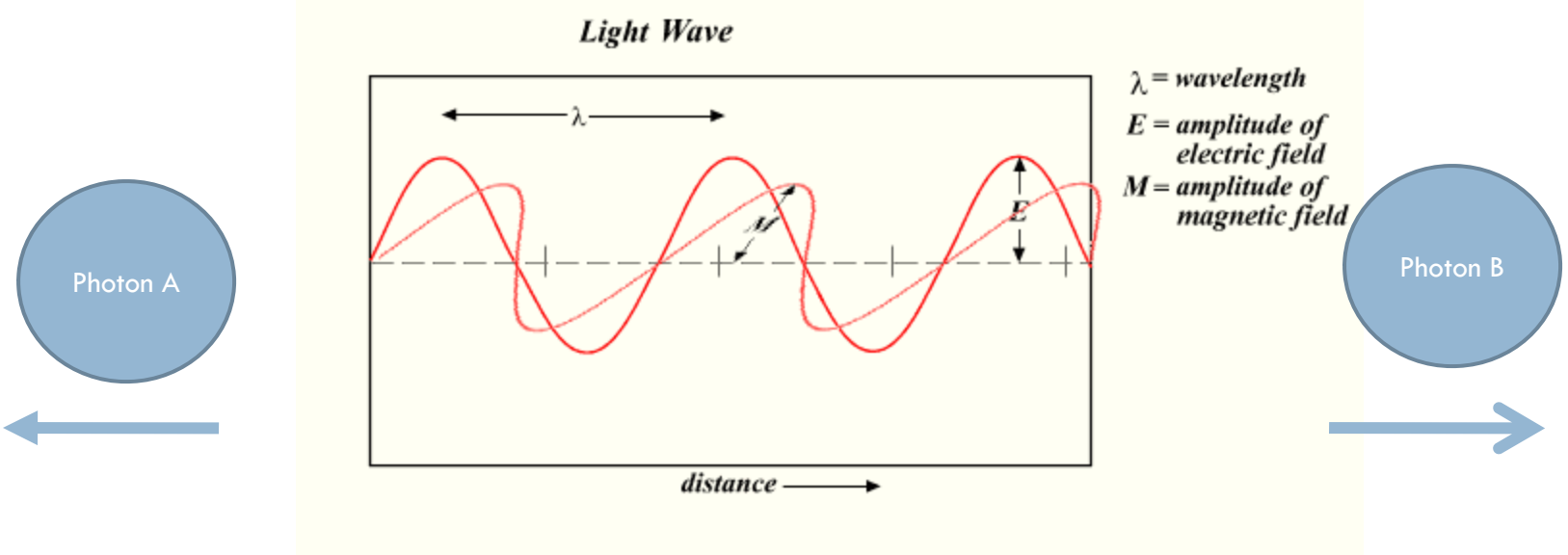
What if Sally could send a key?

☐ How can you send a message that only Kate can receive?

☐ With quantum computing you can do it.

☐ Trick is to use "entanglement"
  ☐ A way to create two particles that behave like one
  ☐ And… head in different directions

Entangled particles

Using entangled particles

- Quantum mechanics tells us that if we measure a property of a particle we see one of its possible states

- But if Sally and Kate measure the same property of these different but entangled photons, *they see the identical observation!*

