What is this Quantum thing people keep talking about?

Joran van Apeldoorn

Instituut voor Informatierecht
Institute for Information Law

QuSoft
Research Center for Quantum Software

October 12, 2021

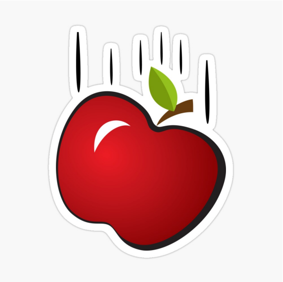
Modern physics

Three scales of the universe

Modern physics

Three scales of the universe

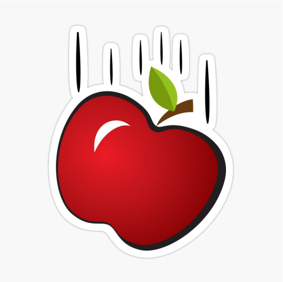
- Classical/Newtonian physics: world around us.
  Mostly found by Newton in 17th century.



Modern physics

Three scales of the universe

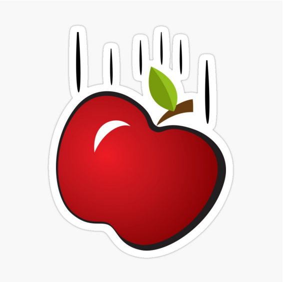
- Classical/Newtonian physics: world around us.
  Mostly found by Newton in 17th century.
- Relativity: Really fast and really big things.
  Early 20 century by Einstein.

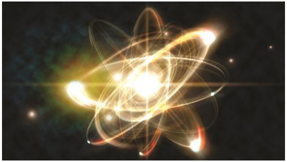


Modern physics

Three scales of the universe

- Classical/Newtonian physics: world around us.
  Mostly found by Newton in 17th century.
- Relativity: Really fast and really big things.
  Early 20 century by Einstein.
- Quantum mechanics: Really small things.
  Early 20 century collaboration between many people.



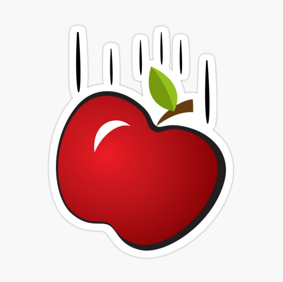


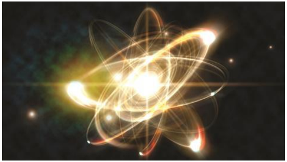
Modern physics

Three scales of the universe

- Classical/Newtonian physics: world around us.
  Mostly found by Newton in 17th century.
- Relativity: Really fast and really big things.
  Early 20 century by Einstein.
- Quantum mechanics: Really small things.
  Early 20 century collaboration between many people.

The later two are more general than classical physics.





Quantum computing?

Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy.
– Richard Feynman

Computational model

Computational model

Basic overview - Superposition

Basic unit is a Qubit

- Two base states: $|0\rangle$ & $|1\rangle$.

Basic overview - Superposition

Basic unit is a Qubit

- Two base states: $|0\rangle$ & $|1\rangle$.
- In general in some superposition of both:

$$\alpha |0\rangle + \beta |1\rangle$$

- If we measure/look at it we find only one outcome randomly.

Basic overview - Superposition

Basic unit is a Qubit

- Two base states: $|0\rangle$ & $|1\rangle$.
- In general in some superposition of both:

$$\alpha |0\rangle + \beta |1\rangle$$

  where amplitudes $\alpha, \beta \in \mathbb{C}$.
- If we measure/look at it we find only one outcome randomly.

$$Pr[0] = |\alpha|^2, Pr[1] = |\beta|^2$$

Basic overview - Superposition

Basic unit is a Qubit

- Two base states: $|0\rangle$ & $|1\rangle$.
- In general in some superposition of both:

$$\alpha |0\rangle + \beta |1\rangle$$

  where amplitudes $\alpha, \beta \in \mathbb{C}$.
- If we measure/look at it we find only one outcome randomly.

$$Pr[0] = |\alpha|^2, Pr[1] = |\beta|^2$$

- A qubit state is a (unit) vector in $\mathbb{C}^2$.

Basic overview - Superposition

Basic unit is a Qubit

- Two base states: $|0\rangle$ & $|1\rangle$.
- In general in some superposition of both:

$$\alpha |0\rangle + \beta |1\rangle$$

  where amplitudes $\alpha, \beta \in \mathbb{C}$.
- If we measure/look at it we find only one outcome randomly.

$$Pr[0] = |\alpha|^2, Pr[1] = |\beta|^2$$

- A qubit state is a (unit) vector in $\mathbb{C}^2$.
- Takeaway: Amplitudes are like probabilities but can be negative.

