Quantum Theory

&

Quantum Computation

- *To understand quantum computing, you absolutely must become fluent in the mathematical model.* Michael Nielsen

- *... it is impossible to explain honestly the beauties of the laws of nature in a way that people can feel, without their having some deep understanding of mathematics. I am sorry, but this seems to be the case.* Richard Feynman

- **DON'T PANIC** Douglas Adams. The Hitchhiker's Guide to the Galaxy.

Weird Things in the Quantum World — explanations to follow

1. A quantum bit (qubit) is a superposition of classical bits 0 ($|0\rangle$) and 1 ($|1\rangle$):
   $$\alpha\,|0\rangle + \beta\,|1\rangle, \quad \alpha, \beta \text{ are complex numbers, } |\alpha|^2 + |\beta|^2 = 1.$$
2. Quantum computation relies on superposition and entanglement.
3. A qubit has a (mostly) private/secret world, called state space.
4. After measurement (using a process which always produces states $|0\rangle$ or $|1\rangle$) the above qubit gives value
   - 0 with probability $|\alpha|^2$ and jumps to the state $|0\rangle$,
   - 1 with probability $|\beta|^2$ and jumps to the state $|1\rangle$.
5. Different measurement processes also produce 0 and 1, but with different states after measurement and different probabilities.
6. The qubit "decides" its measurement outcome at the instant of measurement.
7. But if two qubits are entangled and one is taken to Mars, and both are then measured, their measurement outcomes will correlate. This happens even if not enough time at the speed of light to pass information between the two qubits!

Classical Computer

MacBook Pro $> 10^{11}$ bit computer

BIT

- basic unit of information for *classical* computer
- it is called a (classical) bit — from binary digit
- mathematically: value 0 or 1
- physically: current on/off, voltage low/high, orientation in flash memory cells, . . .
- information stored as a sequence of bits, with values 0 or 1
- 16 GB (RAM) has $\approx 16 \times 10^9 \times 8 = 1.28 \times 10^{11}$ bits
- 500 GB hard drive stores $\approx 500 \times 10^9 \times 8 = 4 \times 10^{12}$ bits

Quantum Computer

Google's 53 qubit quantum computer

QUBIT

- basic unit of information for *quantum* computer
- qubit — from quantum bit (as compared with a classical bit)
- mathematically: a qubit is a type of *complex superposition* of the bits 0 and 1 — soon to be discussed (Weird fact no. 1)
- physically: energy levels of atom, spin of atom, polarisation of photon (light), . . .

Quantum Supremacy?

- Google announces “quantum supremacy” 23 October 2019 with its 53 qubit computer (IBM quibbles)
- Bigger quantum computers could break RSA and elliptic curve cryptography
    - Need $\approx$ 4000 qubits to break 2048-bit RSA, i.e. 617 digits. Another 20 years?
- Modelling physical processes at quantum level
    - e.g. protein folding, too difficult for classical computers
- Quantum computation relies on *superposition* and *entanglement* (Weird no. 2)
- Entanglement not stable, due to *decoherence* – interaction with environment.
    - Minimising decoherence is a very difficult engineering & mathematical problem.

Superposition 1

If you think you understand quantum mechanics, you don't understand quantum mechanics Richard Feynman

Here I always use a *fixed* measurement process to read the value of qubits. (More on this later.)

- A qubit has a (mostly) private/secret world, called *state space* (Weird no. 3)
  - we refer to the "*state*" of the qubit
- "Measuring" a qubit always gives one of two values, usually labelled 0 and 1.
- The qubit state determines the *probability* of 0 or 1, not the actual value.
  - see next slide!
  - think of running the same experiment with the same qubit state 1000 times
- However, one particular quantum state *always* gives 0.
  - this state is written $|0\rangle$ and corresponds to the "classical" bit 0
- Another quantum state *always* gives 1
  - this state is written $|1\rangle$ and corresponds to the "classical" bit 1
- The most general quantum state for a qubit is a *superposition* of $|0\rangle$ and $|1\rangle$:

  $$\alpha\,|0\rangle + \beta\,|1\rangle\,, \quad \text{where } \alpha, \beta \in \mathbb{C}, \quad |\alpha|^2 + |\beta|^2 = 1. \qquad \text{(Weird no. 1)}$$
  - (remember: if $\alpha = x + iy$ then $|\alpha|^2 = x^2 + y^2$.)

