Quantum Computing: A Candidate for Future Technological Revolution

Robin Luo
Supervisor: **John C.S. Lui**
September 5, 2024

香港中文大學
The Chinese University of Hong Kong

Table of Contents

1 Introduction

▶ Introduction

▶ Bell's Game

▶ Applications and Future of Quantum Computing

▶ Conclusion and Takeaways

▶ Reference

What is Quantum Computing?

- Quantum computing uses the principles of quantum mechanics to perform complex calculations much faster than traditional computers. It is a multidisciplinary field comprising aspects of computer science, physics, and mathematics.

What is Quantum Computing?

- Quantum computing uses the principles of quantum mechanics to perform complex calculations much faster than traditional computers. It is a multidisciplinary field comprising aspects of computer science, physics, and mathematics.
- Unlike classical computers that use bits to represent information as either 0 or 1, quantum computers use quantum bits, or qubits. Due to the quantum property of superposition, a qubit can exist simultaneously in a state of $|0\rangle$, $|1\rangle$, or any superposition of these states.
- Imagine a qubit like a spinning coin that can be in a state of heads (0), tails (1), or any mixture of both while it's spinning. This allows quantum computers to perform multiple calculations at once, potentially solving problems faster than classical computers.

What is Quantum Computing?

- Quantum computing uses the principles of quantum mechanics to perform complex calculations much faster than traditional computers. It is a multidisciplinary field comprising aspects of computer science, physics, and mathematics.
- Unlike classical computers that use bits to represent information as either 0 or 1, quantum computers use quantum bits, or qubits. Due to the quantum property of superposition, a qubit can exist simultaneously in a state of $|0\rangle$, $|1\rangle$, or any superposition of these states.
- Imagine a qubit like a spinning coin that can be in a state of heads (0), tails (1), or any mixture of both while it's spinning. This allows quantum computers to perform multiple calculations at once, potentially solving problems faster than classical computers.
- Another crucial property of qubits is entanglement, where two qubits become intertwined such that the state of one qubit directly affects the state of the other, no matter how far apart they are.

What is Quantum Computing?

1 Introduction

- Quantum computing uses the principles of quantum mechanics to perform complex calculations much faster than traditional computers. It is a multidisciplinary field comprising aspects of computer science, physics, and mathematics.
- Unlike classical computers that use bits to represent information as either 0 or 1, quantum computers use quantum bits, or qubits. Due to the quantum property of superposition, a qubit can exist simultaneously in a state of $|0\rangle$, $|1\rangle$, or any superposition of these states.
- Imagine a qubit like a spinning coin that can be in a state of heads (0), tails (1), or any mixture of both while it's spinning. This allows quantum computers to perform multiple calculations at once, potentially solving problems faster than classical computers.
- Another crucial property of qubits is entanglement, where two qubits become intertwined such that the state of one qubit directly affects the state of the other, no matter how far apart they are.
- Similar to how classical computers use logic gates (AND, OR, NOT) to manipulate bits, quantum computers use quantum gates to operate on qubits. However, quantum gates can create and manipulate superpositions and entanglement, enabling more complex and powerful computations.

Why is it Exciting?

Revolutionizing Cryptography

- Quantum computers could potentially break current cryptographic systems and revolutionize data security.
  - Classical cryptographic techniques heavily rely on solving a complex math problem, e.g., factoring a large number.
  - Shor's algorithm, developed by Peter Shor in 1994, can factor integers in polynomial time, which is exponentially faster than the best-known classical algorithms.

Why is it Exciting?

Revolutionizing Cryptography

- Quantum computers could potentially break current cryptographic systems and revolutionize data security.
  - Classical cryptographic techniques heavily rely on solving a complex math problem, e.g., factoring a large number.
  - Shor's algorithm, developed by Peter Shor in 1994, can factor integers in polynomial time, which is exponentially faster than the best-known classical algorithms.
- Quantum cryptography offers new methods of secure communication, such as Quantum Key Distribution (QKD), which is theoretically immune to hacking.

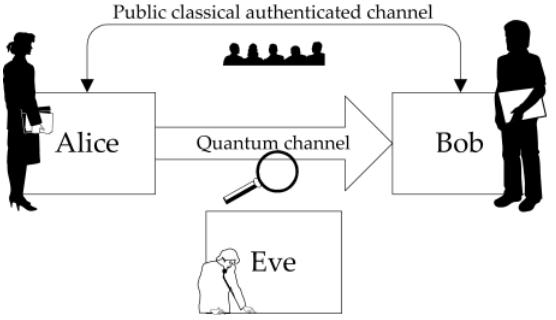


Figure: Any attempt to intercept the key would have been detected!

Why is it Exciting?