Basic overview - Interference

- Amplitudes can cancel each other out or strengthen each other.

Basic overview - Interference

- Amplitudes can cancel each other out or strengthen each other.
- Quantum algorithms cancel the unwanted stuff and strengthen the wanted stuff.

Basic overview - More qubits

- What happens is you have multiple (say n) qubits?

Basic overview - More qubits

- What happens is you have multiple (say n) qubits?
- You get a superposition over all possible classical states:

$$\alpha_{000} |000\rangle + \alpha_{001} |001\rangle + \cdots + \alpha_{111} |111\rangle$$

Basic overview - More qubits

- What happens is you have multiple (say n) qubits?
- You get a superposition over all possible classical states:

$$\alpha_{000} |000\rangle + \alpha_{001} |001\rangle + \cdots + \alpha_{111} |111\rangle$$

- There are 2^n possible classical states.
- So a single n-qubit state has 2^n amplitudes.

Basic overview - More qubits

- What happens is you have multiple (say n) qubits?
- You get a superposition over all possible classical states:

$$\alpha_{000} |000\rangle + \alpha_{001} |001\rangle + \cdots + \alpha_{111} |111\rangle$$

- There are 2^n possible classical states.
- So a single n-qubit state has 2^n amplitudes.
- If we measure we only see n classical bits, but until then all possibilities can interfere.

Basic overview - More qubits

- What happens is you have multiple (say n) qubits?
- You get a superposition over all possible classical states:

$$\alpha_{000} |000\rangle + \alpha_{001} |001\rangle + \cdots + \alpha_{111} |111\rangle$$

- There are 2^n possible classical states.
- So a single n-qubit state has 2^n amplitudes.
- If we measure we only see n classical bits, but until then all possibilities can interfere.
- Some correlations do not happen in classical probabilities:

$$\sqrt{1/2}\,|00\rangle + \sqrt{1/2}\,|11\rangle$$

This is entanglement.

Simulation

- Quantum computers can simulate quantum mechanics.
- Possible applications in:
  - Medicine
  - Chemistry
  - Material sciences
  - Fundamental physics

Simulation

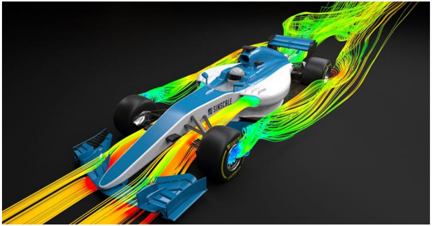
- Quantum computers can simulate quantum mechanics.
- Possible applications in:
  - Medicine
  - Chemistry
  - Material sciences
  - Fundamental physics
- Simulation does not solve everything.

Simulation

- Quantum computers can simulate quantum mechanics.
- Possible applications in:
  - Medicine
  - Chemistry
  - Material sciences
  - Fundamental physics
- Simulation does not solve everything.

Simulation

- Quantum computers can simulate quantum mechanics.
- Possible applications in:
  - Medicine
  - Chemistry
  - Material sciences
  - Fundamental physics
- Simulation does not solve everything.



Period finding & Breaking RSA

Given a way to compute a k-periodic function f, can you find the period?

Period finding & Breaking RSA

Given a way to compute a k-periodic function f, can you find the period?

- Classically: keep checking values until you find a repetition $\rightarrow O(k)$

Period finding & Breaking RSA

Given a way to compute a k-periodic function f, can you find the period?

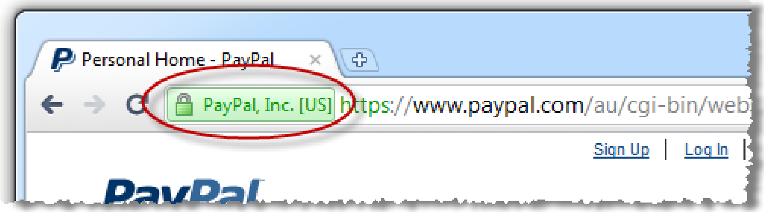
- Classically: keep checking values until you find a repetition $\rightarrow O(k)$
- Quantum using Shor's algorithm: superposition over values and apply a Quantum Fourier Transform $\rightarrow O(\log(k))$

Period finding & Breaking RSA

Given a way to compute a k-periodic function f, can you find the period?

