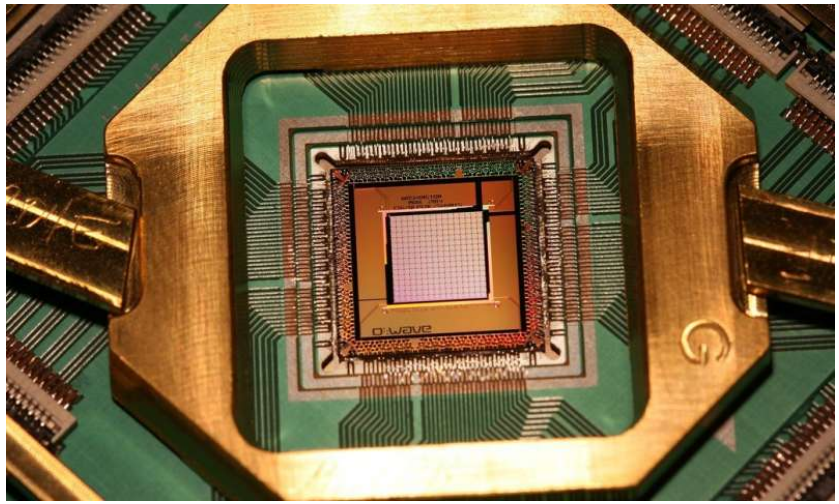
A brief survey on quantum computing



Edward Poon
University of Ottawa

Outline

Goal: Provide a high-level overview of what quantum computing is, including its history and applications.

Overview:

1. Classical vs quantum computing
2. Timeline of quantum computing
3. Applications of quantum computing

Outline

Goal: Provide a high-level overview of what quantum computing is, including its history and applications.

Overview:

1. Classical vs quantum computing
2. Timeline of quantum computing
3. Applications of quantum computing

Outline

Goal: Provide a high-level overview of what quantum computing is, including its history and applications.

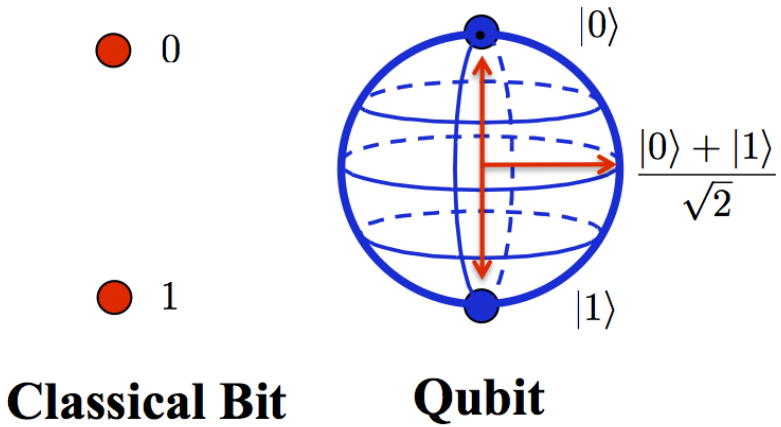
Overview:

1. Classical vs quantum computing
2. Timeline of quantum computing
3. Applications of quantum computing

Classical vs quantum computing

Superposition

- Classical computers: bits are in the state 0 or 1.
- Quantum computers: qubits are in the state 0 or 1 or a superposition of the two.



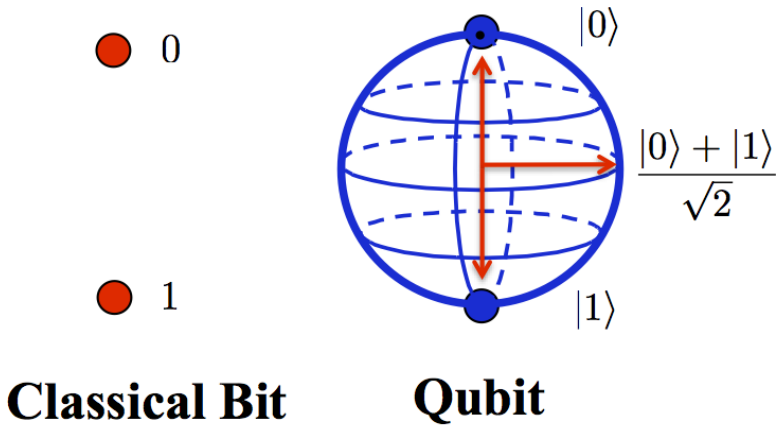
Example

Three bits can be in one of eight states, but three qubits can be in a superposition of eight states.

