Veijo Hänninen

Aiming for Quantum Computer

AIMING FOR A QUANTUM COMPUTER

Veijo Hänninen

Publisher: BoD™ – Books on Demand, Helsinki, Finland
Print: Books on Demand GmbH, Norderstedt, Germany
ISBN: 978-952-800-258-1

TABLE OF CONTENTS

QUANTUM COMPUTER

Revolution or not

The quantum computer has raised a lot of interest, particularly in the sense that it would be able to disable the data protection methods that are currently widely in use, i.e. internet encryption.

The fact that we delve deeper in to the quantum world, naturally also interests researchers and scientists in particular.

The subject is also occasionally present among information technology users, but the theme of this book is how the subject is currently progressing.

There is a strong belief among researchers in the emergence of a quantum computer. It can be partially said to already be a reality, but it is yet to be seen whether it will reach the level at which it is most blazed.

From quantum limits to quantum space

Nowadays, electronics and information technology dive even deeper in to the quantum world.

It used to think quantum mechanics was actually a type of endpoint for the development of information technology; since all the components keep getting smaller, they eventually reach the fragile phenomena of the quantum world.

In 1985, theoretical physicist, David Deutsch, from the University of Oxford counterversed this composition. He proved that quantum mechanics does not limit computing in any way, but rather, expands on it in an amazing manner.

While the advantage of standard information technology's circuit engineering is component density, the advantage of the quantum computer is not the density of qubits as such, rather the possibility to operate with the superposition of quantum states. The basis of the quantum computer's operation can certainly be sought at even a level of one atom.

Computing space

Quantum physics involves the mathematical concept Hilbert space, which is a certain type of "space of vectors". Although the classical state space is infinite, time only runs in one direction.
In physicist Robert Penronen's words, "Hilbert space is the same as the universe, where time and all possible vectors run in all possible directions".

These additional degrees of freedom provide an amazing bonus, and for this reason the quantum computer can calculate certain things extremely quickly. That is, it can reach an infinitely larger space - Hilbert space - than a traditional computer.

Computing method

Traditional computers calculate step-by-step, using a method called serial computing. They can also breakdown the computation work by separately calculating, for example, the units, tens, hundreds and thousands, and then, at the end, combining the results. The time to execute parallel computing such as this is divided among the participating portions.

But quantum computers also work by using a method called massively parallel computing. The quick implementation of parallel logic operations is achieved with a superposition of states.

Normal computers utilise transistor-based logic gates, which are circuits found throughout circuit boards. Quantum logic gates work with a superposition of qubit states. In other words, with specific spatial states.

When Deutsch developed massively parallel computing, he recognised that it was an excellent and strong solution, which looks for suitable problems.
Finding them is a work of its own, to create an algorithm.

Decoherence

Although quantum computing is efficient, it is also technically incoherent.
The properties of quantum computing that make it extremely efficient also make it exceptionally vulnerable.

The core of quantum computing is quantum entanglement.
Entanglement allows qubits and their combinations to be processed as one unit, because they are inseparably connected to each other.
But this makes it also very sensitive to unwanted interference from the outer environment. Interferences can make the entire chain of entangled qubits collapse in to a queue of traditional random bits, in which case the original computing objective has been lost.

This problem almost caused development to collapse. But developers accepted, for example, the necessity of errors caused by noise and invented various methods to correct errors. Since the computing power is so strong, a lot of resources, or qubits, can be sacrificed for the correction of errors.

Complex hardware

The current experimental implementations of quantum computers are based on various solutions. In principle, a two-state physical system is sufficient for forming qubits. Technically speaking, the most difficult part is to keep the qubits, and the various states formed with them, isolated from external interferences, or else the quantum mechanical properties of qubits are lost. One basic solution for this is to keep the temperature of qubits extremely close to absolute zero.

Lasers and accurate microwaves and/or other electro-magnetic waves can be used to modify the states of qubits, but in more recent solutions, control is managed with voltages.

Of course, the control of such complex operations requires traditional control technology, such as for entering quantum computing inputs and calculating the results.

How does quantum computing work?

The basic operating unit of a quantum computer is a qubit. It can be any two-state quantum system. They are apparent in, for example, atoms, electrons, photons or superconducting connections. The idea is that their two states can be placed in a superposed state.

A digital bit is 1 **or** 0. An analogue bit can be any value between 0 and 1. For example, a value within the control quantity of 0 - 1 volts, at a certain resolution.

A qubit is the superposition of values 0 **and** 1, and it can be expressed with a vector, in the same way as an imaginary figure familiar to electricians, but unlike in a two-dimensional coordinate system, in a ball-like space.

So, a qubit can be in the superposition of two states, and when it is measured, it restores one of the two states on the basis of each state's probability, and it is given the value 0 or 1.

No computing can be carried out with a single qubit, instead mutually interacting qubits are required. In this case, they are said to be entangled and only then does the actual parallel computing take place.

When two qubits become entangled, and if we first measure one and obtain a clockwise spin, then the other one provides a counter clockwise spin, and vice versa.
Therefore, until we measure them, these two qubits can be considered as one system, which has probable values, i.e. amplitudes.

If we process two qubits, the basic states can be 00, 01, 10, 11, but qubits can also simultaneously be in the superposition of all of these. To be able to present two qubits, we need four probabilities/amplitudes, while eight probabilities/amplitudes are needed to present three qubits.

Amplitude is increased or decreased by means of constructive or destructive interference. Computing ends once an amplitude reaches 1 or 0.

Superposition has a significant purpose in quantum computing, because they behave similarly to waves that overlap each other.

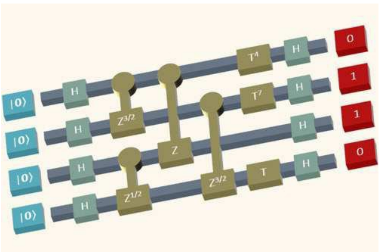
If we have n number of qubits, we need an amount of 2^ n to represent the general state of the relevant quantum system. So, by increasing the number of qubits, we can produce systems that represent an enormous amount of states.

Quantum logic gates

Quantum computers also need a logic that can process more than one qubit.

The structural modules of quantum circuits (quantum computing model) are quantum logic gates. They are equivalent to the logic gates of the traditional data processing model, but unlike many classical logic gates, quantum logic gates can restore themselves.

For example, the classical AND gate is not suitable for the quantum world, but the NOT gate works. The Hadamard gate also operates as one qubit and creates a superposition.



University of Bristol

Various controlled gates operate with two or more qubits, where one or more qubits work as the control for a certain action. For example, the controlled NOT gate (CNOT) operates with two qubits and performs the NOT operation with the second qubit once the first qubit is |1>, otherwise it remains unchanged.

The quantum computer has raised a lot of interest, particularly in the sense that it would be able to disable the data protection methods that are currently widely in use i.e. Internet´s encryption technology.

There is strong belief among researchers in the emerge of a quantum computer. It can be partly stated to already be reality, but is its future at the stage to which it is most blazed.

The author has been working as a journalist of professional electronic magazines and is now publishing the nanobitteja.fi website focusing on future electronics.

9 789528 002581

BoD™ BOOKS on DEMAND

www.bod.fi