Quantum Supremacy

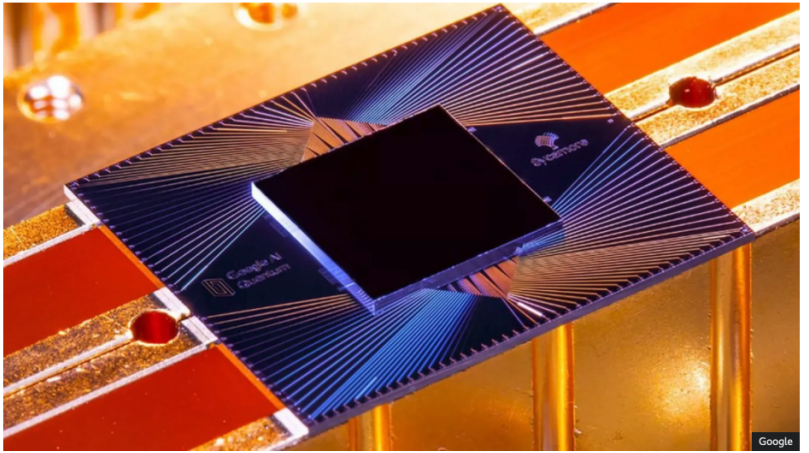
- On 23 October 2019, Google published a paper claiming quantum supremacy.

Google claims 'quantum supremacy' for computer

23 October 2019

Share

Paul Rincon
Science editor, BBC News website



Why is it Exciting?

Nobel Prize in Physics 2022

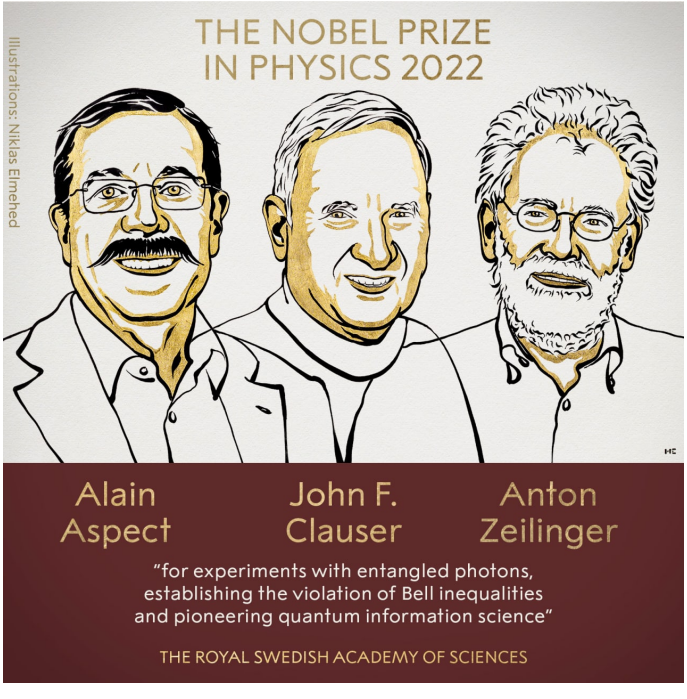


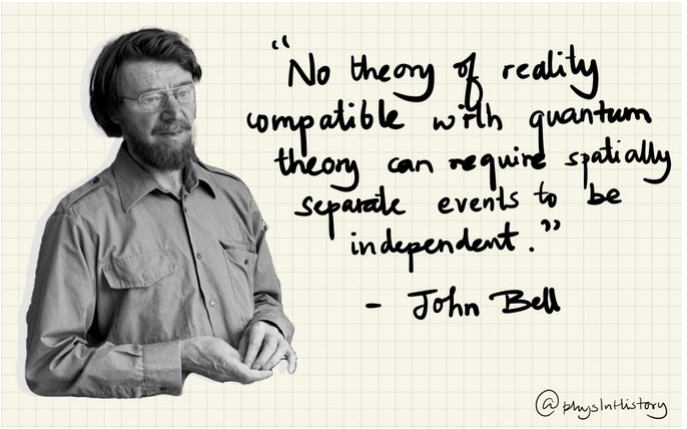
Table of Contents

2 Bell's Game

- Introduction
- Bell's Game
- Applications and Future of Quantum Computing
- Conclusion and Takeaways
- Reference

Introduction to Bell's Game

- Bell's game, often referred to as the CHSH (Clauser-Horne-Shimony-Holt) game, is a thought experiment in quantum mechanics used to illustrate the concept of quantum entanglement and the violation of Bell's inequalities.
- It is based on a famous result by John Bell, which shows that certain predictions of quantum mechanics cannot be reproduced by any local hidden variable theory, thus challenging classical intuitions about the nature of reality.