Classical vs quantum computing

Superposition

- Classical computers: bits are in the state 0 or 1.
- Quantum computers: qubits are in the state 0 or 1 or a superposition of the two.



Example

Three bits can be in one of eight states, but three qubits can be in a superposition of eight states.

Timeline of quantum computing

1980 Yuri Manin proposes idea of quantum computing
1981 Richard Feynman proposes model for a quantum computer
1982 Paul Benioff proposes theoretical framework for a quantum computer
1985 David Deutsh formulates a description for a quantum turing machine
1998 Jonathan Jones and Michelle Mosca succesfully run a quantum algorithm on a 2 qubit quantum computer

Figure: David Deutsh

Applications of quantum computing

Fields of applications

- Security
  - Classical cryptography
  - Post-quantum and quantum cryptography
- Scientific modelling
  - Precision weather forecasting
  - Medical science
- Artifical intelligence
  - Autonomous cars
  - Machine learning models

Applications of quantum computing

Fields of applications

- Security
  - Classical cryptography
  - Post-quantum and quantum cryptography
- Scientific modelling
  - Precision weather forecasting
  - Medical science
- Artifical intelligence
  - Autonomous cars
  - Machine learning models

Applications of quantum computing

Fields of applications

- Security
  - Classical cryptography
  - Post-quantum and quantum cryptography
- Scientific modelling
  - Precision weather forecasting
  - Medical science
- Artifical intelligence
  - Autonomous cars
  - Machine learning models

Applications of quantum computing

Fields of applications

- Security
  - Classical cryptography
  - Post-quantum and quantum cryptography
- Scientific modelling
  - Precision weather forecasting
  - Medical science
- Artifical intelligence
  - Autonomous cars
  - Machine learning models

Quantum computing and the RSA cryptosystem

Rivest-Shamir-Adleman cryptosystem (1977)

- Widely used public-key cryptosystem
- Easy to multiple two prime numbers together
- Hard to find prime factors of a larger number

Shor's algorithm (Shor 1994)

- Finds the period of a function containing the RSA key and computes the greatest common divisor
- Factors an n-bit number in $\mathcal{O}(n^3)$ time

Quantum computing and the RSA cryptosystem

Rivest-Shamir-Adleman cryptosystem (1977)

- Widely used public-key cryptosystem
- Easy to multiple two prime numbers together
- Hard to find prime factors of a larger number

Shor's algorithm (Shor 1994)

- Finds the period of a function containing the RSA key and computes the greatest common divisor
- Factors an n-bit number in $\mathcal{O}(n^3)$ time

Summary

- More powerful than classical computers
- Many applications in different fields
- Current quantum computers have few qubits
  - Recommended RSA key size: 2048 bits
  - Largest number factored by a quantum computer: 56153 (16 bits)
- Fully functioning quantum computer with many qubits still a long-term goal

Summary

- More powerful than classical computers
- Many applications in different fields
- Current quantum computers have few qubits
  - Recommended RSA key size: 2048 bits
  - Largest number factored by a quantum computer: 56153 (16 bits)
- Fully functioning quantum computer with many qubits still a long-term goal

Summary

- More powerful than classical computers
- Many applications in different fields
- Current quantum computers have few qubits
  - Recommended RSA key size: 2048 bits
  - Largest number factored by a quantum computer: 56153 (16 bits)
- Fully functioning quantum computer with many qubits still a long-term goal