Superposition 2

Remember: we are working with some *fixed* manner/direction of measurement

- In general, the quantum state for a qubit is a *superposition* of $|0\rangle$ and $|1\rangle$
  $$\alpha\,|0\rangle + \beta\,|1\rangle\,, \quad \text{where } \alpha, \beta \in \mathbb{C}, \quad |\alpha|^2 + |\beta|^2 = 1.$$
- It is possible to prepare 1000 qubits all in the same state
- If a qubit in the state $\alpha\,|0\rangle + \beta\,|1\rangle$ is measured, then
  - value will be 0 with probability $|\alpha|^2$, 1 with probability $|\beta|^2$
  - after measurement the qubit's state immediately changes to $|0\rangle$ or $|1\rangle$ respectively (Weird no. 4)
- Examples
  - *Discuss*: What happens if a qubit in state $\frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle$ is measured?
  - *Discuss*: In the state $\frac{3}{5}\,|0\rangle + \frac{4}{5}\,|1\rangle$? In the state $\frac{3}{5}\,|0\rangle - i\frac{4}{5}\,|1\rangle$?
  - *Discuss*: What happens if we again measure the qubit in the same manner/direction? And again?
- Measurement in a different manner/direction changes the probabilities and the new state after measurement. There are precise formulae for this. (Weird no. 5)

Could we avoid using probabilities if we had more information?

NUP

- The qubit does not “know” which value it will take until the instant of measurement. (Weird no. 6)
- Weird — But perhaps if we had more information?
- *God does not play dice with the universe*: Albert Einstein.
  - PS: “God” as metaphor, Einstein emphasized he did not believe in a personal God.
- However, John Bell designed an experiment that showed: it *cannot* be determined/known before measurement what the measurement result will be.

Entanglement

- We have seen 5 weird things for just a *single* qubit.
- With two (or more) qubits it gets much weirder.
- The simplest states for a single pair of qubits are

  $$|0\rangle\,|0\rangle\,,\ \ |0\rangle\,|1\rangle\,,\ \ |1\rangle\,|0\rangle\,,\ \ |1\rangle\,|1\rangle; \qquad \text{written } |00\rangle\,,|01\rangle\,,|10\rangle\,,|11\rangle.$$

  $|10\rangle$ means the first (Alice's) qubit is $|1\rangle$ and the second (Bob's) is $|0\rangle$, etc. Each of these is a "product" state and is not entangled.
- In general, the quantum state for a pair of qubits is a *superposition*

  $$\alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle\,,$$

  where $\alpha, \beta, \gamma, \delta \in \mathbb{C}$, $\quad |\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1.$
- *Bell state*: $\frac{1}{\sqrt{2}}\,|0\rangle\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle\,|1\rangle$. Bob and Alices' qubits are *entangled*.
  - If Bob takes his qubit to Mars (or another galaxy) — the qubits can remain entangled.
  - If either measures their qubit and gets 0 (or 1) then the other will get same 0 (or 1)
  - This happens even if not enough time at the speed of light to pass information between the two qubits! (Weird no. 7)

Entanglement

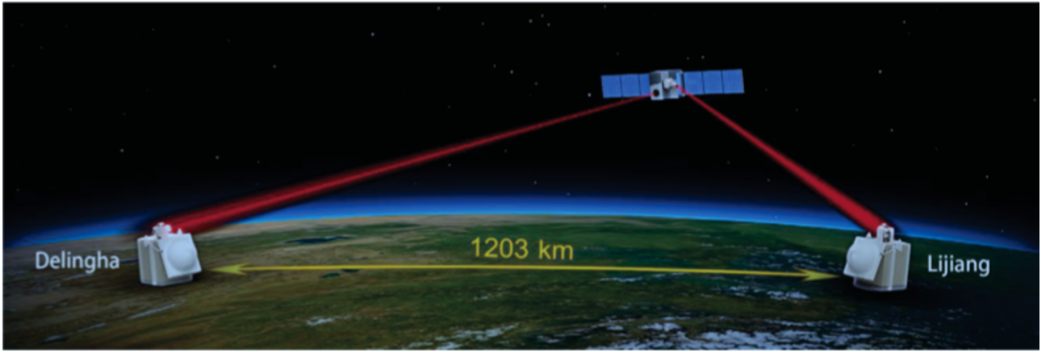

Figure: Experimental set-up of satellite-based entanglement distribution. China 2017.

