The benefits of quantum computing for ICTs

Introduction to quantum computing

KOBENAN Ali Ouattara
Speaker

Institut National Polytechnique Félix Houphouet Boigny

19th September 2023

Plan

1. Some fundamental notions of quantum mechanics

Plan

1. Some fundamental notions of quantum mechanics
2. Quantum computing

Plan

1. Some fundamental notions of quantum mechanics
2. Quantum computing
3. Quantum computing and current needs

Plan

1. Some fundamental notions of quantum mechanics
2. Quantum computing
3. Quantum computing and current needs
4. Synthesis

quantum mechanics

Fundamental principles

- In quantum mechanics, all matter is both a particle and a wave: *wave-particle duality*;
- Two fundamental laws govern quantum mechanics:
  - Intrication;
  - Superposition.

Quantum intrication

Definitional approach

- Particles do not have a fixed cinematic state;

Quantum intrication

Definitional approach

- Particles do not have a fixed cinematic state;
- Intrication The phenomenon whereby two previously related particles or groups of particles form a (linked) system of each other regardless of the distance between them;

Quantum intrication

Definitional approach

- Particles do not have a fixed cinematic state;
- Intrication The phenomenon whereby two previously related particles or groups of particles form a (linked) system of each other regardless of the distance between them;
- These particles are then said to be intricated or to be in an intricated state.

The law of conservation of an intricated system

- "When you 'touch' one object in a pair of entangled objects, the second one twitches, despite the distance," says Swiss physicist Nicolas Gisin.

The law of conservation of an intricated system

- "When you 'touch' one object in a pair of entangled objects, the second one twitches, despite the distance," says Swiss physicist Nicolas Gisin.
- Quantum intrication refers to the existence of an invisible link between two particles that were emitted at the same time, regardless of the distance between them.

Quantum superposition

Definitional approach to superposition

- Richard Feynman (winner of the 1965 Nobel Prize in Physics) said: "If you think that an electron revolves around a nucleus like a satellite revolves around a planet, then your vision of the atom is stuck in 1915";

Quantum superposition

Definitional approach to superposition

- Richard Feynman (winner of the 1965 Nobel Prize in Physics) said: "If you think that an electron revolves around a nucleus like a satellite revolves around a planet, then your vision of the atom is stuck in 1915";
- The same quantum state can have several values for a certain observable quantity.

Approach to the concept of quantum computing

- One of the multidisciplinary fields that includes computer science, physics and mathematics that uses **the principles of quantum mechanics** to solve complex problems more quickly than traditional computer science;

Approach to the concept of quantum computing

- One of the multidisciplinary fields that includes computer science, physics and mathematics that uses **the principles of quantum mechanics** to solve complex problems more quickly than traditional computer science;

- It uses a class of bits called quantum bits or qbits;

Approach to the concept of quantum computing

- One of the multidisciplinary fields that includes computer science, physics and mathematics that uses **the principles of quantum mechanics** to solve complex problems more quickly than traditional computer science;
- It uses a class of bits called quantum bits or qbits;
- The computers used in this field have properties that apply the use of qbits: they are called quantum computers.

quantum computers

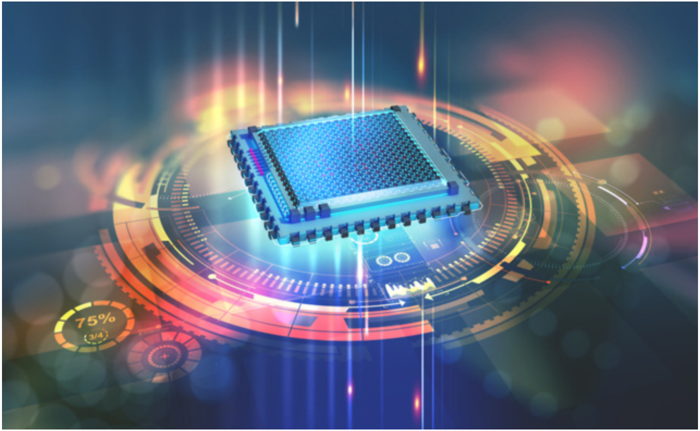

Figure 1: quantum computers

Bits and qbits

- The bit is the representation and processing unit for information stored in memory in conventional computing;
- A classical bit can only take two states, represented by 0 and 1;
- Information is characterised by a stream of bits (the binary word);
- The states of the bits are taken sequentially;
- The processing of an item of information represented by the binary word uses the combination of the two states of each bit making up the binary word in each clock execution sequence.