- Classically: keep checking values until you find a repetition $\rightarrow O(k)$
- Quantum using Shor's algorithm: superposition over values and apply a Quantum Fourier Transform $\rightarrow O(\log(k))$

Big application: factoring large integers & breaking RSA encryption.



Grover search

Can we use superposition to search exponentially faster?

Grover search

Can we use superposition to search exponentially faster?
No.

Grover search

Can we use superposition to search exponentially faster?
No.

- Measuring a large superposition just gives one possibility, might not be the correct one.

Grover search

Can we use superposition to search exponentially faster?
No.

- Measuring a large superposition just gives one possibility, might not be the correct one.
- You can improve quadraticly. Quantum computing is linear in the amplitudes, while classical computing is linear in probabilities.

Grover search

Can we use superposition to search exponentially faster?
No.

- Measuring a large superposition just gives one possibility, might not be the correct one.
- You can improve quadraticly. Quantum computing is linear in the amplitudes, while classical computing is linear in probabilities.
- If some algorithm has probability p of success:
  - Classical: Use $O(1/p)$ repetitions.
  - Quantum: Use $O(1/\sqrt{p})$ repetitions.

Grover search

Can we use superposition to search exponentially faster?
No.

- Measuring a large superposition just gives one possibility, might not be the correct one.
- You can improve quadraticly. Quantum computing is linear in the amplitudes, while classical computing is linear in probabilities.
- If some algorithm has probability p of success:
  - Classical: Use $O(1/p)$ repetitions.
  - Quantum: Use $O(1/\sqrt{p})$ repetitions.
- Most versatile quantum algorithm:
  - Search N things in $O(\sqrt{N})$ operations.

Grover search

Can we use superposition to search exponentially faster?
No.

- Measuring a large superposition just gives one possibility, might not be the correct one.
- You can improve quadraticly. Quantum computing is linear in the amplitudes, while classical computing is linear in probabilities.
- If some algorithm has probability p of success:
  - Classical: Use $O(1/p)$ repetitions.
  - Quantum: Use $O(1/\sqrt{p})$ repetitions.
- Most versatile quantum algorithm:
  - Search N things in $O(\sqrt{N})$ operations.
  - Maximum over N numbers in $O(\sqrt{N})$ operations.

Grover search

Can we use superposition to search exponentially faster?
No.

- Measuring a large superposition just gives one possibility, might not be the correct one.
- You can improve quadraticly. Quantum computing is linear in the amplitudes, while classical computing is linear in probabilities.
- If some algorithm has probability p of success:
  - Classical: Use $O(1/p)$ repetitions.
  - Quantum: Use $O(1/\sqrt{p})$ repetitions.
- Most versatile quantum algorithm:
  - Search N things in $O(\sqrt{N})$ operations.
  - Maximum over N numbers in $O(\sqrt{N})$ operations.
  - Easy to apply to graph algorithms, NP-hard problems, optimization, ect.

Errors

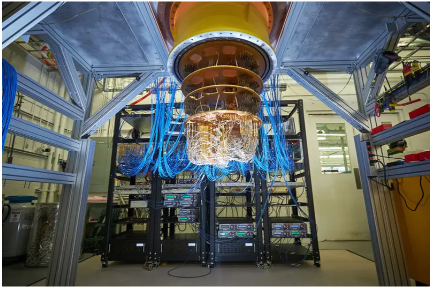
- You meed to isolate quantum systems really well.

Errors

- You meed to isolate quantum systems really well.
- Small interactions are like accidental measurements and destroy the state.

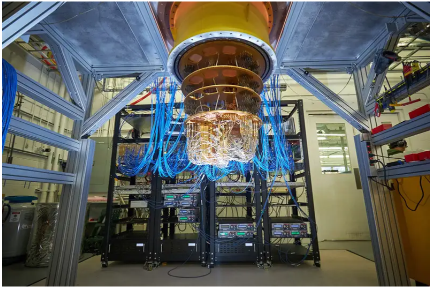
Errors

- You meed to isolate quantum systems really well.
- Small interactions are like accidental measurements and destroy the state.
- This is really hard to do!



Errors

- You meed to isolate quantum systems really well.
- Small interactions are like accidental measurements and destroy the state.
- This is really hard to do!
- Luckily there is error correction:
  use multiple physical qubits to create a logical qubit.



Errors

- You meed to isolate quantum systems really well.
- Small interactions are like accidental measurements and destroy the state.
- This is really hard to do!
- Luckily there is error correction:
  use multiple physical qubits to create a logical qubit.
- Roughly factor 1000 overhead. We now have ≈ 100 physical qubits on the same chip.