Setup of the Game

- One referee plays a game with two cooperating but separated players: Alice and Bob.
- Referee flips two coins to get random bits $x, y \in \{0, 1\}$.
- Alice receives an input $x \in \{0, 1\}$.
- Bob receives an input $y \in \{0, 1\}$.
- Alice and Bob need to output a and b respectively without any communication, where $a, b \in \{0, 1\}$.
- They win the game if $x \cdot y = a \oplus b$ (where $\oplus$ denotes XOR).
  - $0 \oplus 0 = 0$, $1 \oplus 0 = 1$, $0 \oplus 1 = 1$, and $1 \oplus 1 = 0$.

Classical vs. Quantum Strategy

- Analysis on the game:
  - When $x = 0$ and $y = 0$, the winning condition is $a = b$.
  - When $x = 0$ and $y = 1$, the winning condition is $a = b$.
  - When $x = 1$ and $y = 0$, the winning condition is $a = b$.
  - When $x = 1$ and $y = 1$, the winning condition is $a \neq b$.
- What is the maximum win probability for Alice and Bob? How to achieve that probability?

Classical vs. Quantum Strategy

- Analysis on the game:
  - When $x = 0$ and $y = 0$, the winning condition is $a = b$.
  - When $x = 0$ and $y = 1$, the winning condition is $a = b$.
  - When $x = 1$ and $y = 0$, the winning condition is $a = b$.
  - When $x = 1$ and $y = 1$, the winning condition is $a \neq b$.
- What is the maximum win probability for Alice and Bob? How to achieve that probability?
- Classical strategy:
  - Deterministic: 75%.
  - Private randomness: 75%.
  - Shared randomness: 75%.
  - follows Bell's inequality

Classical vs. Quantum Strategy

- Analysis on the game:
  - When $x = 0$ and $y = 0$, the winning condition is $a = b$.
  - When $x = 0$ and $y = 1$, the winning condition is $a = b$.
  - When $x = 1$ and $y = 0$, the winning condition is $a = b$.
  - When $x = 1$ and $y = 1$, the winning condition is $a \neq b$.
- What is the maximum win probability for Alice and Bob? How to achieve that probability?
- Classical strategy:
  - Deterministic: 75%.
  - Private randomness: 75%.
  - Shared randomness: 75%.
  - follows Bell's inequality
- Quantum strategy:
  - Shared quantum entanglement: $(\cos \frac{\pi}{8})^2 \approx 85\%$.
  - [Boris, 1980] proves that the quantum strategy is optimal.
  - violates Bell's inequality.

Classical vs. Quantum Strategy

- Analysis on the game:
  - When $x = 0$ and $y = 0$, the winning condition is $a = b$.
  - When $x = 0$ and $y = 1$, the winning condition is $a = b$.
  - When $x = 1$ and $y = 0$, the winning condition is $a = b$.
  - When $x = 1$ and $y = 1$, the winning condition is $a \neq b$.
- What is the maximum win probability for Alice and Bob? How to achieve that probability?
- Classical strategy:
  - Deterministic: 75%.
  - Private randomness: 75%.
  - Shared randomness: 75%.
  - follows Bell's inequality
- Quantum strategy:
  - Shared quantum entanglement: $(\cos \frac{\pi}{8})^2 \approx 85\%$.
  - [Boris, 1980] proves that the quantum strategy is optimal.
  - violates Bell's inequality.
- Please refer to Wikipedia for more information about this Bell's game by searching the keywords: CHSH inequality/CHSH game.

Implications of Bell's Game

- Physical perspective: The violation of Bell's inequality implies that quantum mechanics allows for non-local correlations and challenges the classical notion of realism.
  - Locality: The effect of an event at one location cannot travel faster than the speed of light to influence another event at a different location.
  - Realism: The idea that physical properties exist with definite values, independent of whether they are measured. This implies that particles have pre-existing properties (like position, momentum, or spin) even when not observed.
- Quantum supremacy: Quantum computers can solve a problem that is infeasible for any classical computer to solve in a reasonable time frame.
  - We can encode 2^n bits of classical information with only n qubits. Then quantum computer can operate on a superposition of all possible states simultaneously, exponentially increasing its computational power.
  - Just as entanglement allows Alice and Bob to achieve correlations in Bell's game that are impossible classically, it also allows quantum computers to perform complex operations on many qubits at once, leading to a parallelism that classical computers cannot match.

Table of Contents

3 Applications and Future of Quantum Computing

- ▶ Introduction
- ▶ Bell's Game
- ▶ Applications and Future of Quantum Computing
- ▶ Conclusion and Takeaways
- ▶ Reference

Current Applications: Quantum Computer

- Quantum information theory: This field explores how quantum systems can be used to store, process, and transmit information at most.
- Quantum coding theory: This theory extends classical error-correcting codes to quantum systems and focuses on designing codes that can detect and correct errors without disturbing the quantum information, ensuring the reliability of quantum computations and communications.
- Quantum theoretical computer science (quantum TCS): The key problems include understanding which problems quantum computers can solve more efficiently than classical computers.
- Quantum algorithm design: This direction involves creating algorithms that run on quantum computers and can outperform classical algorithms for certain tasks.
  - Shor's algorithm: factoring large numbers.
  - Grover's algorithm: searching unsorted databases.