Bits and qbits

- Quantum computers use qbits as information processing symbols and storage units;
- Quantum bits (qbits) can take on several states simultaneously in a single clock sequence;
- Quantum bits use the notion of superposition of states;
- The state of a qbit is represented by $:|0>,<1|$;
- Using the superposition of qbit states in words enables multiple results to be obtained in a single sequence of operations, and speeds up information processing.

Bits and qbits

Operations with qbits

- The qubit enables operations to be processed much more efficiently and quickly, thanks to the parallelisation of calculations;

Bits and qbits

Operations with qbits

- The qubit enables operations to be processed much more efficiently and quickly, thanks to the parallelisation of calculations;
- Data represented on n qbits requires 2^n parallel operations;

Bits and qbits

Operations with qbits

- The qubit enables operations to be processed much more efficiently and quickly, thanks to the parallelisation of calculations;
- Data represented on n qbits requires 2^n parallel operations;
- During task execution, the register of qubits is in a quantum superposition of all its possible states ($|00\ldots0>$, $|10\ldots0>$, $|11\ldots1>$, $|10\ldots1>$), This enables parallel computing, which increases the speed at which operations are carried out.

The requirements of new applications

- We live in a digital age, with an increasingly connected world;

The requirements of new applications

- We live in a digital age, with an increasingly connected world;
- Today's applications require large quantities of data, with processing requiring more operations;

The requirements of new applications

- We live in a digital age, with an increasingly connected world;
- Today's applications require large quantities of data, with processing requiring more operations;
- Information and communication technology has complex problems, and solving them depends on their complexity.

The requirements of new applications

The requirements of new applications

- The traditional computers used in ICT today are beginning to show their limitations in this generation of problems;

The requirements of new applications

- The traditional computers used in ICT today are beginning to show their limitations in this generation of problems;
- One solution motivated by the limitations of the classical computer is the use of the quantum computer.

Different areas of application

Simon Perdrix, researcher in quantum computing at CNRS

When we manage to make full use of quantum computing, we will be able to solve a large number of problems that are beyond the reach of conventional computers.

Different areas of application

Artificial intelligence

Weather forecasts, financial forecasts, road traffic forecasts and all areas using artificial intelligence will be optimised. As will all those that use "machine learning", a special feature of artificial intelligence.

Different areas of application

Artificial intelligence

Weather forecasts, financial forecasts, road traffic forecasts and all areas using artificial intelligence will be optimised. As will all those that use "machine learning", a special feature of artificial intelligence.

Medicine

Investment in pharmaceutical laboratories because of the price that this technology could be worth when it is released. Faster, more accurate medical diagnoses, the development of therapeutic molecules or the creation of new drugs requiring enormous calculation and modelling times.

Different areas of application

Cryptography and security

The current global cryptography system used by multinationals, trading systems, banks, etc. is RSA. Given the technological advances used by hackers today, companies could use quantum code to increase the complexity of their security system to make it difficult to penetrate.

Different areas of application

Mathematical modelling

Modelling today's life problems requires much more advanced computing power. It is absolutely essential to use techniques that are adapted to this century to ensure that the results are as accurate as possible. Modelling is part and parcel of solving complex problems that require huge computational operations that would take supercomputers long enough to achieve.

Challenges in standardising quantum computing

- Each organisation creates its own quantum technology according to its objectives and needs (Europe, the United States, Asia);
- Most inventions are still in the experimental stage;
- Africa needs to align itself with the standard that will be in force to deal with the huge gap in new technologies;
- This is an evolving field, and there is a need for a universal standard so that each structure can popularise its own machine adapted to its own realities.

General review

synthesis

Quantum computing brings many advantages to new Information and Communication Technologies in terms of security, computing power and optimisation capabilities. It paves the way for innovative solutions in this new era using the principles of quantum mechanics.

Some references

- https://www.pwc.fr/fr/assets/files/pdf/2019/11/fr-france-pwc-point-of-view-quantum-computing-2019.pdf
- https://www.cscience.ca/chroniques/informatique-quantique-et-cybersecurite-une-arme-a-double-tranchant/
- https://www.ibm.com/fr-fr/topics/quantum-computing
- https://www.zdnet.fr/pratique/tout-comprendre-a-l-informatique-quantique-39891035.htm

Thank you for your kind attention!