Quantum Algorithms

Daniel Aguilera

Quantum Theory

- Very small particles and light behave differently from objects we encounter in normal life, which are described by classical mechanics and classical electrodynamics. The mechanics of light and matter at the atomic and subatomic scale are described by quantum theory, which forms the underlying principles of chemistry and most of physics.
- An important part of quantum theory was established at the beginning of the 20th century, by people like Erwin Schrödinger, Wolfgang Pauli, Marie Curie, Hendrik Lorentz, Werner Heisenberg, Louis de Broglie, Max Planck and Albert Einstein, all of them present at the 5th Solvay Conference on Quantum Mechanics, 1927 as.

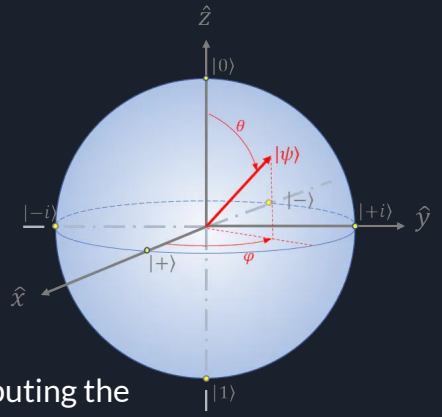
Quantum Computers

A quantum computer is a device performing quantum computations. It manipulates the quantum states of qubits in a controlled way to perform algorithms. A universal quantum computer is defined as a machine that is able to adopt an arbitrary quantum state from an arbitrary input quantum state. Quantum computers use this principle to accurately compute the behavior of quantum systems or very small particles that follow the laws of quantum mechanics, for example the behaviour of electrons in a hydrogen molecule or more complex systems like how proteins fold. It can also be used to run optimization algorithms very efficiently, execute machine learning algorithms or do pattern recognition much more efficiently then classical (super)computers canj.

The development of a quantum computer is currently in its infancy, systems consist of a few to a few tens of quantum bits (qubits). Main challenges in further development are to make the quantum computer scalable. This means that it will be able to perform universal quantum operations using unreliable components.

In the last two decades of the previous century more and more quantum mechanical concepts were brought into information processing, allowing the development of so-called quantum algorithms. One of the early breakthroughs and still one of the strongest arguments for quantum computing to date is Shor's algorithm for integer factorization into primes. In many ways this algorithm can be seen as a starting signal. Since then the efforts in learning about what is required to build a quantum computer increased manifold.

What is a qubit?

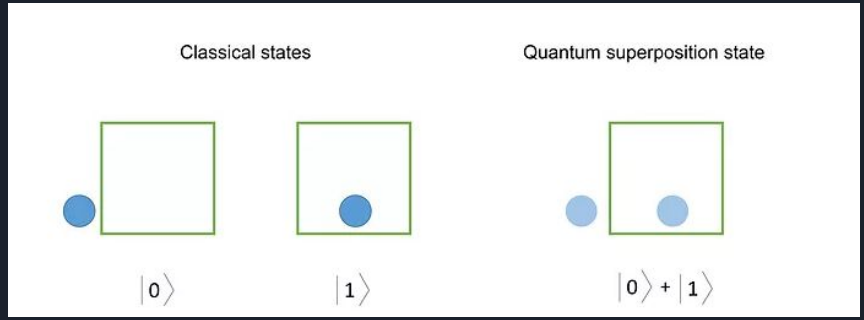


A qubit (or quantum bit) is the quantum mechanical analogue of a classical bit. In classical computing the information is encoded in bits, where each bit can have the value zero or one. In quantum computing the information is encoded in qubits. A qubit is a two-level quantum system where the two basis qubit states are usually written as $|0\rangle$ and $|1\rangle$. A qubit can be in state $|0\rangle$, $|1\rangle$ or (unlike a classical bit) in a linear combination of both states. The name of this phenomenon is superposition.A general -pure- qubit state is expressed as:

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

where α and β are the complex probability amplitudes for each basis state. Note that the choice of basis states is arbitrary, each set of orthogonal states can be used as basis states.

Superposition



One of the properties that sets a qubit apart from a classical bit is that it can be in superposition. Superposition is one of the fundamental principles of quantum mechanics. In classical physics, a wave describing a musical tone can be seen as several waves with different frequencies that are added together, superposed. Similarly, a quantum state in superposition can be seen as a linear combination of other distinct quantum states. This quantum state in superposition forms a new valid quantum state.