In this experiment, entanglement was shown over 1200 km.

Shor's Algorithm 1

To break RSA, need to factor large integers such as N with n digits, think of $n = 1000$ and $N \approx 10^{1000}$.

- Classical computer can only do this in a time which grows roughly like $\sqrt[3]{N}$
  - For N as above, $\sqrt[3]{N} \approx 10^{333}$ ($>>$ picoseconds in lifetime of universe! (picosecond $= 10^{-12}$ second)
- Peter Shor, 1994, proved a quantum computer can factor N in a time which grows roughly like n^2
  - For N as above, $n \approx 1000^2 = 10^6$, i.e. almost "nothing".
- This is, at least initially, why governments are putting billions into quantum computing.

Shor's Algorithm 2

Shor's algorithm is not easy. Can only give outline how it works.

We want to factorise large $N = pq$ (two prime factors) with $n = 1000$ digits, say.

- A quantum computer *cannot* just try all possible factors (i.e. $< \sqrt{N}$) "in parallel".
  - This is a common misconception in the news.
  - Need to be much more subtle.
- Fact: by some number theory, one way to factor N is the following
  1. for an arbitrarily chosen integer x, compute x^s mod N for $s = 1, 2, 3, \ldots$
  2. find s such that $x^s = 1$ mod N
  3. after a "small" number of steps, information achieved this way leads to factors of N.
  4. the problem is that for classical computer no. of calculations in Step 2 grows like N.
- A quantum computer can do Step 2 with, say, $10n$ qubits and a fixed number of steps
  - Suppose N can be expressed with b binary digits ($b < 4n = 4,000$ here, why?)
  - Put each qubit in the superposition $\frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle$
  - The first two qubits together will be in the superposition

$$\frac{1}{\sqrt{4}} \big(|00\rangle + |00\rangle + |00\rangle + |00\rangle \big), \text{ etc.}$$

Shor's Algorithm 3

1. Recall, N is expressed with b *binary* bits
    - $b < 4n = 4,000$ here. *Why?*
2. *Enormous Superposition*:
    - The first three qubits together will be in the superposition,
      $$\tfrac{1}{\sqrt{8}}\big(\,|000\rangle + |001\rangle + |010\rangle + |011\rangle + \cdots + |111\rangle\,\big)$$
    - All b qubits together give a superposition of $0, 1, 2, 3, \ldots, 2^b - 1$
    - Relabelling and restricting a little gives a superposition
      $$\tfrac{1}{\sqrt{N}}\big(\,|1\rangle + |2\rangle + \cdots + |N\rangle\,\big)$$
3. *Enormous Entangled Superposition*
    - Pick a *random* number $x < N$ and use a quantum computer to compute
      $$\frac{1}{\sqrt{N}}\Big(\,|1, x\rangle + \big|2, x^2 \bmod N\big\rangle + \big|3, x^3 \bmod N\big\rangle + \cdots + \big|N, x^N \bmod N\big\rangle\Big)$$
    - This uses the facts:
        - One can efficiently compute *individual* powers mod N with a classical computer.
        - A quantum computer can then do the same for a *superposition* of powers.

Shor's Algorithm 4

4. Use the *Quantum Fast Fourier Transform* to find k such that $x^k = 1 \bmod N$.
   - This is called *period finding*. Using the Quantum Fast Fourier Transform is subtle.
   - The fact there *is* such a k where $1 \leq k \leq N$ uses some algebra.
5. *If* we are lucky and k is even, then
   $$0 = x^k - 1 = (x^{k/2} - 1)(x^{k/2} + 1) \bmod N.$$
   If we are again lucky, neither $x^{k/2} - 1$ nor $x^{k/2} + 1$ are multiples of N.
   One can prove we will be lucky at least $3/8$ of time. So just keep trying!
6. After a few tries we obtain "good" x, and so the product $(x^{k/2} - 1)(x^{k/2} + 1)$ is divisible by N but neither factor is itself divisible by N.
   Hence p divides one factor and q divides the other.
   Computing $\gcd(x^{k/2} - 1, N)$ now gives either p or q.

So we have factored N and cracked RSA.