Quantum computer

What is a quantum computer?

- A quantum computer uses the quantum properties of matter, such as superposition and inseparability, to perform operations on data.
  - The superposition principle states that a quantum system can simultaneously exist in several distinct quantum states, and its general state is a combination of these states. Only at the moment of measurement, the system "collapses" into one of the possible states. For example, an electron can simultaneously be in a superposition of positions or spin states until it is observed. This property underlies the wave function in Schrödinger's equation.
  - Quantum inseparability refers to the phenomenon whereby two or more quantum particles become correlated in such a way that the state of one cannot be described independently of the state of the other, even if the particles are at great distances from each other. Any change in the state of one particle instantly affects the state of the other. This principle goes against classical intuition and was called by Einstein "spooky action at a distance".
- Unlike classical computers that perform logical operations using bits (binary strings of 0s and 1s) and transistors, quantum computers operate by controlling the behavior of qubit particles, or quantum bits, which can simultaneously have several positions (1 and 0 in the same time), which means they can process an enormous number of potential results simultaneously.
- Quantum computers are rated with a quantum volume rating, which takes into account the total number of qubits. Although quantum computer prototypes already exist, they can currently only perform tasks similar to those performed by a normal computer, but much faster.

Advantages

- A quantum computer is very fast in finding solutions.
  - Quantum computers can solve certain problems (such as factoring large numbers or optimization - Shor Algoritm) much faster than classical computers
- Quantum parallelism
  - Due to the principle of superposition, a qubit can simultaneously represent multiple states (0 and 1), allowing the parallel processing of a huge number of combinations.
- Improving cyber security
  - Although quantum computers can break classical encryption methods, they can also provide more secure cryptography solutions based on quantum key distribution, which are virtually impossible to intercept without being detected.

Disadvantages

- Cooling difficulties
  - Quantum computers require extremely low temperatures, close to absolute zero, to keep the qubits stable.
- Limited accessibility and high costs
  - Quantum computers are very expensive and access to them is limited to research centers, advanced laboratories and large companies such as IBM, Google and D-Wave.
- Impact on cyber security

Programming language

- Quantum computation language (QCL)
  - High-level quantum programming language written in C++.
  - It is open-source and runs under Linux.
  - It can work on any quantum computer architecture based on qubits, as well as a quantum computing simulation language. The first version appeared in 1998, and the current version appeared in 2006.

Quantum Algorithms

- Deutsch-Jozsa Algorithm

  - The first quantum algorithm, the simplest example of a quantum algorithm that outperforms a classical algorithm in efficiency. This algorithm distinguishes between a function $f: \{0,1\}^n \rightarrow \{0,1\}$ that is constant and one that is balanced. A function is balanced if it takes the value 0 for exactly half of the possible values of the argument and the value 1 for the other half (the function for $n=1$ is balanced if $f(0) \neq f(1)$).
- Simon Algorithm
  - Is related to the Deutsch-Jozsa algorithm.
- Grover Algorithm
  - Is a search algorithm.
- Euclid Algorithm
  - Is used to find the greatest common divisor of two integers.
- Shor Algorithm
  - Is used for efficient factorization of a large number using qubit entanglement and the principle of superposition.

Areas of use

- Quantum Cryptography
  - Quantum computers are being used in the development of much more secure versions of information encryption. Qubits, because they obey the laws of quantum mechanics, can provide a secure basis for exchanging secret messages. Quantum encryption could make it impossible for hackers to discover the access keys of vulnerable systems, due to the indeterminate state in which the information needed ,for decryption, is found.
- Medicine
  - Another application of these systems would be in medicine, in the field of molecular modeling. One of the most promising applications of quantum computers is simulating the behavior of matter down to the molecular level. Pharmaceutical companies use quantum simulations to analyze and compare compounds that could lead to the creation of new drugs and protein models, or to improve the speed and quality of medical imaging.
- Artificial Intelligence
  - Artificial intelligence can benefit massively from the use of quantum computers. The most intelligent machine learning systems work based on a process of "trial and error" (identification of statistical anomalies). "Deep" and "machine learning" systems will become much stronger and faster if they can take advantage of the superposition phenomenon.
- Automotive Industry
  - Automakers such as Volkswagen and Daimler are using quantum computers to simulate the chemical makeup of electric vehicle batteries to help find new ways to improve their performance. Volkswagen has presented a service that calculates optimal routes for buses and taxis in cities to minimize traffic congestion.

- Aeronautical Industry
  - Airbus uses quantum computers to help calculate the most efficient take-off and landing paths for aircraft and route optimization.
- Internet
  - The big companies that provide search services on the Internet - Google, Yahoo, Microsoft - could benefit enormously from quantum algorithms that can index and search huge databases much faster. Also for detecting viruses and hacking in networks.
- Weather forecast
  - Quantum computers could help build better climate models. The UK's National Weather Service has already started investing in these new technologies.

Conclusion

Quantum computers are just at the beginning and we are still looking for efficient ways of exploiting their processing power. Their main advantage over classic computers is huge only in specific areas of application, and the optimal extreme running conditions make them a rather difficult choice for ordinary consumers.

Refereces

- https://ro.wikipedia.org/wiki/Calculator_cuantic
- https://usv.ro/fisiere_utilizator/file/Doctorat/2015/rezumate/rezumat teza Ailutoaiei (Barila).pdf
- https://despretot.info/computer-cuantic-calculator-cuantic-definitie-functionare/
- https://tehnocultura.ro/2013/07/27/cum-functioneaza-un-computer-cuantic-si-ce-sunt-qubitii/

TITIENI ROBERT PAUL
227