  - The value wasn't predetermined; experiments prove this
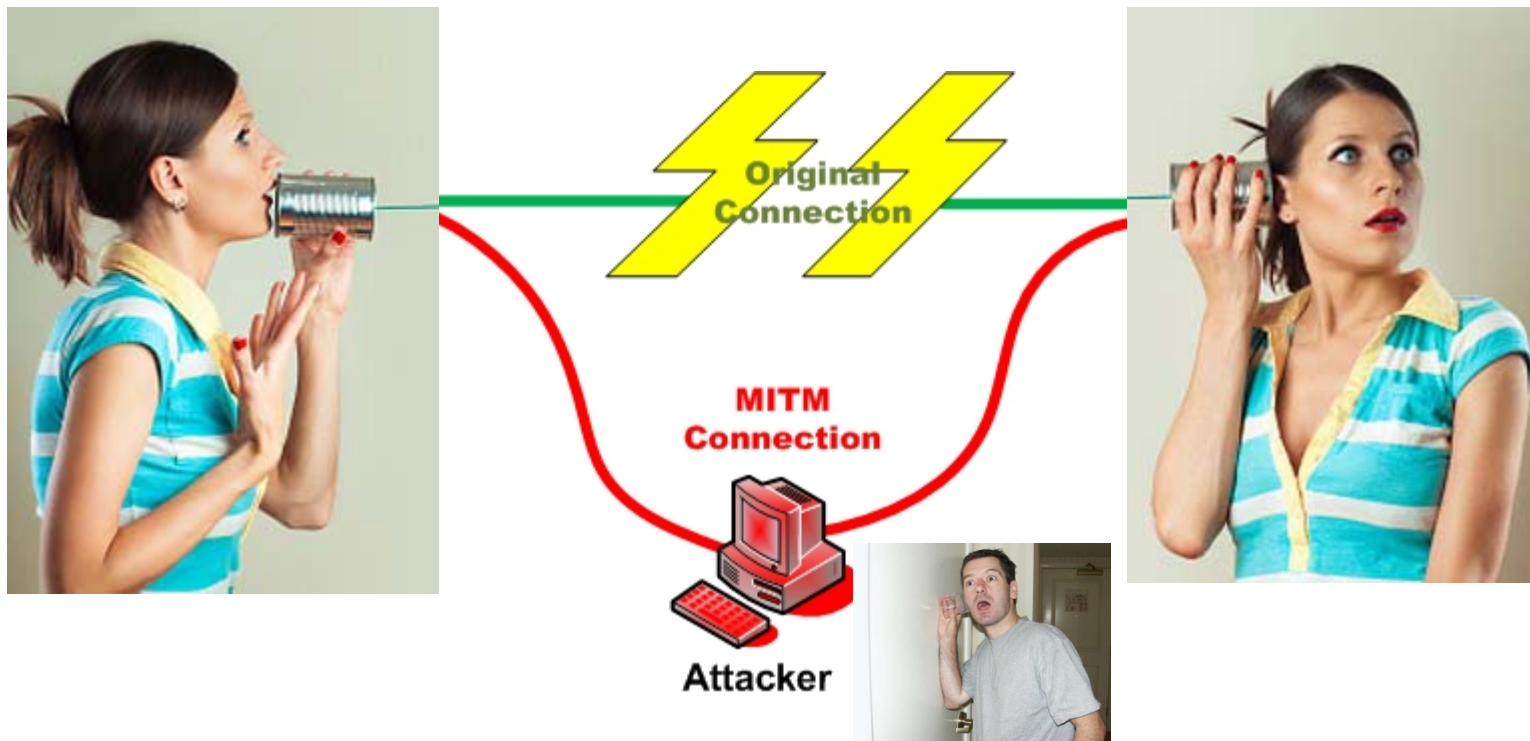 - Yet they always see the exact same result!

So…

- Sally and Kate have a way to create infinite sequences of random bits
  - Each sees the identical values
  - Yet the values were totally unpredictable in advance
- Best of all, if Sam snoops on the entangled photons, he breaks the entanglement property. Sally and Kate just see gibberish and realize that something is wrong

Man in the middle

□ Sam cuts the cable and "relays" data trying to conceal this from Sally and Kate

How a man-in-the-middle works

- Sam cuts the cable, and Sally ends up talking to him, but he relays her message to Kate

- And vice versa.

- They think they are talking to each other, but in fact Sam is seeing every word!

- Can we defeat Sam's evil plot?

Sally and Kate win!

- They take Rafael Pass' course in cryptography and learn to use their entangled data stream in a fancier way.
  - It involves a simple back-and-forth "protocol" in which Sally and Kate make use of additional keys ("public key cryptography")
    - In effect they start with relatively *small* preexisting keys, but use them to generate arbitrarily long shared random bit streams.
    - Arguably these small existing keys can't be avoided: at the digital level they are Sally's and Kate's digital identifiers ("names")
  - *Sam can't defeat that protocol, so he loses the game.*
    - *… unless he can buy (or build) a working quantum computer and crack those public keys!*

Learn more: *Science News, 178:11,* Nov. 20, 2010.