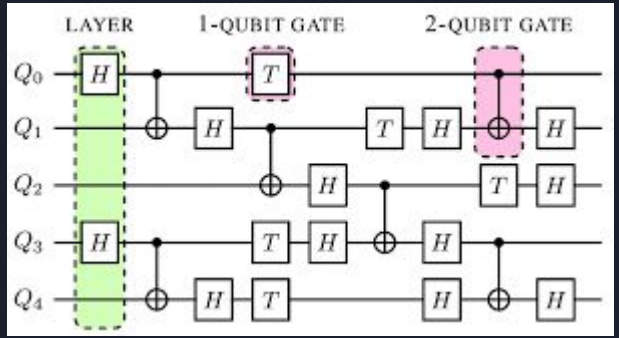
Qubits can be in a superposition of both the basis states $|0\rangle$ and $|1\rangle$. When a qubit is measured (to be more precise: only observables can be measured), the qubit will collapse to one of its eigenstates and the measured value will reflect that state. For example, when a qubit is in a superposition state of equal weights, a measurement will make it collapse to one of its two basis states $|0\rangle$ and $|1\rangle$ with an equal probability of 50%. $|0\rangle$ is the state that when measured, and therefore collapsed, will always give the result 0. Similarly, $|1\rangle$ will always convert to 1.

Entanglement

One of the other counter-intuitive phenomena in quantum physics is entanglement. A pair or group of particles is entangled when the quantum state of each particle cannot be described independently of the quantum state of the other particle(s). The quantum state of the system as a whole can be described; it is in a definite state, although the parts of the system are not. When two qubits are entangled there exists a special connection between them. The entanglement will become clear from the results of measurements. The outcome of the measurements on the individual qubits could be 0 or 1. However, the outcome of the measurement on one qubit will always be correlated to the measurement on the other qubit. This is always the case, even if the particles are separated from each other by a large distance. Examples of such states are the Bell states.

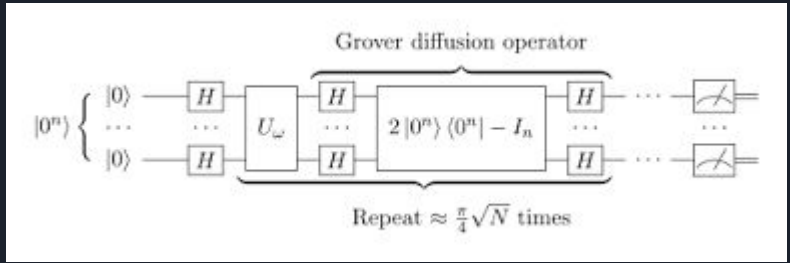
Quantum circuits

Quantum algorithms are most commonly described by a quantum circuit, of which a simple example is shown in the figure below. A quantum circuit is a model for quantum computation, where the steps to solve the problem are quantum gates performed on one or more qubits. A quantum gate is an operation applied to a qubit that changes the quantum state of the qubit. Quantum gates can be divided into single-qubit gates and two-qubit gates, depending on the number of qubits on which they are applied at the same time. Three-qubit gates and other multi-qubit gates can also be defined. A quantum circuit is concluded with a measurement on one or more qubits. A difference with a classical algorithm is that a quantum algorithm is always reversible. This means that if measurements are not a part of the circuit, a reverse traversal of the quantum circuit will undo the operations brought about by a forward traversal of that circuit.



The Power of Quantum Algorithms

An algorithm is a step-by-step procedure to perform a calculation, or a sequence of instructions to solve a problem, where each step can be performed on a computer. Therefore, an algorithm is a quantum algorithm when it can be performed on a quantum computer. In principle it is possible to run all classical algorithms on a quantum computer. However, the term quantum algorithm is applied to algorithms of which at least one of the steps is distinctly ‘quantum’, using superposition or entanglement. Problems that are fundamentally unsolvable by classical algorithms (so called undecidable problems) cannot be solved by quantum algorithms either. The added value of quantum algorithms is that they can solve some problems significantly faster than classical algorithms. The best-known examples are Shor’s algorithm and Grover’s algorithm. Shor’s algorithm is a quantum algorithm for integer factorization. Simply put, when given an integer N, it will find its prime factors. It can solve this problem exponentially faster than the best-known classical algorithm can. Grover’s algorithm can search an unstructured database or unordered list quadratically faster than the best classical algorithm with this purpose.



Thank You