Current Applications: Quantum Computer

- Has anyone built a quantum computer yet?

Current Applications: Quantum Computer

- Has anyone built a quantum computer yet?
  - IBM Quantum: Their IBM Quantum System One is among the most advanced commercially available quantum computers.
  - Google Quantum AI: Google made headlines in 2019 by claiming "quantum supremacy" when its quantum computer, Sycamore, solved a problem in 200 seconds that would take the fastest classical supercomputer 10,000 years to complete.
  - Microsoft Azure Quantum: While they haven't yet built a large-scale quantum computer, they offer cloud access to quantum simulators and hardware through Azure Quantum, partnering with other hardware providers like IonQ and Honeywell.
  - Alibaba Quantum Laboratory (AQL): Alibaba, through its cloud computing division Alibaba Cloud, has been developing quantum computers and offers cloud access to quantum computing resources.
  - the Chinese Academy of Sciences: a 176-qubit quantum computing platform called Zuchongzhi, which has performed quantum supremacy experiments.

Current Applications: Quantum Network

- Quantum key distribution (QKD): A technique ensuring secure communication by leveraging quantum entanglement and the no-cloning theorem.
- Quantum repeaters for long-distance communication: A crucial device for building long-distance quantum networks and enabling reliable transmission of quantum information.
- Distributed quantum computing: Distributed quantum computing can combine quantum resources from different locations, allowing the parallel execution of quantum algorithms or tasks that may be too complex for a single quantum processor.
- Entanglement-based Quantum Networks: Quantum networks use entangled qubits to perform quantum teleportation, where quantum information is transferred between distant locations without physically moving the qubits themselves.

Future Potential

- Civilian quantum computer
- Optimization problem: combinatorial optimization problem
- Drug discovery.
- Weather prediction.
- Solve complex math problem.
- Global quantum network.
- Quantum AI.
- ...

Table of Contents

4 Conclusion and Takeaways

- ▶ Introduction
- ▶ Bell's Game
- ▶ Applications and Future of Quantum Computing
- ▶ Conclusion and Takeaways
- ▶ Reference

Key Points

4 Conclusion and Takeaways

- Quantum computing leverages superposition, entanglement, and quantum gates to perform calculations that are infeasible for classical computers.
- Bell's game is a simple example that shows how quantum mechanics can outperform classical systems.
- The development of quantum computing mainly benefits from quantum mechanics in Physics.
- Quantum computing has spawned fruitful applications, including quantum computers and quantum networks.
- There are many more potential future applications for quantum computing, such as global quantum networks and quantum AI.

Further Exploration

Recommended books

- Nielsen M A, Chuang I L. *Quantum computation and quantum information*[M]. Cambridge university press, 2010.
- J. Watrous, *The Theory of Quantum Information*, Cambridge University Press, 2018.
- M. M. Wilde, *Quantum Information Theory*, 2nd Edition, Cambridge University Press, 2017.
- B. C. Hall, *Quantum Theory for Mathematicians*, Springer, 2013
- P. A. M. Dirac, *The Principle of Quantum Mechanics*, Oxford University Press, 1935
- J. von Neumann, *Mathematical Foundations of Quantum Mechanics*, Princeton University Press, 1955.
- R. P. Feynman and A. R. Hibbs, *Quantum Mechanics and Path Integrals*, McGraw-Hill Companies Inc., 1965.

Recommend online course

- Youtube video: Quantum Computing-CMU by Ryan O'Donnell

Recommended papers

- M. Liu, Z. Li, X. Wang and J. C. S. Lui, "*LinkSelFiE: Link Selection and Fidelity Estimation in Quantum Networks*," IEEE INFOCOM 2024 - IEEE Conference on Computer Communications, Vancouver, BC, Canada, 2024
- M. Liu, Z. Li, K. Cai, J. Allcock, S. Zhang and J. C. S. Lui, "*Quantum BGP with Online Path Selection via Network Benchmarking*," IEEE INFOCOM 2024 - IEEE Conference on Computer Communications, Vancouver, BC, Canada, 2024

Contact me via email: bluo23@cse.cuhk.edu.hk

Table of Contents

5 Reference

- Introduction
- Bell's Game
- Applications and Future of Quantum Computing
- Conclusion and Takeaways
- Reference

References

5 Reference

Boris, T. (1980).
Quantum generalizations of bell's inequality.
Letters in Mathematical Physics, 4:93–100.

Quantum Computing: A Candidate for Future Technological Revolution

Thank you for listening!
Any questions?