Quantum security in networks

- Companies are selling devices that work offer quantum secrecy for communications
  - They use optical cables to share the secret keys
  - Technique really works over 10km distances or so

- Of course, you also need to trust the software that runs on the computers, and the hardware that those cables connect to!
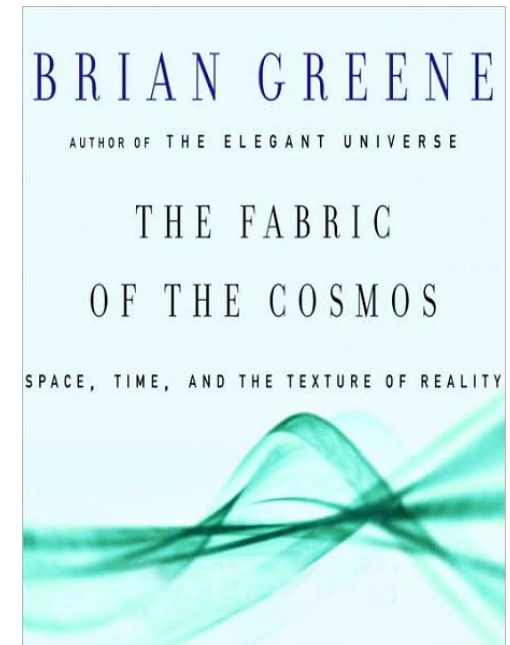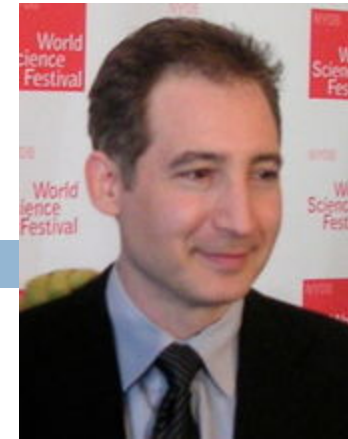
A few quick comments

- Science fiction writers imagine that quantum computing (or some other form of physical computing) might somehow break all classical limits

- This seems not to be possible, but we could be wrong. After all, we've only been in this business for a few years…

- Right now, quantum computing may be most useful for learning more about quantum physics, but as the field matures, we may find other important uses

Learning more

- A fantastic book, very accessible
  - Brian Greene
  - The Fabric of the Cosmos:
    Space, Time and the Texture of Reality

- Learn amazing facts… and some speculation too… like
  - What caused the big bang?
  - How much did the initial universe weigh?
  - And…. *what time is it*, anyhow?

A few other ideas for physical computing

- Even if the O() complexity of hard problems doesn't vanish, what if we could just use massive parallelism from some physical source to solve problems?
  - For example, set up our travelling salesman problem as a huge physical array of beam splitters that also insert polarization (they rotate the optical beam) by precise amounts.
  - Send in a laser beam and watch for first photon with just the right polarization: it visited every "city"
  - Block one edge at a time to recover edges belonging to the winning travelling salesman path
- This has actually been done and it works!
  - But the array itself grows as the problem grows. A complexity issue…

Computing with bacteria

- Recently scientists in Japan showed how to solve a Sudoku puzzle (a small one) using bacteria
    - For an n x n puzzle, they need n^2 bacterial strains
    - So this works… but isn't a very "scalable" solution

- This is just one instance of a major emerging area

- Don't confuse with biological quantum computers, which people are *also* exploring

Physical computing…

- A related idea was to use biological molecules as tiny computers
  - Not QC but exploiting randomization. Similar idea but here the angle is massive parallelism, not one qBit with many states superimposed in it.
- Make them fluoresce to reveal answer, or use a mechanism that destroys the molecules that didn't find the right answer
  - But it was soon shown that the number of molecules needed to read out the answer grows with the size of the question
  - Factoring a tiny number might be easy in a test-tube. But factoring a big one, like an RSA security key with 1024 bits, could take an ocean the size of Jupiter! (And you would need to "find" the molecules that encoded solutions, too)

Physical computing….

- …. can only solve problems if
  - You can find a physical system able to solve the problem
  - The setup won't be so physically huge as to be infeasible
  - The solution won't take so long to read out that it would take just as long as if you used classical methods

Infinite thanks to…

- Our slides today owe a lot to Cornell graduate Scott Aaronson, now a professor at MIT

- Scott (who once took courses like cs2110) went on to become one of a tiny number of experts on quantum computing and other kinds of physical computing

  - Extremely promising area, even if it has many limits

  - Proof that cs2110 can launch you on a path to glory!

- These slides quote Scott once or twice, but they aren't his slides. They reflect Ken's (limited) understanding of this stuff… Check out Scott's web site to see more of what he does. He has a very cool blog! (www.scottaaronson.com)